Univerzita Palackého v Olomouci
Přírodovědecká fakulta
Společná laboratoř optiky

DISERTAČNÍ PRÁCE

Experimentální testování a využití kvantové provázanosti s fotonovými páry

Vypracovala:	**Mgr. Kateřina Jiráková**
Studijní program:	P1703 Fyzika
Studijní obor:	Aplikovaná fyzika
Forma studia:	Prezenční
Vedoucí diplomové práce:	doc. Mgr. Karel Lemr, Ph.D.
Termín odevzdání práce:	leden 2022

Prohlášení

Prohlašuji, že jsem předloženou disertační práci vypracovala samostatně pod vedením doc., Mgr. Karla Lemra, Ph.D., konzultovala ji s Mgr. Antonínem Černochem, Ph.D., a že jsem použila zdrojů, které cituji a uvádím v seznamu použitých pramenů.

V Olomouci dne 14. ledna 2022

. . . .

Mgr. Kateřina Jiráková

Palacky University in Olomouc
Faculty of Science
Joint Laboratory of Optics

DOCTORAL THESIS

Experimental Testing and Application of Quantum Entanglement With Photon Pairs

Author:	**Mgr. Kateřina Jiráková**
Study program:	P1703 Fyzika
Major:	Aplikovaná fyzika
Form of study:	Present study
Supervisor:	doc. Mgr. Karel Lemr, Ph.D.
Term of commitment:	January 2022

Poděkování

Chtěla bych poděkovat především svému školiteli doc. Mgr. Karlu Lemrovi, Ph.D. a konzultantovi Mgr. Antonínu Černochovi, Ph.D. za jejich rady a odborné vedení během mého studia a také za kontrolu této práce. Jejich nadšení pro vědu mě motivovalo během celého studia. Nebýt jejich ochoty se mnou text této práce konzultovat, nejspíš by ani nevznikl. Obdivuji jejich trpělivost, kterou mi tak často prokazovali, hlavně při práci v laboratoři, i přes to, že jsem při justování zpravidla udělala všechny chyby, které bylo možné udělat. A samozřejmě si velmi vážím jejich podpory stran mých obou stáží v Polsku.

Dále děkuji kolegům doc. Mgr. Janu Soubustovi, Ph.D., neboť mi vždy ochotně pomáhal s nástrojem `GLE` a prof. Mgr. Janu Peřinovi, Ph.D. za dobré rady během mého studia.

Kolegům Mgr. Vojtovi Trávníčkovi a Mgr. Ievgenijovi Archipovi, Ph.D. také patří můj vřelý dík, neboť mi byli nejen psychickou oporou po čas studia, ale naše časté debaty pro mě byly cenných zdrojem myšlenek a námětů.

Serdecznie dziękuję moim kolegom z Polski, prof. dr hab. Adamu Miranowiczowi, dr hab. Karolu Bartkiewiczowi i dr Arturu Barasińskemu za wsparcie oraz bardzo dobre pomysły do badań. Bardzo dobrze mi się z nimi współpracowało. Drogi Adamie, nigdy nie przestaje mnie zadziwiać, jak wpadasz na takie świetne pomysły. Praca z Tobą była cennym doświadczeniem i źródłem inspiracji. Karolu, jestem Ci bardzo wdzięczna za to, że mogłam spędzić te kilka miesięcy w Poznaniu pod Twoją opieką. Poszerzyło to znacznie moje horyzonty, nie tylko naukowo, ale i życiowo. Drogi Arturze, dziękuję bardzo za wspaniałą współpracę i twoją chęć zaproszenia mnie do Wrocławia i konsultacji pomimo ograniczeń w związku z Covid-19.

Děkuji také poskytovateli interního grantu Univerzity Palackého (IGA_PrF_2021_004), z něhož byl podporován můj výzkum.

A v neposlední řadě patří poděkování mé rodině a přátelům, kteří mně po celou dobu studia podporovali jak slovem, tak i mnoha skutky, nesobecky se pro mě obětovali a vím, že jen s jejich pomocí jsem se dostala tak daleko. Moc vám za to děkuji!

Bibliografická identifikace

Jméno a příjmení autora	Mgr. Kateřina Jiráková
Název práce	Experimentální testování a využití kvantové provázanosti s fotonovými páry
Typ práce	Disertační
Pracoviště	Společná laboratoř optiky
Vedoucí práce	doc. Mgr. Karel Lemr, Ph.D.
Rok obhajoby práce	2022
Abstrakt	Kvantová provázanost, neboli entanglement, je bezesporu jednou z nejzajímavějších stránek kvantové fyziky, neboť je v rozporu s naší přirozenou intuicí. Velmi zajímavé je, že se kvantová provázanost stala nepostradatelnou součástí různých kvantově-mechanických postupů, a proto ji stojí za to intenzivně studovat. Detekce kvantové provázanosti a určování její míry stále zůstává složitým problémem, a to jak z teoretického, tak experimentálního hlediska. Hlavním cílem této disertační práce je studium kvantových korelací a jejich hierarchie na experimentálně připravených a syntetizovaných dvou- a tří-qubitových Wernerových stavech s kontrolovatelným bílým šumem. Jeden z prezentovaných experimentů ukazuje, jak důležitou roli kvantová provázanost hraje v praktickém provádění kvantových protokolů, jako např. při kvantovém klonování. V tomto případě byl kvantový komunikační protokol zaměřen na kvantové peníze a jejich neodhalené padělání. Kvůli překotnému pokroku kvantových technologií může být pouze otázkou času, než budou kvantové peníze běžně používány při placení.
Klíčová slova	kvantová provázanost, nelokalita, schéma kvantových peněz, “concurrence”, nelokální podíl, Wernerův stav, kvantové korelace, odolnost vůči bílému šumu, kvantové klonování, kvantový útok
Počet stran	140
Počet příloh	5
Jazyk	anglický

Bibliographical identification

Autor's first name and surname	Mgr. Kateřina Jiráková
Title	Experimental Testing and Application of Quantum Entanglement With Photon Pairs
Type of thesis	Doctoral
Department	Joint Laboratory of Optics
Supervisor	doc. Mgr. Karel Lemr, Ph.D.
The year of presentation	2022
Abstract	Quantum entanglement is arguably one of the most striking features of quantum physics since it contradicts our natural intuition. Interestingly enough, entanglement has become indispensable part of diverse quantum mechanical procedures and is, therefore, worth being a subject of intensive study. Also its quantification and detection still remains a difficult problem from both theoretical and experimental point of view. The main objective of this Thesis is to study quantum correlations and their hierarchy on both experimentally prepared and synthesised two- and three-qubit Werner states with controllable white noise. One of the presented experiments showcases how important role entanglement plays in practical quantum protocols, e.g. in quantum cloning. In this case a quantum communications protocol focused on quantum money and their undetected counterfeiting. Since the rapid advancement of quantum technologies is indisputable, it might be only a matter of time before quantum money are used in practical payments.
Keywords	quantum entanglement, nonlocality, quantum money scheme, concurrence, nonlocal fraction, Werner states, quantum correlations, robustness against white noise, quantum retrieval game, quantum cloning, quantum attack
Number of pages	140
Number of appendices	5
Language	English

Tuto práci věnuji své mamince, která, třebaže vůbec nechápe, čím se vlastně zabývám, mě ze všech sil podporuje.

Contents

Symbols, Notation and Acronyms

Introduction & Chater 1

$\|0\rangle$, $\|1\rangle$	one-qubit logical states/basis
$\hat{\mathbb{1}}$	unitary matrix
A	amplitude of electromagnetic field
A ($\|A\rangle$)	anti-diagonal linear polarisation (state)
$\hat{a}$	annihilation operator
$\hat{a}^\dagger$	creation operator
BD	beam displacer
BDA	beam displacer assembly
BS	beam splitter
CC	coincidence counts
CHSH	Clauser-Horne-Shimony-Holt (inequality)
D ($\|D\rangle$)	diagonal linear polarisation (state)
EPR	Einstein-Podolsky-Rosen (paradox)
E., P. & R.	Einstein, Podolsky and Rosen
H ($\|H\rangle$)	horizontal linear polarisation (state)
HOM	Hong-Ou-Mandel (e.g., interference or dip)
I_{inc}	incident beam power intensity
LHV(T)	local hidden variable (theory)
L ($\|L\rangle$)	left-handed circular polarisation (state)
PBS	polarising beam splitter
PC	polarisation controller
PDBS	polarisation-dependent beam splitter
p-polarisation	polarisation in parallel direction w.r.t. plane of incidence
QI	quantum information
QWP, HWP	quarter-, half-wave plate
$\mathcal{R}$, $\mathcal{T}$	reflectance, transmittance
r, t	reflection and transmission amplitudes associated with A
R ($\|R\rangle$)	right-handed circular polarisation (state)
s-polarisation	polarisation in perpendicular direction w.r.t. plane of incidence
$\hat{\mathfrak{u}}$	unitary matrix
V ($\|V\rangle$)	vertical linear polarisation (state)
WP	wave plate
β-BaB$_2$O$_4$, β-BBO	β-barium borate (nonlinear crystal)
λ	wavelength of electromagnetic wave
ν	visibility (e.g., of interference pattern)
$\hat{\varrho}$	density matrix

Chapter 2 & Chater 3

$\mathbb{1}_4$ ($\mathbb{1}_8$)	4×4 (8×8) identity matrix
A and B	subsystems
C_{LHV}	upper threshold of $\mathcal{I}(\mathbf{P})$ for the local realistic description
$\mathcal{C}(\rho_2)$	two-qubit mixed state concurrence
$\mathcal{C}(\|\psi\rangle_2)$	concurrence for two-qubit pure state
$\mathcal{C}(\rho_2^{\mathrm{W}})$	Werner state concurrence
$\mathcal{C}_{\mathrm{GME}}$	genuine multipartite entanglement-concurrence
F	fidelity
$F(\rho_\theta^{\mathrm{expt}})$	fidelity of $\rho_\theta^{\mathrm{expt}}$ with respect to the ideal pure state $\|\theta\rangle_3$
gGHZ	generalised GHZ (state)
GHZ	Greenberger-Horne-Zeilinger state
GME	genuine multipartite entanglement
GWS	generalised Werner state
HMAC	hash-based message authentification code
I_{sec}	mutual information between the bank and the attacker
$I_{\max}$	maximum information to gain in given strategy
$\mathcal{I}(\mathbf{P})$	Bell inequality
$\mathcal{I}_{\min}$	strength of violation of randomly sampled measurements
$\mathcal{K}$	Kraus operator
MS	maximal slice states
$\hat{M}_{r_i\|S_i}$	positive operator-valued measure
P	probability of successful cloning of one input qubit
P_{c}	probability of obtaining correct information from the attack
P_{e}	probability of getting an erroneous result
$\mathbf{P} = \{P(\mathbf{r}_N\|\mathbf{S}_N)\}$	set of joint conditional probability distributions
$P(\rho)$	purity of the output state
p_{V}	nonlocal fraction
QM	quantum money
QRG	quantum retrieval games
RFI	reference-frame independent
$\|\psi\rangle_2$ ($\|\psi\rangle_3$)	two-(three-)qubit pure state
r_i	possible outcomes of measurement
S_i	measurement settings
SN	serial number
SPCC	symmetric phase-covariant cloning
T	tetrahedral states
v	visibility
$v_2^{\mathrm{cr}}(\theta) = 1/\beta_2$	critical visibility with the maximal violation of the CHSH inequality
v_θ	visibility associated with strength of the effective noise inherently present during the experiment
v_0	estimated visibility
v_c	parameter of controlled mixing
WS	Werner state
β_2	maximal violation of the CHSH inequality

β_3	maximal strength of Bell-nonlocality for three-qubit Werner-like states
Δ_2^{W}	difference between $\mathcal{C}(\rho_2^{\mathrm{W}})$ and $\mathcal{C}(\rho_2)$
Δ_3^{W}	difference between $\mathcal{C}_{\mathrm{GME}}(\theta_1)$ and $\mathcal{C}_{\mathrm{GME}}(\theta_2)$
ϵ	probability of an error being reported to the bank, i.e., error rate for all strategies
θ	an angle defining an arbitrary two-qubit pure state
$\|\theta\rangle_2$	arbitrary two-qubit pure state
$\|\theta\rangle_3$	gGHZ state
$\{\mu_{\mathbf{r}_N}^{\mathbf{S}_N}\}$	real coefficients
$\|\hat{\Pi}_1 \otimes \hat{\Pi}_2 \otimes \hat{\Pi}_3\rangle$	local projections
ρ_A	denotes the reduced density matrix of subsystem A
$\rho_2^{\mathrm{W}}(v)$ $(\rho_3^{\mathrm{W}}(v))$	two-(three-)qubit Werner state
ρ_2^{K}	two-qubit Kagalwala states
ρ_2^{MEMS}	two-qubit maximally entangled mixed states
ρ_2^{PhN} (ρ_3^{PhN})	two-(three-)qubit GHZ states subjected to the local phase-damping noise
$\rho_2(\theta, v)(\rho_3(\theta, v))$	two-(three-)qubit mixed state
ρ_2^{GSMS} (ρ_3^{GSMS})	two-(three-)qubit GHZ symmetric mixed state
ρ_3^{AD}	GHZ state subjected to the local amplitude-damping noise
$\rho_\theta^{\mathrm{expt}}$	output-state density matrix
σ^y	the Pauli matrix

Chapter 4

1A, 1B	vertical modes of photons forming state $\|\phi^+\rangle$
2A, 2B	horizontal modes of photons forming state $\|\psi^+\rangle$
2MS (3MS)	two-(three-)measurement scenario
$\hat{\mathbb{1}}$	unitary matrix
BIV	Bell inequality violation
$B(\rho)$	Bell nonlocality measure
$\mathcal{B}$	Bell-CHSH operator
CC	classes of correlations (hierarchy)
$C(\rho)$	Wootters concurrence
GWS	generalised Werner states
I	single-qubit identity operator
LHS	local hidden state (model)
MEMs	maximally entangled mixed states
$\{M_{a\|x}\}, \{M_{b\|y}\}$	measurement set of Alice (Bob)
$N(\rho)$	negativity
POVMs	positive-operator-valued measures
p	mixing parameter
$p(ab\|xy)$	Bell local decomposition
$p_A(a\|x, \lambda)$, $p_B(b\|y, \lambda)$	local response distributions
p_{est}, q_{est}	best-fitting parameters

p'_N, p'_B, p'_{S_2}, p'_{S_3}	threshold values
p_S^{up} (p_S^{low})	tight upper (lower) bound on steering for the GWSs for a large number of measurements
QST	quantum state tomography
q	superposition coefficient
q_{opt}	optimal superposition parameter maximising the white-noise robustness
S	steerable weight
SDPs	semidefinite programs
S_n	steering weight in n-measurement scenario
S_2^{XY}	steerable weight for measurements X and Y
WS	Werner state
$\Delta_{ij}(q)$	difference between threshold values $p_i(q)$ and $p_f(q)$
ν	visibility
$\pi(\lambda)$	density of distribution of local hidden variable
ρ_{W}	Werner(-like) state
$\rho_{\mathrm{W}}^E(p)$	experimental Werner(-like) state
ρ_{GW}	general Werner state
$\rho_{\mathrm{GW}}^E(p;\, q)$	experimental general Werner state
ρ^Γ	partial transpose of ρ
σ_1, σ_2 and σ_3	Pauli matrices
$\sigma_{a\vert x}$	assemblage of Alice
$\sigma_{a\vert x}^{\mathrm{S}}$	steerable part of the assemblage of Alice
$\sigma_{a\vert x}^{\mathrm{US}}$	unsteerable part of the assemblage of Alice
σ_λ	local (hidden) quantum state of Bob
$\lvert\phi^+\rangle$	$= (\lvert 00\rangle + \lvert 11\rangle)/\sqrt{2}$; a Bell state
$\lvert\phi_q^+\rangle$	$= (\sqrt{q}\,\lvert 00\rangle + \sqrt{1-q}\,\lvert 11\rangle)/\sqrt{2}$; a general two-qubit pure state
$\lvert\psi^+\rangle$	$= (\lvert 01\rangle + \lvert 10\rangle)/\sqrt{2}$; a Bell state

Introduction

> “No one ever obliges us to know, Adso. We must, that is all, even if we comprehend imperfectly.”
> “Nikdo nás nenutí k tomu, abychom věděli, Adsone. Vědět se prostě musí, i za cenu, že všechno pochopíme špatně.”
>
> *Umberto Eco, Name of the Rose, Chapter Sixth Day Nona*

It is only appropriate to begin this Thesis with the quote reflecting a genuine desire of a lonesome individual to unravel tangled state of affairs. So much has, in my view, a physicist or generally a scientist in common with the main character of the above mentioned novel, a curious detective, struggling to gain knowledge no matter the cost. Such desire is probably inherent to all humans to a certain extend, yet some have been endowed more than others. The history of physics has been written by many such individuals whose curiosity incited them to shed light onto basic principles governing the Universe. As for the field of quantum physics, some of these physicists will be mentioned. Indeed, the great riches of principles of physics provide more than enough room to satisfy one’s desire for discovering.

Quantum Physics

Quantum physics was established more than 100 years ago which makes it a well-proven and recognised field of physics. It was mainly the incapability of classical physics to satisfactorily describe several phenomena that emerged at the end of the 19th century leading to the gradual development of quantum physics [1, 2]. These peculiar phenomena include, for example, black body radiation [3], photoelectric effect [4] or explanation of atom’s stability [1, 5–7].

In the first case mentioned, the issue was to describe spectrum of radiation of the black body which one can imagine as a cavity absorbing all incident radiation and emitting only radiation due to its temperature [8, 9]. Several scientists aimed to explain it like J. Stephan [10], L. E. Boltzmann [11], J. W. S. Rayleigh [12, 13] and J. H. Jeans [14, 15]. Their findings, although based on well-established laws of statistical physics, did not correspond with the experimental data in the whole range of the electromagnetic spectrum [3]. It was only M. Planck who first derived a law fully describing the observations [16]. He used, as he thought himself, a mathematical construct without any physical significance: light (or generally radiation) is emitted in quanta having energy $h\nu$, where h is a constant and ν stands for frequency of this radiation.

In the second case mentioned, i.e. the photoelectric effect, physicists observed, besides other, an unexpected feature [1]. When radiation of frequency ν is incident to a cathode in a vacuum tube resultant number of emitted electrons and, in effect, photoelectric current depends on radiation intensity I. This is fully in compliance with classical theory. There exists, however, a lower threshold frequency ν_{thr} under which radiation looses its ability to cause photoelectric current regardless of the impinging I. It has been established that ν_{thr} depends on material of the cathode.

A. Einstein, by using results of M. Planck, described the photoelectric effect suggesting that light is interacting with the metal cathode discretely via these energy quanta $h\nu$, later denoted as photons [17]. Thus, he basically suggested that light has apart from the wave nature also a quantum or corpuscular behaviour. Should there exist a corpuscle of light it ought to have assigned a momentum p. It was indeed proved by A. S. Compton in the year 1922 [18]. The connection between wavelength λ of a light wave and its p ($p = \frac{h}{\lambda}$) was suggested shortly after that by L. V. de Broglie [19]. It should be noted that interpretation of this relation allows to ascribe λ or wave-like nature to both particles with or without mass, say photon or electron.

In agreement with the concept of wave-like behaviour of quantum objects (i.e. both light and particles) Schrödinger put a link between object's position x and time t expressing its state by a wave function $\Psi(x,\, t)$. By solving the so-called Schrödinger equation[1] [20] which takes the very form of a wave equation one can obtain $\Psi(x,\, t)$. Born's statistical interpretation [21] of quantum physics enables retrieving probability of finding the quantum object in a certain interval of x and t as an integral of $|\Psi(x,\, t)|^2$ within that interval. It is, thus, possible, only to certain degree (or with limited probability), to learn object's position at given time. This approach is in sharp contrast with the classical (Newtonian) mechanics where one is always able to find exact position of a particle as a function of time $x(t)$. For more details on formulation of quantum theory see [1, 22, 23].

Contemporary quantum theory seen by the mainstream physicists is based on a number of fundamental axioms. Various sources of literature present these axioms in slightly different forms [24–30]. For the purpose of this Thesis let us focus on those that are of particular relevance for the presented research: principle of superposition and probabilistic measurement. One of the consequences of these axioms is quantum entanglement.

The principle of superposition states that if Ψ_1 or Ψ_2 are valid quantum states then also expression $\alpha\Psi_1 + \beta\Psi_2$ represents a valid state given complex coefficients α and β are normalised ($|\alpha|^2 + |\beta|^2 = 1$). Nice example of the superposition principle is the famous thought (aka gedenken) experiment by Schrödinger involving an imaginary cat [31] (schematically illustrated in Figure 1). A cat is closed in a box containing an ampoule with poison that can be released by a random process (for instance, when fission of radioactive isotope occurs). Within a certain period of time, the cat can be either alive (in the state Ψ_{alive}) or dead (in the state Ψ_{dead}). However, one cannot know the state of the cat until one opens the box and take a look. Should the laws of quantum mechanics apply to cats then before one opens the box, the cat could be also in the superposition state $\alpha\Psi_{\mathrm{alive}} + \beta\Psi_{\mathrm{dead}}$. Since it is seemingly a nonsense this thought experiment is referred to as Schrödinger cat paradox. Accentuating obvious absurdity (at the time of paradox's formulation) of application of quantum-physical laws to macroscopic world, this thought experiment eventually stresses the crucial (but for the cat fatal) role of measurement. Until the box is opened and a visual measurement is done the cat is not in any classically acceptable state: dead, or alive but is rather in

[1] Equation in its time dependent form: $i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar}{2m}\frac{\partial^2\Psi}{\partial x^2} + \hat{V}\Psi$, where $\hat{V}$ is a potential energy operator of the given system (in general a function of t and x) and m is a mass.

both states simultaneously. It should be stressed out that over the course of the 20th century quantum nature of macroscopic objects has been demonstrated [32–35].

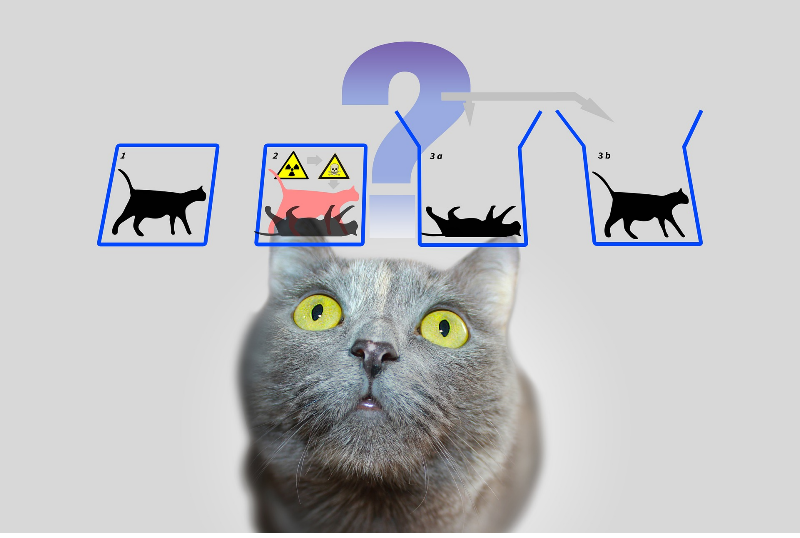


Figure 1: Schrödinger cat paradox. Visualisation of possible scenarios of the thought experiment. In the two inset figures to the left, a cat is in the closed box. Before the box is opened it is in the superposition state. Only after the box is opened and one takes a look, which is denoted by two inset figures to the right, the cat's wavefunction collapses and takes up a classical state, dead or alive. Image by Gerd Altmann [36].

Probabilistic measurement. In the formalism of quantum mechanics [22–25] quantum states are denoted as $|\cdot\rangle$, where this symbol is read as "ket" and stands for a vector in Hilbert space[2]. Likewise, symbol named "bra" $\langle\cdot|$ is a hermitian adjoint or conjugate, i.e. transposed and complex conjugate, of respective ket vector. Vectors bra and ket, respectively, form an inner product $\langle\cdot|\cdot\rangle$. Employing this notation, superposition state of a quantum system may be rewritten as $|\Psi\rangle = \alpha\,|\Psi_1\rangle + \beta\,|\Psi_2\rangle$. It should be noted that $|\alpha|^2$ and $|\beta|^2$ characterise probability p_i, $i \in \{1,\ 2\}$, of finding the system in state $|\Psi_1\rangle$ and $|\Psi_2\rangle$, respectively. Formally, the procedure is accomplished by means of inner product. It is only logical because in analogy with classical physics the relation (geometrically equivalent to the angle) between two vectors may be characterised by the measure of mutual overlap between projection of one vector onto the direction of the other vector. In terms of quantum mechanics, the probability p_1 of finding upon measurement the photon in state $|\Psi_1\rangle$ is understood as such "measure of mutual overlap" between $|\Psi_1\rangle$ and $|\Psi\rangle$ squared: $p_1 = |\langle\Psi_1|\Psi\rangle|^2 = |\alpha|^2$ assuming for simplicity that states $|\Psi_1\rangle$ and $|\Psi_2\rangle$ form mutually orthogonal basis and their inner product is, thus, zero. Although the probability p_i can be simply calculated for the known state $|\Psi\rangle$, the outcome of an individual projection of $|\Psi\rangle$ in the $\{|\Psi_1\rangle\,,\,|\Psi_2\rangle\}$ basis is random. Upon such measurement, $|\Psi\rangle$ collapses onto one of the states $|\Psi_1\rangle$, or $|\Psi_2\rangle$. Within the framework of this formalism such collapse may be described in terms of a projection operator $\hat{\Pi}_i = |\Psi_i\rangle\,\langle\Psi_i|$ applied to the state $|\Psi\rangle$, where i indexes the actual outcome from the set of all possible measurement results.

Entanglement. By far entanglement is among the most striking features of quantum mechanics mainly because it contradicts human intuition which is naturally based on

[2] It is a mathematical or algebraic vector space with inner product. Simply put, its properties are convenient for quantum mechanical description.

classical physics. For now it is enough to say that certain states show correlations or statistical dependencies that cannot be explained by a classical theory. Entanglement will be described in more detail in Section 1.1 and in affect throughout the whole doctoral Thesis.

In the course of more than 100 years of development, quantum theory started influencing and improving understanding of other fields of physics or science in general. Those fields include: nanotechnology, condensed matter [37], computing, cryptography [38, 39, A1], standard model of particle physics, field theory [40], electrodynamics [40] and even chemistry [41], mentioning just a few. Specific effects unknown before like quantum teleportation [42] or superfluidity [43] have been achieved in the field of quantum physics. This makes quantum mechanics an indispensable tool in physics with great potential which is worth studying. It also helps understanding the underlying nature behind classical phenomena and is an imperative for further advancement of science in general.

Basics of Quantum Information

Principle of superposition is undoubtedly an essence of quantum information[3] [44, 45]. Formulation of quantum physics and feasibility of experimental demonstration of it's conclusions led to an abrupt advancement of quantum information (QI) sciences. Quantum computing is nowadays accessible even to general public via quantum computer and simulator run by IBM quantum experience project [46]. Development of quantum computers goes naturally hand in hand with implementation of quantum programming languages such as Qiskit [47], quantum algorithms such as well-know Shor's [48–50] or Grove's algorithm [30, 51] and remarkably quantum machine learning [52, 53, A2]. Furthermore, quantum cryptography [54] is already commercially available [55–57] thanks to the preceding research discovering many QI protocols such as BB84 [58], six-state protocol [59], Eckert protocol [60], etc. This, however, triggered discussion on an issue of security of quantum communication. While quantum mechanics intrinsically possesses means to guarantee safety, its specific implementation vulnerabilities can be exploited. One such successful attack is discussed in Chapter 2. Attention is also paid to the implementation of quantum memories to enhance quantum communications networks [61–63] in order to push quantum technologies closer to practical everyday usage.

A unit of quantum information is the quantum bit or often abbreviated *qubit* or qbit. Before explaining the term qubit it will be fitting to summarise what a classical bit is. Bit is a basic unit of classical information. It is represented by binary digits, 0 and 1. In electronic devices, in order to perform logic operations, bit is represented for instance by two levels of voltage or current. In other words, physical systems carrying the information are electrons in electric current and the physical quantity expressing binary digit is the macroscopic voltage or current. For instance, in TTL logics, widely used in integration circuits, lower voltage up to 0.8 V corresponds to logical 0 and higher voltage above 2 V to logical 1.

In contrast to its classical counterpart, qubit can take superposition states of the form $\alpha\,|0\rangle + \beta\,|1\rangle$. Resembling a classical bit, qubit is also a two-level quantum object, having levels labelled 0 and 1 or in Dirac notation $|0\rangle$ and $|1\rangle$. These mutually orthogonal

[3] Since superposition is the phenomenon laying behind parallelism of quantum computer which is the core of supremacy of quantum computer.

states, i.e. $\langle i|j\rangle = \delta_{ij}$ for $i,\ j \in \{0,\ 1\}$, are called computational basis or logical basis states. Qubit can be encoded into any physical system capable of supporting mutually distinguishable states and their coherent superposition. Discrete photons are particularly suitable candidates for quantum computing. Encoding of qubits into polarisation and spatial modes is explained bellow in Section 1.5. Interestingly, a single qubit can hold more than 1 bit of information, theoretically even infinite amount of classical information. Unfortunately, one can only extract a single bit of classical information when subjecting a qubit to a projection measurement.

Recent years witnessed striking development of quantum technologies. Remarkably, People's Republic of China included quantum communication tasks into their 14. five-year plan [64]. Namely, they set an ambitious goal to develop an advanced multipurpose quantum computer consisting of hundreds of interconnected qubits suitable for various quantum communication tasks. However, big companies such as Google LLC or IBM do not fall behind with innovations and plans. For instance, Google implements a quantum processor Sycamore based on superconducting qubits. Moreover, it is not just a scientific gadget but is even capable to perform practical scientific simulations [65, 66]. This processor along with Chinese quantum computer Jiuzhang features so-called quantum supremacy [67–69]. It means that quantum computer exceeds capabilities of a classical supercomputer and performs a given task within considerably shorter time than its classical counterpart. IBM company as mentioned at the beginning of this Section provides a unique opportunity on commercial and educational basis to implement own quantum tasks. For this purpose it employs more than 20 quantum processors [46]. The company, however, strives to provide it's users with more than a 1 000-qubit computer [70, 71] by the year 2023.

Quantum transmission of information is most likely the future of secure communications. As a proof-of-principle several long-distance transmissions has been carried out [72–75]. To support this highly promising emerging field, China along with the USA has concentrated on development of satellites suitable for quantum communications [64]. In addition to that, a new satellite by ESA, whose objective is performing quantum information tasks for both commercial and governmental use, should be launched this year [76, 77]. Despite tremendous resources and earnest endeavour has been already invested, still a lot of effort will be necessary to devote to make quantum technologies part of an everyday life.

Outline

The main objective of this Thesis is presentation of three quantum-optics experiments. These experiments, performed in the Joint Laboratory of Optics of UP Olomouc[4] and Institute of Physics of the Czech Academy of Sciences, will be discussed in subsequent chapters. Theoretical background was provided by colleagues either from Faculty of Physics of Adam Mickiewicz University in Poznań, Poland or Faculty of Physics and Astronomy of University of Wrocław, Poland.

Methods and equipment used to carry out the experiments are presented in Chapter 1 of this Thesis. This Chapter includes all stages of photon's life, from its origin to its detection including analysis methods. Part of the text is devoted to introducing terms of quantum entanglement and nonlocality. Chapters 2-4 then describe the specific experimental tasks.

[4] Joint Laboratory of Optics of Palacký University in Olomouc and Institute of Physics of Czech Academy of Sciences, 17. listopadu 50A, 771 46 Olomouc, Czech Republic

Appendices A-C contain supplementary material belonging to Author's publications discussed within this Thesis. The Appendix D includes co-authors' statements regarding contribution of the Author to the research. Finally, the Appendix E comprises a list of contents of the CD-ROM attached to the printed version of this Thesis.

Experimentally Attacking Quantum Money Schemes Based on Quantum Retrieval Games

Based on Author's publication *Kateřina Jiráková, Karol Bartkiewicz, Antonín Černoch,* and *Karel Lemr*, *Sci. Rep.* **9**, 16318 (2019) [A1][5].

Topic of quantum money and their unnoticed counterfeiting is covered in Chapter 2. We witness rapid advancement of quantum technologies, therefore, it is only a matter of time before quantum money are used in practical payments. Advantages of quantum money (QM) have been recognised even in the late 1970s by S. Wiesner [38]. The most interesting feature of QM is that perfect counterfeiting is intrinsically impossible since quantum cloning forming irreplaceable part of forging procedure cannot be done flawlessly on an unknown state. Verification of QM was in original Wiesner's scheme accomplished in the issuing bank. However, such solution required establishment of quantum channel between users. This setback has been overcome by M. Bozzio *et al.* [78] who made use of classical verification of QM instead of utilising quantum channel, and the procedure of quantum retrieval game (QRG). Although, the authors claimed impossibility of successful attacking of their scheme, the experiment in Chapter 2 shows vulnerability of QM protocols based on QRG.

Measuring Concurrence in Qubit Werner States without an Aligned Reference Frame

Based on Author's publication *Kateřina Jiráková, Artur Barasiński, Antonín Černoch, Karel Lemr,* and *Jan Soubusta*, Phys. Rev. Applied **16**, 054042 (2021) [A3].

Alice lives on Venus, Bob lives on Mars... The biggest problem in their communication is to establish a common reference frame, so that they can use quantum cryptography for their secret letters (Figure 2). To help them, this study proposes a method for entanglement quantification that does not rely on synchronized reference frames. Counterintuitively, measurements in random and unknown bases can be used to establish just how entangled a quantum state is. This strategy may prove useful in complex quantum communication networks, where establishing a common reference frame (measurement basis) is impractical or impossible.

The genuine concurrence is a standard quantifier of multipartite entanglement, detection, and quantification of which still remains a difficult problem from both the theoretical and experimental points of view. Although many efforts have been devoted to the detection of multipartite entanglement (e.g., using entanglement witnesses), measuring the degree of multipartite entanglement, in general, requires some knowledge about the exact shape of a density matrix of the quantum state. An experimental reconstruction of such a density matrix can be done by full state tomography, which amounts to have the distant parties share a common reference frame and well-calibrated

[5] Publications of the Author are marked in the form [A No.] to clearly differentiate them in the text.

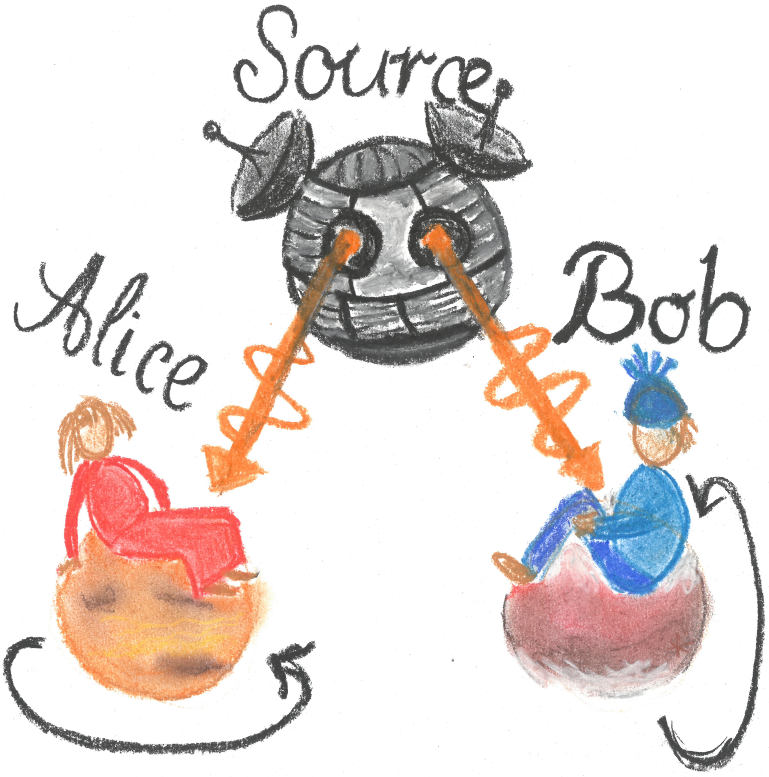


Figure 2: The Author's drawing featured on the Physical Review Applied website on the occasion of Ref. [A3] being published.

devices. Although this assumption is typically made implicitly in theoretical works, establishing a common reference frame, as well as aligning and calibrating measurement devices in experimental situations, are never trivial tasks. It is therefore an interesting and important question whether the requirements of having a shared reference frame and calibrated devices can be relaxed. In Chapter 3, we study both theoretically and experimentally the genuine concurrence for the generalised Greenberger-Horne-Zeilinger states under randomly chosen measurements on individual qubits without a shared frame of reference and calibrated devices. We present the relation between genuine concurrence and the so-called nonlocal volume, a recently introduced indicator of nonlocality.

Experimental Hierarchy and Optimal Robustness of Quantum Correlations of Two-Qubit States with Controllable White Noise

Based on Author's publication *Kateřina Jiráková, Antonín Černoch, Karel Lemr, Karol Bartkiewicz,* and *Adam Miranowicz*, Phys. Rev. A **104**, 062436 (2021) [A4].

Main objective of Chapter 4 is to demonstrate a hierarchy of various classes of quantum correlations on experimentally prepared two-qubit Werner-like states with controllable white noise. Werner states, which are white-noise-affected Bell states, are prototypal examples for studying such a hierarchy as a function of the amount of white noise. We experimentally generated Werner states and their generalisations, i.e., partially entangled pure states affected by white noise. These states enabled us to study the hierarchy of the following classes of correlations: separability, entanglement, steering in three- and two-measurement scenarios, and Bell nonlocality. We show that the generalised Werner states (GWSs) reveal fundamentally new aspects of the hierarchy compared to the Werner states. In particular, we find five different parameter regimes of the GWSs, including those steerable in a two-measurement scenario but not violating Bell inequalities. This regime cannot be observed for the usual Werner states. Moreover, we find threshold curves separating different regimes of the quantum correlations and find the optimal states which allow for the largest amount of white noise which does not destroy their specific quantum correlations (e.g., unsteerable entanglement). Thus, we could identify the optimal Bell-non-diagonal GWSs which are, for this specific meaning, more robust against white noise compared to the Bell-diagonal GWSs (i.e., Werner states).

The Author also participated in implementation of an all-optical setup demonstrating kernel-based quantum machine learning for two-dimensional classification problems. In this hybrid approach, kernel evaluations are outsourced to projective measurements on suitably designed quantum states encoding the training data, while the model training is processed on a classical computer [A2]. Further, the Author took part in research dealing with machine-learned quantum gate driven by a classical control. The gate learned to achieve optimal cloning fidelity, allowed for this particular class of cloned states, in a reinforcement learning scenario having fidelity of the clones as reward [A5].

During her master studies, the Author collaborated on construction and testing of a Time-of-Flight detector which was later mounted on LHC in CERN [A6–A8]. Currently, the Author collaborates with historians of fine art. Topic of a bachelor thesis supervised by the Author covers application of classical neural networks in identification of colour pigments. The other publication [A9] of the Author is listed in Chapter Author's publications as well.

Chapter 1

Experimental Equipment, Methods and Techniques

1.1 Quantum Entanglement and Nonlocality

Quantum entanglement plays a prominent role within the field of quantum physics and has constantly drawn physicists' attention. Since 1935, when it was firstly considered by A. Einstein, B. Podolsky, N. Rosen [79] and E. Schrödinger [80], until now, entanglement has been diligently studied [45]. The reason for such an endeavour is that entanglement has found its application in fields of practical importance such as quantum computing, communications and metrology [81]. In addition to that, phenomenon of entanglement is interesting also from the theoretical point of view.

To consider entanglement, imagine a quantum system containing two distinct subsystems[1], say two particles, $\mathscr{A}$ and $\mathscr{B}$. Each of the two particles can take the state $|0\rangle$ and $|1\rangle$[2]. In other words, state of the particle $\mathscr{A}$ ($\mathscr{B}$), denoted as $|\Psi\rangle_{\mathscr{A}}$ ($|\Psi\rangle_{\mathscr{B}}$), can be $|0\rangle_{\mathscr{A}}$ or $|1\rangle_{\mathscr{A}}$ ($|0\rangle_{\mathscr{B}}$ or $|1\rangle_{\mathscr{B}}$). Each of these states span a 2-dimensional Hilbert space $\mathscr{H}^{(2)}$, where the index $^{(2)}$ denotes the dimension of Hilbert space. Evidently, both particles can be in $|0\rangle$ state yielding the state of the entire system $|0\rangle_{\mathscr{A}} \otimes |0\rangle_{\mathscr{B}}$ or simply $|00\rangle$ spanning $\mathscr{H}^{(4)}$, where the symbol $\otimes$ denotes tensor or Kronecker product. On the other hand, nothing prevents the particles from being in the state $|1\rangle$ in which case the whole state becomes $|11\rangle$. All together, states of the set $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ form an orthogonal basis of the whole system.

According to the principle of superposition, mentioned in the Introduction, the whole quantum system can be prepared as a balanced superposition of these two constituent states

$$|\Psi\rangle_{\mathscr{A}\mathscr{B}} = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) . \tag{1.1}$$

Such state, despite being physically realisable, *cannot* be expressed as a tensor product of its subsystems, i.e. $|\Psi\rangle_{\mathscr{A}\mathscr{B}} \neq |\Psi\rangle_{\mathscr{A}} \otimes |\Psi\rangle_{\mathscr{B}}$ and is, therefore, called entangled. In other words, one cannot describe the state of the individual subsystems separately. Taken from the experimental point of view, this inseparability causes that any time the state $|0\rangle_{\mathscr{A}}$ is measured on subsystem $\mathscr{A}$ then the subsystem $\mathscr{B}$ is always found in the state $|0\rangle_{\mathscr{B}}$. Interchangeably, this is valid for $|1\rangle_{\mathscr{A}}$ and $|1\rangle_{\mathscr{B}}$. One never measures remaining two options where each particle takes a different state. Expressed mathematically, the probabilities of measurement of both states $|00\rangle$ and $|11\rangle$ is $|\langle 00|\Psi\rangle_{\mathscr{A}\mathscr{B}}|^2 = |\langle 11|\Psi\rangle_{\mathscr{A}\mathscr{B}}|^2 = \frac{1}{2}$. Whereas for the remaining two states, $|01\rangle$ and $|10\rangle$, is this probability zero. Such

[1] Entanglement can be also defined for multipartite system containing more than 2 subsystems.

[2] For instance, states $|0\rangle$ and $|1\rangle$ may be represented as vectors $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, respectively.

correlations can be, though, characteristic even for a classical system and comes, thus, as no surprise.

Physical systems featuring entangled state (as in Equation (1.1)) are for instance π-meson decay [22] into an electron and a positron ($\pi^0 \to e^- + e^+$) where, due to the conservation of angular momentum, each of these particles e^- and e^+ has opposite orientation of spin or a process of spontaneous Type-I parametric down-conversion [1, 82, 83] occurring in a non-linear crystal (more details on this process are provided in Section 1.3). The mere fact that certain state $|\Psi'\rangle_{\mathscr{AB}}$ can be factorised by states of the two subsystems, $|\Psi'\rangle_{\mathscr{AB}} = |\Psi\rangle_{\mathscr{A}} \otimes |\Psi\rangle_{\mathscr{B}}$, causes that such state is not entangled but separable.

To illustrate the unique effect of entanglement of the state $|\Psi\rangle_{\mathscr{AB}}$, diagonal basis, $|+\rangle \, / \, |-\rangle$, such that $|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right)$ and $|-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right)$ will be introduced. A simple substitution reveals that the entangled state in Equation (1.1) takes the form of

$$|\Psi\rangle_{\mathscr{AB}} = \frac{1}{\sqrt{2}} \left(|{+}{+}\rangle + |{-}{-}\rangle\right) . \tag{1.2}$$

Suppose two measurements on both subsystems' states, $|\Psi\rangle_{\mathscr{A}}$ and $|\Psi\rangle_{\mathscr{B}}$ are carried out in this basis $+/-$. The probability of finding both $\mathscr{A}$ and $\mathscr{B}$ in the same state, either $|{+}{+}\rangle$ or $|{-}{-}\rangle$, $|\langle{+}{+}|\Psi\rangle_{\mathscr{AB}}|^2 = |\langle{-}{-}|\Psi\rangle_{\mathscr{AB}}|^2$, is again $\frac{1}{2}$. On the contrary, subsystems cannot be found in mutually opposite states ($|\langle{+}{-}|\Psi\rangle_{\mathscr{AB}}|^2 = 0$ and $|\langle{-}{+}|\Psi\rangle_{\mathscr{AB}}|^2 = 0$). This behaviour is a manifestation of stronger-than-classical correlations that cannot be explained by classical physics.

The question arises, how is this correlation transferred and by what means is it mediated? How does one particle "know" of the result measured on the other particle? Before the measurement is done particles occupy a superposition state. When a measurement takes place the two-particle state $|\Psi\rangle_{\mathscr{AB}}$ collapses into an eigenstate of the measurement appartus. Now, suppose that both particles are separated by a very long distance, for example light years away from each other, and measurements on them are done exactly in the same moment. Then the collapse of two-qubit state would have to propagate faster than light which seems to be incorrect since it contradicts theory of relativity [84]. It was generally accepted that no physical event can influence its surroundings more quickly then light can propagate not to break principle of causality, one of two statements of the so-called local realism. This concept was advocated by Einstein, Podolsky and Rosen (E., P. & R.) in a famous thought experiment which is drawing the same seeming paradox. Later it became also known under acronym EPR paradox.

E., P. & R. concluded, among other things, that quantum mechanics does not seem to describe reality completely. They believed that all properties of any system are well-defined independently on whether they are measured or not [85]–the second assumption of local realism. The apparent randomness of measurement outcomes is according to E., P. & R. caused by our mere deficiency of understanding of physical systems. Advocates of local realism proposed that this insufficient knowledge can be modelled in terms of an unknown (hidden) variable Λ, inaccessible for us, which is influencing behaviour of the state. Existence of such variable is referred to as local hidden variable theory (LHVT).

Later, in 1964, J. S. Bell [86] theoretically derived inequalities and also predicted their violation in accordance to laws of quantum mechanics. If such violation were experimentally achieved, it would disprove the description by local hidden variable theory and, in affect, would indicate whether quantum mechanics describes reality completely. Group of physicists J. Clauser, M. Horne, A. Shimony, and R. Holt (often abbreviated as CHSH) proposed in 1969 a more general CHSH inequalities [87] that could be more feasibly experimentally implemented than the original Bell's inequalities. It was not until 1981 that A. Aspect, P. Grangier and G. Roger experimentally broke the inequalities proving that existence of hidden variable model is incompatible with quantum mechanics and that quantum entanglement is a real phenomenon [88, 89]. Since then Bell inequalities are a subject of testing in various setups, quantum systems and using more accurate and modern equipment. All experiments are in favour of quantum-mechanical description of the Universe and contradict the LHVT [90–94].

To illustrate the contrast between quantum theory and LHVT, let us consider a simple model. Two experimentalists in two separate laboratories, Alice and Bob, share a bipartite quantum state. Alice and Bob chose to perform one of two mutually orthogonal projection measurements, denoted A and B, on their part of the state independently on one another. Each measurement outcome for A and B, respectively, can take two values a, $b \in \{0,1\}$. After many measurements have been performed, a resulting statistics is revealed being described by a set of joint probabilities $\mathbf{P} = \{P(ab|AB)\}$, where $P(ab|AB)$ means probability that Alice obtains upon measurement A result a and similarly Bob after measuring B gets b. LHVT suggests that the result of a measurement is not given merely on random but is rather governed by a probability distribution of hidden variable $q(\Lambda)$ such that the joint probability is in the form

$$P(ab|AB) = \sum_{\Lambda} q(\Lambda) P_{\Lambda}(a|A) P_{\Lambda}(b|B) \ . \tag{1.3}$$

Naturally, $q(\Lambda)$ is non-negative and normalisable, $\sum_{\Lambda} q(\Lambda) = 1$. When the joined probabilities $P(ab|AB)$ obtained from experimental observations cannot be described in the form of Equatin (1.3) then these observations cannot be explained by any LHVT and, thus, break local realism. Whenever the respective joint probabilities of parties are not factorisable in manner of the above equation, they are called nonlocal [95, 96]. Usual way how to detect nonlocality is to test Bell's (or various Bell-type, e.g. Svetlichny [97], CHSH, etc.) inequalities. For instance, CHSH inequality [87] is defined as

$$\mathrm{CHSH} = P(00|AB) - P(01|AB) + P(10|AB) + P(11|AB) \ . \tag{1.4}$$

When gathering the measurement statistics of CHSH factor, only events when detectors of both Alice and Bob clicked, so-called coincident counts (detections) denoted CC, are considered. Joint probabilities are expressed in terms of these coincidence counts as $P(ab|AB) = \frac{CC_{ab}}{\sum_{i,j=0}^{1} CC_{ij}}$. It can be shown that for an example such as this one can always find LHV model if and only if $|\mathrm{CHSH}| \leq 2$. Quantum mechanics, on the contrary, allows for $|\mathrm{CHSH}| \leq 2\sqrt{2}$. The states with CHSH factor $2 < |\mathrm{CHSH}|$ do not meet the local realism assumptions and are referred to as nonlocal.

All separable states (not entangled) can obviously produce joint probabilities expressed in the form of Equation (1.3). It, thus, follows that in order to violate CHSH inequalities the investigated quantum state must be entangled (nonlocality implies entanglement). The opposite is, however, not always true [98]. There are states that cannot indeed be expressed as separable but the measurement results do not exclude the LHVT interpretation. Besides entanglement and nonlocality, there are other criteria of states describing properties inaccessible to classical physics. They constitute an open area of research like those considered in Chapter 4. Similarly, one can generalise all these criteria to multipartite quantum state and formulate conclusions such as those experimentally studied in Chapter 3.

1.2 Linear-Optical Elements

Goal of this Section is to introduce the reader to optical elements commonly used on the platform of linear optics to implement quantum experiments and tasks. In order to understand operation of more complex experimental setups, the following Section presents the main parts these setups consist of, i.e. (polarising) beam splitters, wave plates and beam displacers. Their action on photonic states will be mathematically expressed. Even though, the considered components were used originally for purposes of classical wave optics, transformations these components impose on the annihilation operators (explained in Section 1.2.1) of individual modes are fairly similar.

Apart from these components there are also opto-mechanical parts playing an important role. They hold (post holders), rotate and tilt (rotation stages), and move (translation and piezo motorised stage) the optical components. Since photons do not directly interact with those auxiliary parts, they will not be described here.

Extensive theory of optical fibres is also omitted here because they are considered only as much as a tool description of which does not directly relate to the topic of this Thesis. It is sufficient to mention that within presented experiments, single-mode (SM 600) or multi-mode fibres by Thorlabs Inc. were used. Both the fibre core and cladding are manufactured of fused silica glass (SiO_2) with typical value of refractive index being around 1.45. Single-mode fibres are much less prone to collect noise with respect to multi-mode fibres because their geometry, namely smaller so-called acceptance angle, complicates coupling of light into them. Another advantage is that the distribution of intensity of light guided by this fibre corresponds to the fundamental mode LP_{01} (TEM_{00}) with only one intensity maximum so higher spatial modes are cut off. Which is particularly important for perfect interference of two beams.

1.2.1 Beam Splitters

Principle of beam splitter (BS) or beamsplitter lies in partial reflection and transmission of incident light. It is compactly manufactured in the form of a glass plate or a prism features of which are obtained by depositing a thin film on its surface. Beam splitters are inseparable components of interferometers like (Mach-Zehnder, Sagnac, Michalson, etc.) because they allow splitting and subsequent rejoining of incident light beams. Alternatively BS can be manufactured on platform of fibre optics by means of coupling of evanescent waves between 2 fibres. Such BSs may even have various splitting ratios like 49:51, 30:70, 10:90, etc. Effective splitting ratio, caused by polarisation dependent losses, is important for quantum cloning discussed further in Chapter 2.

If we neglect losses that each beam splitter intrinsically has, one can describe BS by it's intensity reflectance $\mathcal{R}$ and transmittance $\mathcal{T}$ in the way that $\mathcal{R} = 1 - \mathcal{T}$. In case when splitting ratio $\mathcal{T}/\mathcal{R}$ equals 1, the incident beam power with intensity I_{inc} is evenly split into two output beams. As amplitude of an electromagnetic wave (field) A is proportional to $\sqrt{I_{\mathrm{inc}}}$, its transformation by a BS can be expressed in matrix form:

$$\begin{pmatrix} A_{\mathrm{out}}^{(1)} \\ A_{\mathrm{out}}^{(2)} \end{pmatrix} = \underbrace{\begin{pmatrix} t & r' \\ -r & t' \end{pmatrix}}_{\hat{u}_{\mathrm{BS}}} \begin{pmatrix} A_{\mathrm{in}}^{(1)} \\ A_{\mathrm{in}}^{(2)} \end{pmatrix} , \tag{1.5}$$

with r and t being reflection and transmission amplitudes associated with A which can be conveyed as: $|r|^2 = \mathcal{R}$ and $|t|^2 = \mathcal{T}$. The prime denotes these functions for the second input port. From unitarity, as mentioned further, of a loss-less transformation it follows that $r = r'$ and $t = t'$.

Second quantisation [99, 100] of electromagnetic field postulates that amplitudes A are replaced by annihilation operators $\hat{a}$ resulting into quantum mechanical description

$$\begin{pmatrix} \hat{a}^{(1)}_{\text{out}} \\ \hat{a}^{(2)}_{\text{out}} \end{pmatrix} = \underbrace{\begin{pmatrix} t & r \\ -r & t \end{pmatrix}}_{\hat{\mathcal{U}}_{\text{BS}}} \begin{pmatrix} \hat{a}^{(1)}_{\text{in}} \\ \hat{a}^{(2)}_{\text{in}} \end{pmatrix} . \tag{1.6}$$

The terms r and t have to follow normalisation condition $|r|^2 + |t|^2 = 1$. The BS is considered lossless, therefore energy during the transformation has to be conserved. This requirement ensures unitarity of the transformation done by the BS, i.e. it has to follow $\hat{\mathcal{U}}^\dagger \hat{\mathcal{U}} = \hat{\mathbb{1}}$. For this reason, BS may be characterised by an effective parameter ϑ. Utilising the general form of unitary matrix, equation (1.6) can be rewritten as

$$\begin{pmatrix} \hat{a}^{(1)}_{\text{out}} \\ \hat{a}^{(2)}_{\text{out}} \end{pmatrix} = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix} \begin{pmatrix} \hat{a}^{(1)}_{\text{in}} \\ \hat{a}^{(2)}_{\text{in}} \end{pmatrix} , \tag{1.7}$$

where the minus sign is a consequence of a phase change that the light experiences while reflected from the BS [101].

The commonly used BSs have balanced splitting ratio, i.e. 50:50 or $\mathcal{R} = \mathcal{T} = \frac{1}{2}$, which allows for simplification of above unitary matrix $\hat{\mathcal{U}}$ in Equation (1.7). In order to achieve this, ϑ has to equal to $\frac{\pi}{4}$. Then, the unitary matrix for balanced BS is expressed as

$$\hat{\mathcal{U}}_{\text{BS}} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} . \tag{1.8}$$

For annihilation $\hat{a}$ and creation operator $\hat{a}^\dagger$ it follows from the algebra of quantum mechanics that $[\hat{a},\hat{a}^\dagger] = \hat{a}\hat{a}^\dagger - \hat{a}^\dagger\hat{a} = 1$. It turns out that electromagnetic field has formally the same Hamiltonian[3], $\hat{\mathcal{H}} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})$ with ω representing angular frequency [100] as linear harmonic oscillator. Electromagnetic field has also its eigenstates (also called Fock or number states) $|n\rangle$: $\hat{\mathcal{H}}|n\rangle = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})|n\rangle$, where $n = 1, 2, 3, ...$ stands for number of photons in the given mode. Annihilation and creation operators act on Fock states in the following way: $\hat{a}|0\rangle = 0$, $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$ and $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$. So, $\hat{a}$ decreases the number of photons by one whereas $\hat{a}^\dagger$ adds one photon, hence their names annihilation and creation operator, respectively. In other words, they denote absence or presence of a photon.

By use of this formalism, an effect of Hong-Ou-Mandel (HOM) interference [102] will be shown here. It is a quantum phenomenon involving bunching of photons on BS. It is further discussed from the experimental point of view in dedicated Section 1.4. HOM interference occurs when there is one photon at each input port, denoted as $1^{(1)}_{\text{in}}1^{(2)}_{\text{in}}$, in the same time interacting with the other one. Naturally, there are 4 possible solutions shown in Figure 1.1. Moreover, bearing in mind that vacuum state, $|\emptyset\rangle$, of all input modes needs to yield vacuum output in all modes, it is possible to summarise

[3] Hamiltonian is a function of energy of the system.

the equation as

$$\begin{aligned}
\left|1_{\text{in}}^{(1)}1_{\text{in}}^{(2)}\right\rangle &= \hat{a}_{\text{in}}^{\dagger(1)}\hat{a}_{\text{in}}^{\dagger(2)}\left|\emptyset,\emptyset\right\rangle \xrightarrow{BS:\,|\mathcal{T}|=|\mathcal{R}|} \frac{1}{2}\left(\hat{a}_{\text{out}}^{\dagger(1)}+\hat{a}_{\text{out}}^{\dagger(2)}\right)\left(\hat{a}_{\text{out}}^{\dagger(2)}-\hat{a}_{\text{out}}^{\dagger(1)}\right)\left|\emptyset,\emptyset\right\rangle && (1.9)\\
&= \frac{1}{2}\left[\left(\hat{a}_{\text{out}}^{\dagger(2)}\right)^2-\left(\hat{a}_{\text{out}}^{\dagger(1)}\right)^2\right]\left|\emptyset,\emptyset\right\rangle && (1.10)\\
&= \frac{1}{\sqrt{2}}\left(\left|2_{\text{out}}^{(2)},\emptyset^{(1)}\right\rangle-\left|\emptyset^{(2)},2_{\text{out}}^{(1)}\right\rangle\right)\ , && (1.11)
\end{aligned}$$

where we used unitarity of $\hat{\mathcal{U}}_{\text{BS}}$ and the Equation (1.8). Interestingly enough, cross terms of creation operators in Equation (1.9), $\hat{a}_{\text{out}}^{\dagger(1)}\hat{a}_{\text{out}}^{\dagger(2)}$, cancel out leaving only bunching terms none-zero (Equation (1.10)). Obviously, photons tend to gather together and leave always only by one output port. The output state in Equation (1.11) is entangled, namely spatially, and the entanglement is the strongest for balanced beam splitter ($|\mathcal{T}|=|\mathcal{R}|$).

By facilitating interactions between two spatial modes of light, the BS is a key component for implementation of a large number of quantum information experiments like teleportation [42], quantum logic gates (such as controlled NOT or controlled phase) [103–105], quantum cloning [106–110] discussed further in Chapter 2 and boson sampling [A2] which exploits scattering of identically prepared bosons, like for instance photons.

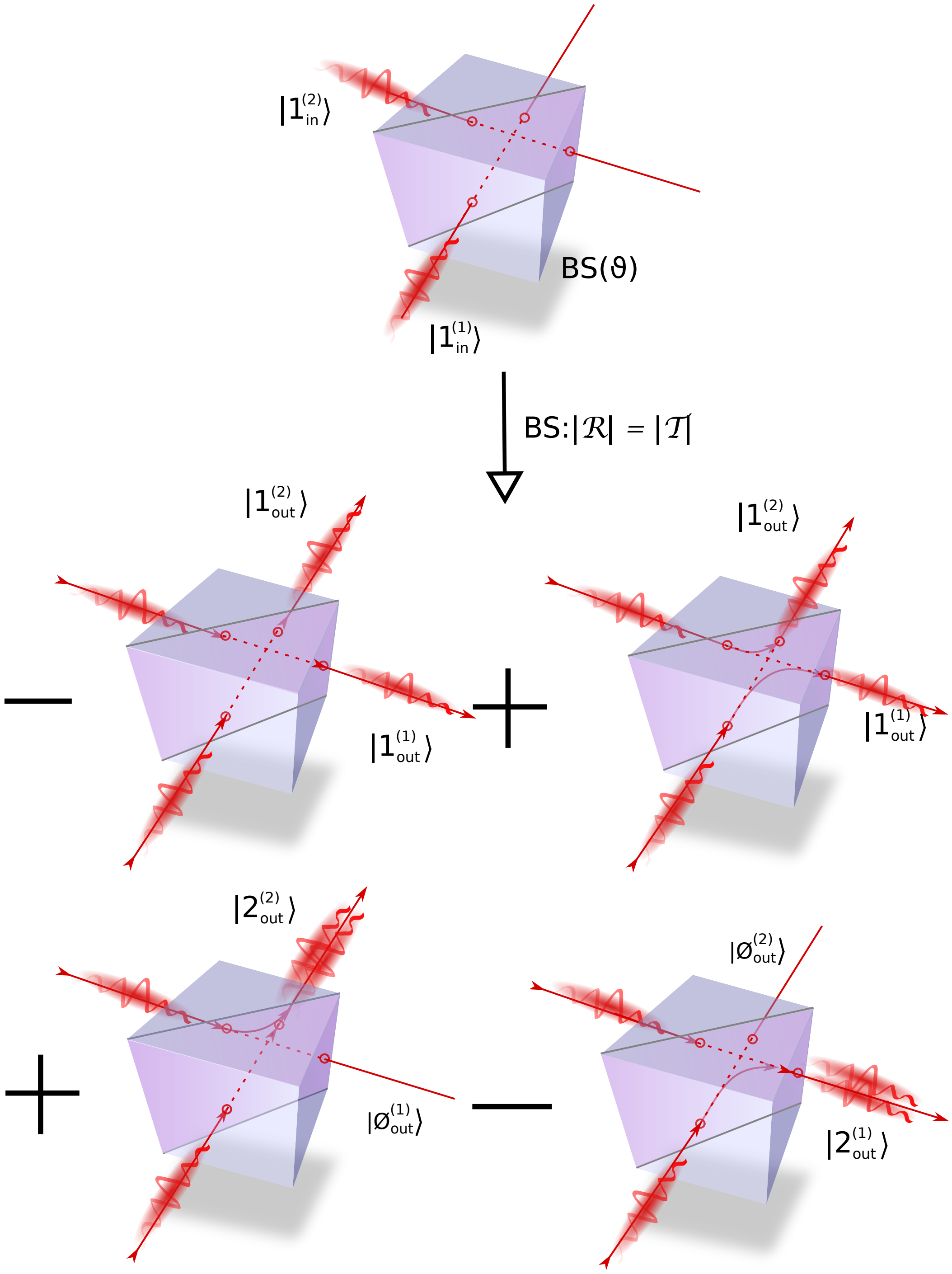

$|1_{\text{in}}^{(2)}\rangle$
BS(ϑ)
$|1_{\text{in}}^{(1)}\rangle$
BS:$|\mathcal{R}| = |\mathcal{T}|$
$|1_{\text{out}}^{(2)}\rangle$
$|1_{\text{out}}^{(2)}\rangle$
$-$
$|1_{\text{out}}^{(1)}\rangle$
$+$
$|1_{\text{out}}^{(1)}\rangle$
$|2_{\text{out}}^{(2)}\rangle$
$|\varnothing_{\text{out}}^{(2)}\rangle$
$+$
$|\varnothing_{\text{out}}^{(1)}\rangle$
$-$
$|2_{\text{out}}^{(1)}\rangle$

Figure 1.1: Visualisation of HOM interference at balanced BS as derived in Equations (1.9) – (1.11). Couple of cube BSs in the middle of the Figure denotes scenarios where either both photons are transmitted or reflected. However, because of opposite signs respective creation operators cancel out and these scenarious will not occur. The only possible scenarios are those where photon from one input port is transmitted and photon from the other input port is reflected (phenomenon of HOM interference). This situation is depicted as couple of BS in the bottom of the Figure.

1.2.2 Polarisation-Dependent Beam Splitters

A beam splitter introducing polarisation dependent splitting ratio will be called polarisation-dependent beam splitter (PDBS). Description of how PDBS acts on single photons may be derived from relations obtained for BS (in Equation (1.6)). It is only necessary to incorporate polarisation degree of freedom in addition to spatial modes $\hat{a}^{(1)}$ and $\hat{a}^{(2)}$. This effectively enlarges the transformation space from 2 to 4. The transformation relation then reads

$$\begin{pmatrix} \hat{a}^{(1),H}_{\text{out}} \\ \hat{a}^{(2),H}_{\text{out}} \\ \hat{a}^{(1),V}_{\text{out}} \\ \hat{a}^{(2),V}_{\text{out}} \end{pmatrix} = \underbrace{\begin{pmatrix} t_{\text{H}} & r_{\text{H}} & 0 & 0 \\ r_{\text{H}} & t_{\text{H}} & 0 & 0 \\ 0 & 0 & t_{\text{V}} & r_{\text{V}} \\ 0 & 0 & r_{\text{V}} & t_{\text{V}} \end{pmatrix}}_{\hat{u}_{\text{PDBS}}} \begin{pmatrix} \hat{a}^{(1),H}_{\text{in}} \\ \hat{a}^{(2),H}_{\text{in}} \\ \hat{a}^{(2),V}_{\text{in}} \\ \hat{a}^{(1),V}_{\text{in}} \end{pmatrix}, \tag{1.12}$$

where just for illustration, p-polarisation[4] was substituted by H and s-polarisation[5] by V. Further simplification is achieved when a fully polarising BS is considered. From the principle of its operation it is valid that $t_{\text{H}} = r_{\text{V}} = 1$ and $r_{\text{H}} = t_{\text{V}} = 0$. The unitary matrix has then the form of

$$\hat{u}_{\text{PBS}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

In its construction PDBS resembles BS just with the difference that deposited thin layer imparts various splitting ratios to differently polarised light. However, both polarisations are not allowed to interact in the basis in which the transformation (1.12) is prescribed [111].

Polarising beam splitter (PBS) or sometimes beam-splitting polariser is a special case of PDBS. It is used to split incident light beam separating it into two beams with perpendicular polarisations as depicted in Figure 1.2. These polarisation components are often denoted as s-polarisation and p-polarisation. Usual PBS transmits p-polarised light and reflects s-polarised one. This is achieved by several methods. One of them is a cube prism made out of two triangular prisms formed by dense flint glass cemented together[6]. Dielectric coating applied to the joint of the cube then mediates the beam separation (via interference [112, 113]).

There are other principles of operation of PBS, one of them employs so-called birefringent prisms. Among the most known types are those of Glan-family, Wollastone, Rochon or Nicol prisms [114] which are made of materials like quartz or calcite. When optical axis is appropriately orientated with respect to the incident beam, this beam is, as a result of birefringence, split into two beams. One of them is polarised along ordinary (o) direction (or axis) and the second one along extraordinary (e) direction. Light incident on such a crystal is decomposed into two mutually orthogonal polarisation

[4] from German word *parallel*, referring to polarisation laying in parallel direction to the plane of incidence

[5] from German word *senkrecht* referring to polarisation laying in perpendicular direction to the plane of incidence

[6] For technical specifications see directly the web side of the manufacturer: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=739

components. Similarly, as in the case of BS they find their application in quantum information tasks.

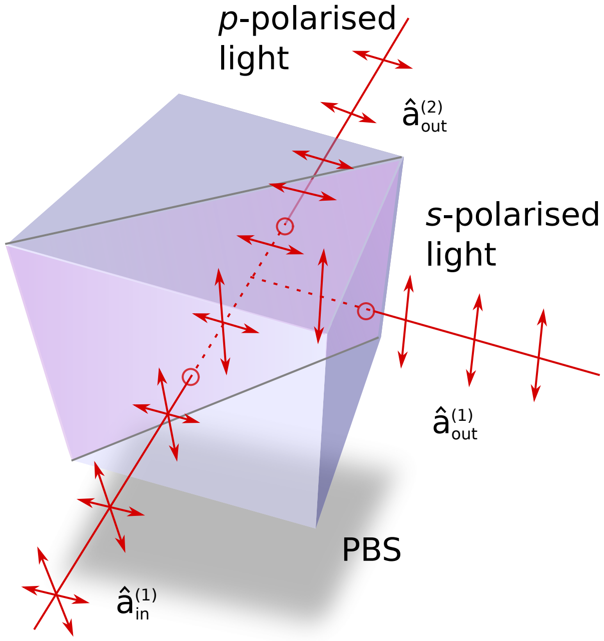

p-polarised light
$\hat{a}^{(2)}_{\text{out}}$
s-polarised light
$\hat{a}^{(1)}_{\text{out}}$
PBS
$\hat{a}^{(1)}_{\text{in}}$

Figure 1.2: Action of a polarising beam splitter. Incident beam is brought to the PBS by an input port (1) denoted by the index (in). The beam is then split into two perpendicularly polarised beams leaving PBS by two output ports (1) and (2). Polarisation of the reflected beam is perpendicular to the plane of incidence (not depicted in the Figure) which is given by incident beam and perpendicular to the boundary (visualised by a purple plane). Polarisation of the transmitted beam is on the other hand parallel to this plane.

1.2.3 Wave Plates

Polarisation state of light may be easily transformed by use of an optical component, a wave plate (WP), made of birefringent material. Two most notable examples are half-wave plate (HWP) and quarter-wave plate (QWP). WPs are made of uniaxial materials such as quartz or mica, where ordinary and extraordinary directions of electromagnetic field oscillations (polarisations) exist. This results in different refractive indices, n_o and n_e. Light incident on such a crystal is decomposed into two mutually orthogonal polarisation components with different phase velocities. Direction for which light experiences higher (lower) refractive index is called slow (fast) axis. Difference of velocities unavoidably imposes phase shift or retardation between both polarisations

$$\Delta\Gamma = \frac{2\pi\, d}{\lambda}\, |n_e - n_o| \ . \tag{1.13}$$

The crystal has to have carefully chosen width d to reach certain value of $\Delta\Gamma$. Specifically, for $\Delta\Gamma = \pi$ the crystal is called HWP and for $\Delta\Gamma = \frac{\pi}{2}$ it is QWP.

A transformation matrix of WP, $\hat{\mathcal{U}}_{\text{WP}}$, acting on a vector of annihilation operators mixes the respective modes in a similar manner as a BS works for spatial modes (Equation (1.6)) [115]. In general, the retardation (in Equation (1.13)) imposes a matrix unitary transformation in the basis of o- and e-directions. It is customary to rotate the WP which produces the following effect in the basis of laboratory H and V polarisations [113]: $\hat{\mathcal{U}}_{\text{WP}} = \mathbf{R}_{-\theta}\, \hat{\mathcal{U}}_{\text{WP}}(0)\, \mathbf{R}_{\theta}$, where θ is an angle between slow axis and the direction of H polarisation, rotation matrix $\mathbf{R}_\theta = \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right)$ and the transformation matrix of WP in non-rotated state reads [115]

$$\hat{\mathcal{U}}_{\mathrm{WP}}(0) = \begin{pmatrix} e^{-i\,\Delta\Gamma/2} & 0 \\ 0 & e^{i\,\Delta\Gamma/2} \end{pmatrix} .$$

Particular solutions for rotated HWP and QWP are:

$$\hat{\mathcal{U}}_{\mathrm{HWP}} = -i \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

and

$$\hat{\mathcal{U}}_{\mathrm{QWP}} = \tfrac{\sqrt{2}}{2} \begin{pmatrix} 1 - i\cos 2\theta & -i\sin 2\theta \\ -i\sin 2\theta & 1 + i\cos 2\theta \end{pmatrix} .$$

Rotated by an angle θ, the effect of the HWP is as follows: It rotates incident linear polarisation by an angle 2θ so output remains linearly polarised. Both HWP and QWP change the global phase. Moreover, QWP adds a phase between H and V polarised light. In other words, depending on the angle θ, it thus changes ellipticity.

Unitary nature of $\hat{\mathcal{U}}_{\mathrm{WP}}(\theta)$ causes that WP transforms a pure polarisation state into another pure one. It can be shown that transformation of any general polarisation state can be accomplished by a set of QWP, HWP and QWP [116]. Similarly, a couple of HWP and QWP is sufficient to produce any polarisation state from any linear polarisation state [117]. This quality was exploited for polarisation encoding and projections of qubits within experiments presented in this Thesis (namely projections are treated in the Section 1.6).

1.2.4 Beam Displacer and Beam Displacer Assembly

Beam displacer (BD) is somewhat similar in its function to BS. BDs are typically fabricated from birefringent material such as calcite or yttrium orthovanadate ($\mathrm{YVO_4}$) for applications at longer wavelengths. Prism like Rochon or Wollastone may be also considered as BDs. Unlike BS, however, the separated beams upon leaving the BD continue in the parallel direction with respect to the input beam. Typically, after exiting the BD both modes remain displaced by a constant length, for instance few[7] mm. As a result of so-called *walk-off* effect, this component separates incident light beam into o- and e-beam, each sensing different refractive index n_o and n_e (Figure 1.3). Specifically, o-beam travels through the crystal along the direction of the incident beam. On the other hand, e-beam has a different direction, dependent on an angle of crystal's optical axis and $\mathbf{k}$-vector of incident beam. Notably, both o- and e-beams are by the action of birefringent crystal mutually orthogonally polarised [113, 118, 119]. Within experiments presented in this Thesis, BDs can be mounted in such a way that horizontally polarised light continues straight whereas vertically polarised light is deviated.

Within the platform of linear optics, BDs are employed as BSs whenever the orthogonal separation of light beams is not desired. BDs were integral parts of setups discussed in Chapter 3 and formed an intermediate step towards construction of setup presented in Chapter 4.

BDs can also implement polarisation dependent losses and a phase shift between polarisation components by means of an interferometric device, referred to as beam

[7] for instance BD40 by Thorlabs Inc. provides 4 mm separation

displacer assembly (BDA) depicted in the Figure 1.3. The term polarisation dependent losses means a change of transmittance of a given polarisation state or mode. To introduce such losses, one might simply employ even a single piece or a couple of plane-parallel glass plates rotated close to Brewster's angle[8]. However, such method has a drawback that all polarisation modes are bound to undergo a change of transmittance. This issue is solved by the very BDA which by means of conversion of polarisation modes into two spatial modes allows to apply separately onto chosen mode some means of attenuation (like neutral density filter).

The working principle of BDA is as follows: the first BD separates the incident beam creating two beams as discussed earlier. In order to rejoin these two beams back together the polarisation states have to be interchanged. For this purpose the setup contains a HWP set at 45° that switches polarisation states of *o*- and *e*-beam. Only now the two beams are brought to the second BD which reunites the two spatial modes. However, complicated adjusting process and reflection losses on surfaces of crystals are among the drawbacks of this method.

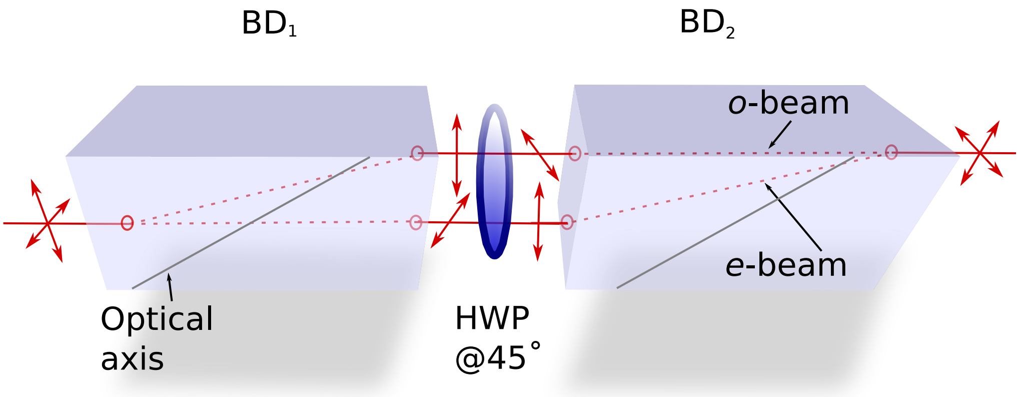


Figure 1.3: Visualisation of a beam displacer assembly. It consists of two BDs and a HWP. First BD separates incident light into *o*- and *e*-beam while the second BD, by virtue of HWP at 45° flipped the polarisation states, joins those two beams back together [118].

1.3 Source of Photon Pairs

In our experiments we used a laser system Paladin Nd:YAG by Coherent company with integrated third harmonic generation at $\lambda = 355\,\mathrm{nm}$. Its repetition rate is 120 MHz and mean power reaches 2 W which is further reduced to 215 mW. This beam is utilised to pump a pair of non-linear crystals β-BaB$_2$O$_4$ (β-barium borate which is often abbreviated as β-BBO). In both of these crystals, a photon pair is generated via phenomenon of spontaneous Type-I parametric down-conversion [1, 82, 83, 118]. With some probability a pump beam photon with angular frequency ω is transformed into two secondary photons of lower angular frequencies ω_1 and ω_2. It holds that $\omega = \omega_1 + \omega_2$ and for wave vectors $\mathbf{k} = \mathbf{k}_1 + \mathbf{k}_2$ (depicted in the upper part of Figure 1.4) so the energy and momentum are conserved in this process. Apart of fulfilment of the law of conservation, the secondary photon's direction $\mathbf{k}_i$ has no preferred space orientation and,

[8] For light wave incident on the boundary between two media each with refractive index n_1 and n_2, the value of Brewster's angle is expressed as $\theta_\mathrm{B} = \arctan \frac{n_2}{n_1}$. Then light transmitted through the medium is partially polarised whereas reflected wave is fully *s*-polarised. Controlling an angle of incidence provides an effective means to acquire polarised light from unpolarised one.

therefore, covers surface of a cone. Further to that, generated photons leave crystals in axially symmetric directions with respect to beam. Everywhere in this direction couplers may be positioned to collect these photons (visualised in the lower part of the Figure 1.4). It is worth stressing that if apex angles are small, for typical BBO crystal $3^\circ - 4^\circ$, the position of photons' origin is smeared and, thus, uncertain due to small size (orders of mm) of the BBO crystal. For this reason the down-converted photons from the 1st and 2nd crystal are indistinguishable.

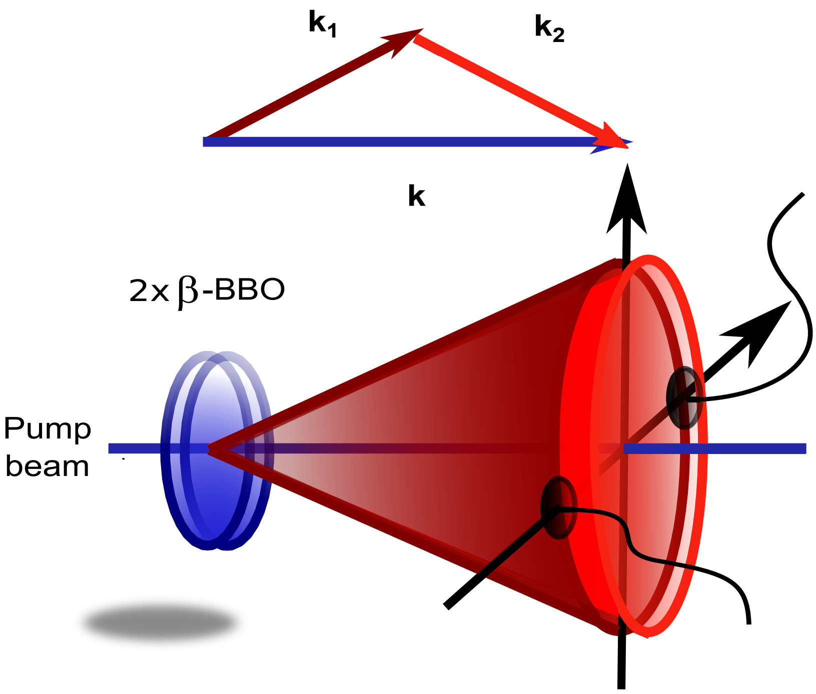


Figure 1.4: The process of Type-I spontaneous parametric down-conversion in a couple of nonlinear crystals β-BBO (Kwiat source). Down-converted photons from the 1st (2nd) crystal cover surface of a deep red (light red) cone centred around the pump beam (blue line). Photons collected in directions (an example of such ones marked by black ellipses) that fulfil the energy and momentum conservation law (visualised in the upper part of the Figure) are by virtue of small apex angle of these cones practically indistinguisable [1, 118].

In case of our source, the BBO crystals provides us with two output photons of equal angular frequencies at wavelength[9] $\lambda_{1,2} = 710$ nm ($= 2 \cdot 355$ nm). This process is interesting because created photons are correlated in polarisation, (angular) frequency (or energy) and in direction of their motion. For this reason it is widely used in quantum optical experiments.

The crystals are positioned so that their optical axes lay in mutually orthogonal plains. With respect to that, the 1st crystal produces H polarised photons when pumped by V polarised laser beam whereas the 2nd crystal produces V polarised photons when pumped by H polarised laser beam. Because of the pump beam coherence and indistinguishability of the photon coupling behind the crystals, we are able to generate a coherent superposition of photons from both the crystals. This technique is known as crystal cascade or a Kwiat source [120, 121]. The pump power together with geometrical and material properties of our crystals make simultaneous generation of multiple photon pairs negligible.

[9] The relation between angular frequency and wavelength is given by equation $\omega = \frac{2\pi c}{\lambda}$

In all experiments presented here we postselect solely on the cases when both photons were registered by the detectors. This procedure effectively eliminates situations when no photon pair was generated or at least one of the photons has not been detected. One can, thus, assume that the generated state takes the effective form

$$|\psi\rangle = \cos\theta \underbrace{|HH\rangle}_{\text{1st crystal}} + e^{i\varphi}\sin\theta \underbrace{|VV\rangle}_{\text{2nd crystal}} \quad , \tag{1.14}$$

where θ and φ are dependent on polarisation state of the pump beam. Specifically, the parameter θ is controlled by rotation of HWP inserted to pump beam before the crystals while the φ is controlled by pump beam ellipticity.

1.4 Hong-Ou-Mandel interference

Once the source is constructed its qualities have to be tested. We can verify indistinguishability and temporal coherence within separable state, e.g. $|HH\rangle$. Photons are governed by Bose-Einstein statistics that dictates photons in the same quantum state to gather together. So, in the case photons are genuinely indistinguishable, they bunch together at the BS and leave it together by the same output port, as demonstrated in Section 1.2.1. This special kind of two-photon interference is called Hong-Ou-Mandel (HOM) interference [102]. When the photons may be distinguished for some reason, they leave BS with some probability by two different ports. Therefore, HOM interference is feasibly detected in terms of coincidence detections or counts (CC), i.e. by means of electronic modules the events are counted when each photon of the pair was detected in different detector within a short time interval referred to as coincidence window. Typical width of this window is several ns which is much more than the spread in time of creation of both photons.

The measurement setup is depicted in Figure 1.5(a). Photons are entering the BS by input ports 1 and 2 and leaving it by ports 3 and 4. One arm of the interferometer has adjustable length which can be fine tuned by means of motorised translation stage coupler in order to scan the interferogram. Control software registers both the position of the motor and the CC from timing electronics. Assuming photons are in the same quantum state, it is expected that when the motor reaches the position where the arms are just of the same length, CC will abruptly decrease ideally to zero. Such observed shape is known as HOM dip and is visualised in Figure 1.5(b).

As every interference pattern, the HOM interference may be evaluated according to its visibility[10]. There are 3 options how to improve the visibility. As already mentioned the source has to be fine tuned to provide indistinguishable photons which have to be in a pure state [122]. In other words, if the generated state is influenced for instance by white noise, such noise increases the minimum of interference pattern and, as a result, visibility drops. Better indistinguishability of photons in terms of their energy may be achieved by frequency filtering by incorporating narrow bandwidth filters (also known as interference filters with typical spectral width of 10 nm and less). Finally, single-mode

[10] In order to obtain distinct interference within the experiment, one needs to achieve maximal separation between baseline or differently value of CC outside the interference pattern ($\mathrm{CC_{max}}$) and minimal value of the HOM dip ($\mathrm{CC_{min}}$). Such quality is described by so-called visibility

$$\nu = \frac{\mathrm{CC_{max}} - \mathrm{CC_{min}}}{\mathrm{CC_{max}} + \mathrm{CC_{min}}} \quad . \tag{1.15}$$

Visibility can maximally reach unit value.

optical fibres (TEM_{00}) make the photons spatially indistinguishable preserving high interference visibility. Employment of these elements, however, unavoidably results in decrease of the signal putting strict requirements on adjusting of the whole setup to obtain as high signal as possible.

It is noteworthy that the dip (Figure 1.5(b)) is accompanied by two side maxima and its shape is of the form $a - b \cdot e^{(x-c)^2/f}\,\mathrm{sinc}(\frac{x-c}{g})$, where a, b, c, f and g are fit parameters. This shape is caused by specific shape of spectral filtering imposed on photons. Their spectrum is effectively a convolution of Gaussian function (due to setup geometry) with the rectangular shape of the interference filter used. Because of the high sensitivity of the HOM interference visibility, it serves as a precise indicator of imperfections of the source.

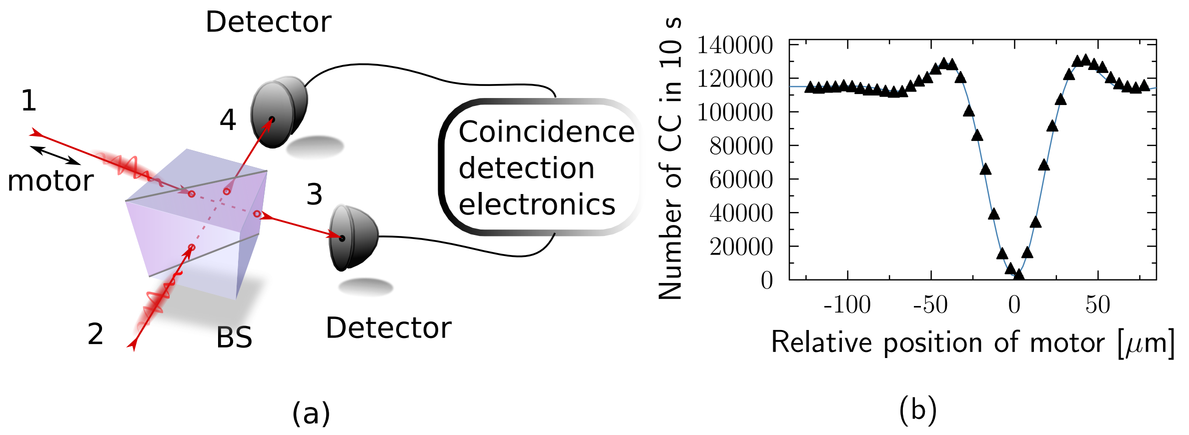


Figure 1.5: (a) Sketch of a part of an experimental setup with which one could obtain HOM dip [122]. Length of one input port may be adjusted by means of a motorised translation. (b) These data of HOM dip were obtained while adjusting the experiment presented in Chapter 2. Error bars are smaller than markers' size. The dip was fitted according to the function mentioned in the text. Visibility that equals to 0.96 was calculated according to Equation (1.15) where intensities were substituted by minimum of the fit function and by baseline of the dip. Each data point has been collected for 10 s.

1.5 Encoding of Qubits

Once the photon source has been described, the focus of this Section will be how to make use of the photons to encode into them quantum information. (For the definition of qubit see again the Introduction: Basics of Quantum Information.) Generally, single photon is a quantum system that provides several means for information encoding. The aim of the following text will be to acquaint the reader with polarisation and spatial encoding since these were used in experiments presented further. As for the first one, it is readily available since it is feasible to change photon's polarisation and finds its application also in classical optics. Other prominent techniques include encoding into continuous variables of position and momentum of photon, $\hat{x}$ and $\hat{p}$, respectively [123, 124], and encoding into angular orbital moment [125–127]. Intrinsically photons carry spin ($s = 1$) and additionally under some circumstances they may have an orbital angular momentum, too. Because orbital angular momentum states are integers and symmetrical with respect to zero, a three- and more-level system is formed. As such, they have a potential to accommodate general qudits [126, 128]. Encoding by means of occupation numbers is also available [129, 130], or time-binning can be used [128, 131].

1.5.1 Polarisation Encoding

Encoding into the polarisation state of light is relatively straightforward. As is depicted in Figure 1.6, there is a multiple choice of basis formed by mutually orthonormal vectors, e.g., $|H\rangle\,/\,|V\rangle$, $|D\rangle\,/\,|A\rangle$ and $|R\rangle\,/\,|L\rangle$. So the encoding is done by choosing a basis, for example H/V, and denoting horizontal state $|H\rangle$ as logical qubit $|0\rangle$ and vertical state $|V\rangle$ as $|1\rangle$. Any general superposition of logical states corresponds to a pure polarisation state[11], e.g. $|0\rangle + |1\rangle$. In this particular example, it would correspond to diagonal polarisation, but in general elliptic polarisation.

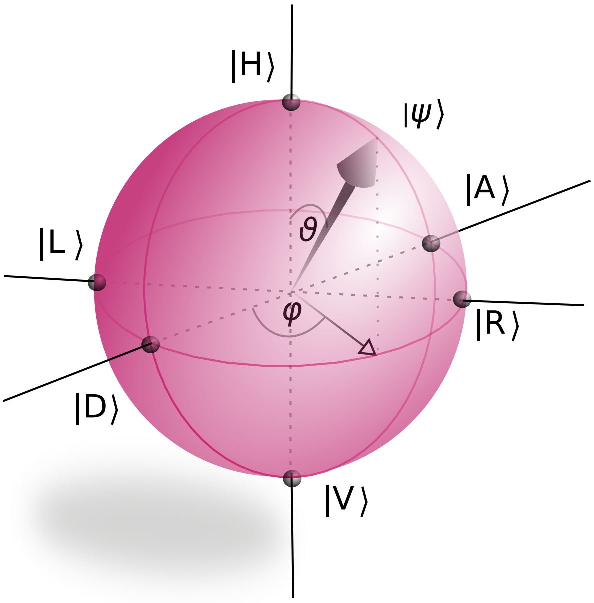


Figure 1.6: A Bloch sphere, depicted in this Figure, facilitates visualisation of polarisation states and corresponding qubit states. Polarisation basis are denoted as follows: horizontal $|\mathrm{H}\rangle$, vertical $|\mathrm{V}\rangle$, diagonal $|\mathrm{D}\rangle$, anti-diagonal $|\mathrm{A}\rangle$, right-handed circular $|\mathrm{R}\rangle$ and left-handed circular $|\mathrm{L}\rangle$, respectively. Ending point of any vector reaching surface of the sphere describes a pure state. Pure states are those mentioned so far like that found in Equation (1.1). Utilising Euler angles the state can be expressed as $|\psi\rangle = \cos(\vartheta/2)\,|\mathrm{H}\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin(\vartheta/2)\,|\mathrm{V}\rangle$. Mixed states (see the next Section 1.6.1) are often expressed in a form of density matrix (in Equation (1.16)) and they are visualised as vectors laying inside the sphere and starting in its centre.

As already mentioned, polarisation state of photons may be easily prepared. It can be shown that by combination of HWP and QWP one may obtain any required pure polarised state from an original $|H\rangle$ state. For exact transformation of input light by a WP see again Section 1.2.3. There is only one drawback: While propagating in standard circularly symmetric fibres, polarisation is easily changed by every bend of the fibre. Therefore, such changes have to be (i) prevented by employing this encoding in free space rather than in fibres or, one has to (ii) e.g. fix the polarisation change by fastening fibres to the optical table, and then (iii) compensate this change on several places within

[11] normalisation constant has been omitted for simplicity

every setup typically by mounting polarisation controller (PC). The polarisation state is easily projected by means of PBS, as is dicussed in Section 1.6, which is able to separate two mutually orthogonal polarisation states. It should be noted that Kwiat source inherently produces photons that are already found in a polarisation entangled state.

1.5.2 Spatial Encoding

Spatial encoding is also referred to as dual-rail encoding. In general, logical qubits denote two distinct paths a photon may take. There are several means of experimental implementation. Within experiments presented in this Thesis, encoding and subsequent decoding of qubits formed two paths, thus, effectively realising a Mach-Zehnder interferometer. Notably, the advantage of optical qubits is that one photon may be encoded into more than one degree of freedom. Such technique was used in the experiment in Chapter 3, where both polarisation and spatial encoding caused creation of 3-qubit state by means of just 2 photons present in the setup.

1.6 Quantum State Analysis

The very last step of each experiment is to analyse encoded qubits. In order to do so qubits have to be first projected into different bases corresponding to the given encoding method. Detectors capable of detection of such low signals are briefly mentioned in the following Section 1.6.2.

1.6.1 Analysis of Polarisation Encoded Qubits

Within presented experimental setups, polarisation encoding is the most frequently used one. Furthermore, another employed means of encoding, spatial encoding, may be converted into polarisation as well (see Chapter 3). The analysis of the encoded state is done by gradual projecting it into bases states and gathering event counts for some given time interval. In case of polarisation encoding the projection is done in the same manner as the encoding: by means of HWP and QWP in addition to PBS that separates two polarisation states from each other. Specifically, by means of these components all 6 projections are set onto horizontal, vertical, diagonal, anti-diagonal, right-handed circular and left-handed circular polarisations while counts are simultaneously measured and cumulated. In case of a 2-photon state, analysis consists of all combinations of $6 \cdot 6$ previously mentioned projections.

Because of unavoidable experimental imperfections or deliberate noise introduction, the description of observed quantum states using the $|\psi\rangle$ formalism is not sufficient. The state needs to be described in terms of a density matrix $\hat{\varrho}$. States that were influenced, e.g. by white noise, are a statistical mixture of pure states which prevents them from being expressed as a simple sum of pure states. Thus, such states are fully characterised by a density matrix $\hat{\varrho}$. To estimate the density matrix of quantum state we employ the maximum likelihood algorithm [132] that searches for the most plausible density matrix with respect to the observed projection counts. Generally, the density matrix is defined as

$$\hat{\varrho} = \sum_{i}^{N} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \quad , \tag{1.16}$$

where it is summed over a general number of N states each included with a probability p_i. Specifically, for example density matrix for 2 logical qubit state is of the form of

$$\hat{\varrho} = \begin{array}{cc} & \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{pmatrix} . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \end{pmatrix} \end{array} .$$

For each density matrix it holds that[12] $\mathrm{Tr}(\hat{\varrho}) = 1$ and that it is hermitian, i.e. $\hat{\varrho}^\dagger = \hat{\varrho}$. Each diagonal component corresponds to projection probability onto a given basis state (depicted as kets in the above Equation). For the pure state, the density matrix has a trivial form $\hat{\varrho} = |\psi\rangle \langle\psi|$. One can quantify purity $P = \mathrm{Tr}(\hat{\varrho}^2)$ and fidelity of the observed density matrix with the target pure state defined as $F = \langle\psi|\hat{\varrho}|\psi\rangle$. It should be noted that in density matrix notation, an entangled state (see Section 1.1) cannot be expressed in the form $\hat{\varrho}_{\mathcal{AB}} = \hat{\varrho}_{\mathcal{A}} \otimes \hat{\varrho}_{\mathcal{B}}$.

1.6.2 Detectors and Electronics

Quantum information experiments presented in this Thesis are constructed such a way that two photons are, with certain probability, found in the same output arm, yet they do not to cause coincidences and, as a result, do not contribute to HOM dip. Further to that, postselection of CC guarantees a well defined source of photon pairs so it is not important to differentiate the exact number of impinging photons. The parameters that are crucial for here presented experiments are high detector efficiency in order to detect the incoming photons with high probability, low dark count rate so that the signal was not lost in noise and a short dead time because of high rate of the source to name just a few.

Within the experiments we employed single-photon avalanche diodes SPCM-AQRH-14-FC by Excelitas company[13] and COUNT® - NIR by Laser Components[14]. Since the detectors produce a TTL pulse and Dual Counter Timer[15] (by Ortec company), registering events from both detectors, is able to work only with NIM logics[16], a TTL to NIM conversion has to take place. Coincidences are recorded by electronic modules TAC (an acronym of **T**ime-to-**A**mplitude **C**onverter) together with SCA (from **S**ingle **C**hannel **A**nalyser) by Ortec company[17].

[12] Tr stands for the trace of a matrix and it is defined as a sum of diagonal elements of that matrix.

[13] https://www.excelitas.com/product/spcm-aqrh

[14] https://www.lasercomponents.com/de-en/product/count-nir/

[15] https://www.ortec-online.com/products/electronics/counters-timers-rate-meter-and-multichannel-scaling-mcs/994

[16] NIM standart defines voltage 0 V as logical 0 and -0.8 V as logical 1. In addition to it, it is required $50\,\Omega$ of input impedance.

[17] https://www.ortec-online.com/products/electronics/time-to-amplitude-converters-tac/567

Chapter 2

Experimentally Attacking Quantum Money Schemes Based on Quantum Retrieval Games

Contents of this Chapter is based on the Author's article [A1].

2.1 Introduction

The concept of quantum money (QM) was proposed by Wiesner in the 1970s. Its main advantage is that every attempt to copy QM unavoidably leads to imperfect counterfeits. In the Wiesner's protocol, quantum banknotes need to be delivered to the issuing bank for verification. Thus, QM requires quantum communication which range is limited by noise and losses. Recently, Bozzio et al. (2018) have demonstrated experimentally how to replace challenging quantum verification with a classical channel and a quantum retrieval game (QRG). This brings QM significantly closer to practical realisation, but still thorough analysis of the revised scheme QM is required before it can be considered secure. We address this problem by presenting a proof-of-concept attack on QRG-based QM schemes, where we show that even imperfect quantum cloning can, under some circumstances, provide enough information to break a QRG-based QM scheme.

All payment methods are potential targets of thieves and counterfeiters. Over the course of history, we have witnessed a race of arms between the counterfeiters and issuers of various currencies. Remarkably, Sir Isaac Newton, who became the master of Royal Mint, enforced laws against counterfeiting. Nevertheless, the methods used by Newton become obsolete when it comes to modern payment methods. With the rapid technological progress, we are beginning to consider a situation where counterfeiting is no longer limited by the available technology, but rather by the laws of nature. An example of such fundamental limitation is the no-cloning theorem,[133, 134] which guaranties security of quantum money [38, 39, 135–137].

In a recent paper, Bozzio *et al.* [78] reported on an implementation of a QM scheme based on QRGs [138–140]. While this result brings QM closer to practical implementation, here we demonstrate that QRG-based QM schemes are still vulnerable to a new kind of attack (for some typical attacks see Ref. [141–145]) which can be considered a quantum version of sniffing (a hacking method used to monitor classical information). The general idea of our attack can be used against a broader range of QM schemes based on QRG [146–148] and potentially on other quantum communication protocols. Thus, our results can facilitate future practical implementations of QM by providing a method for exploring the security limits allowed in QRG-based protocols. For the

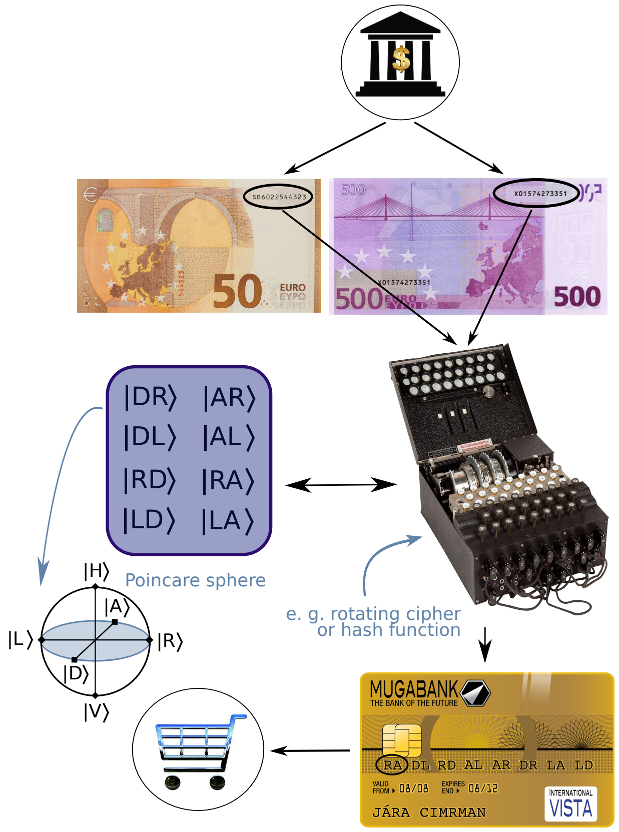


Figure 2.1: Scheme of encoding of classical banknotes using their serial number by the bank. The secret encoding process, like e.g. hash function, is visualised by the Enigma machine [152].

purpose of our research we have experimentally recreated the original scheme of Ref. [78]. Its working principle can be described as follows: the bank encodes QM (as a quantum token) using a secret sequence of qubit pairs chosen from the list of eight options:

$$S = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle, |+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle\}, \tag{2.1}$$

where $|0\rangle$, $|1\rangle$ are logical qubit states, and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ stand for their superpositions. Note that three bits are needed by the bank to store information on one qubit pair on token. The tokens and their serial number are then stored on a quantum credit card [78, 149, 150] subsequently given to a client of the bank (Figure 2.1). Upon payment, the credit card is inserted into the vendor's terminal which is supposed to perform projection measurements on these pairs in a measurement basis requested by the bank (randomly chosen to be either 0/1 or +/- for an entire pair). Then, the terminal sends the classical outcomes of those measurements to the bank. The main advantage of this scheme is that the terminal measurement itself is sufficient for authentication of the credit card, so quantum states do not have to be sent to the bank for verification. The bank just checks the results knowing the specific encoded states and either accepts or denies the payment. A small amount of errors is expected to appear in the verification procedure to account for implementation imperfections. The acceptable amount of errors needs to be small enough to ensure that payment by a cloned quantum credit card is denied. In contrast to the original Wiesner QM scheme [38], no on-line quantum channel has to be used for payment. Thus, the verifiability problem as defined by Aaronson and Christiano [151] is at least partially solved.

This protocol is secure against a dishonest terminal only if each quantum sequence is generated using a truly random encoding. However, such condition would give rise to a giant database problem, as discussed in [151] and [153]. The random sequence approach is highly impractical or even infeasible. In practice, there has to be one secret encoding function shared by a certain number of quantum banknotes or tokens (i.e., sequences of quantum states and their serial numbers). Hence, in our research we test limitations of sharing a secret encoding by multiple tokens. The tokens are therefore encoded using a prescription based on the output of a classical algorithm. Inputs to the this algorithm are the publicly known serial numbers (SN) and secret salt (a secret number).

The aim of suggested attack is not to copy single banknotes but to be able to generate new banknotes that pass as genuine. Note that by employing the studied attack strategy, a terminal can collect in principle unlimited data during its operation. This attack can be run in parallel while having many wiretapped terminals. Moreover, we show that by using optimal quantum cloning we can learn the secret faster than by limiting the attack only to classical data processing.

Although quantum cloning has been already used to counterfeit QM [39], the purpose of quantum cloning here is completely different and as such is virtually undetectable by the bank because we copy only parts of quantum tokens (i.e., quantum sequences). In terms of QRG-based QM protocol, the attacker utilises a compromised payment terminal enabling quantum cloning of an input qubit (see Fig. 2.2). The terminal performs measurements on both copies of a qubit providing the attacker with some information on the encoding used by the bank, if two consecutive qubits from a sequence are cloned. The frequency of cloning can be arbitrarily small and therefore made unrecognisable from noise. After gathering enough data, the attacker reveals the secret encoding used by the bank for preparing credit cards. Since then, they can issue fake quantum credit cards indistinguishable from the original ones issued by the bank.

Quantum cloning has been proposed and tested as a means of attack on quantum communications protocols [141–143, 154, 155]. There is, however, a significant conceptual difference between cloning attack on quantum cryptography and the quantum money scheme discussed in this Chapter. The necessary condition for successful attack on quantum cryptography protocol is having ideally 100% of the quantum key eavesdropped. Otherwise, the security can be attained by privacy amplification arbitrarily lowering the attacker's probability of decoding the shared message [156]. On the other hand, attack on QM based on QRG described within our research only requires to clone a small fraction of the money tokens. Such infrequent cloning is basically undetectable in the noise, albeit gathering data would proceed slowly. A typical obstacle in cloning-based QM attacks is requirement of high cloning success rate as at least half of the token needs to be cloned successfully (i.e. not destroyed) [39]. This fact needs to be dealt with on probabilistic platforms such as linear optics. The method discussed in this Chapter is completely free of this limitation.

2.2 Results of a Quantum Sniffing Attack

We have implemented the quantum sniffing attack on the platform of linear optics, where qubits are encoded as polarisation states of single photons. The optimal cloning strategy (i.e., maximizing single-copy cloning fidelity) for copying qubits from the set S is the symmetric phase-covariant cloning (SPCC) [39, 141, 157]. In the experiment, pairs of input qubits $|\psi_1\psi_2\rangle_{\rm in} \in S$ were subjected to SPCC procedure obtaining two clones $\hat{\varrho}_{1\rm A} \otimes \hat{\varrho}_{2\rm A}$ and $\hat{\varrho}_{1\rm B} \otimes \hat{\varrho}_{2\rm B}$ of the input qubit pair. These clones were then measured in the same but random basis. In a QRG-based QM protocol the basis is selected by the bank. Due to limitations of linear optics based implementations of quantum cloners [108], the SPCC process is probabilistic and sometimes it fails to deliver the clones. The probability of successful cloning of one input qubit is denoted P. Therefore the probability of cloning the entire qubit pair is P^2. Quality of the clones is expressed in terms of fidelity F defined as $F = F_{ij} = {}_{\mathrm{in}}\langle\psi_i|\hat{\varrho}_{ij}|\psi_i\rangle_{\mathrm{in}}$, where $i = 1$, 2 and $j = \mathrm{A}$, B denote the first and the second clone, respectively. The probability of finding both clones $\hat{\varrho}_{i\mathrm{A}}$ and $\hat{\varrho}_{i\mathrm{B}}$ in a given state $|\psi_i\rangle_{\mathrm{in}}$ reads F^2. An example of an attack on a particular qubit pair is shown in Fig. 2.2.

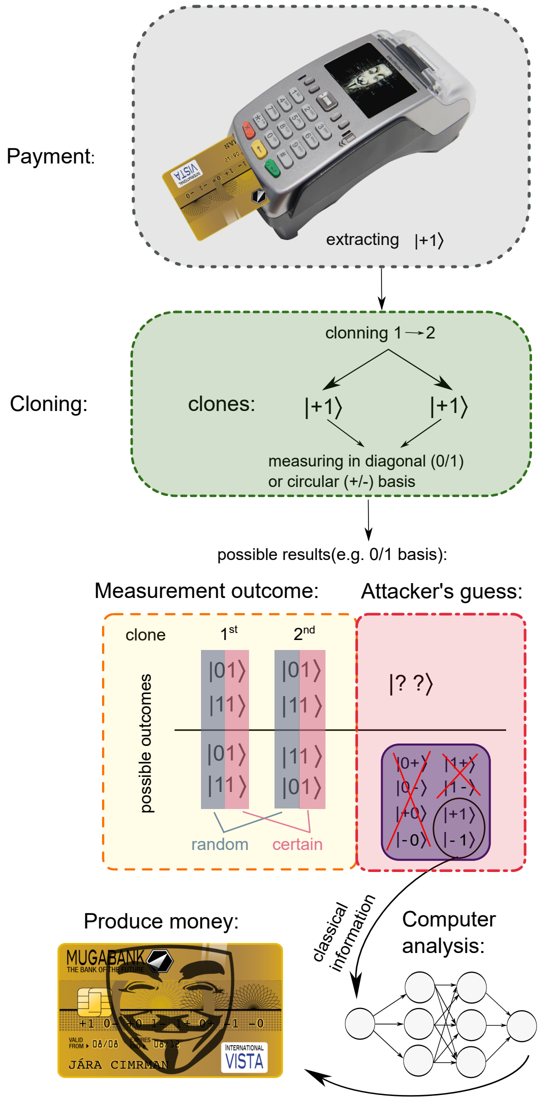


Figure 2.2: Attack on a quantum credit card utilising a hacked terminal. During a transaction a pair of states (e.g., $|+1\rangle$) is extracted from the card and cloned. Here, for simplicity, we depict only the situation where all the qubits are perfectly copied (the probability of such event is proportional to F^2). Then, measurements are performed on all four copies in the basis randomly chosen by the bank (e.g. 0/1). If the measurements on copied qubit pairs produces one of two results from the bottom block of the table of outcomes, the attacker learns the originally encoded state (in this case $|?\,1\rangle$). This procedure is repeated until a relation between the quantum states and serial numbers is learned. Since then, the attacker can issue perfectly counterfeit quantum credit cards.

The theoretical limit for SPCC fidelity [157] is $F = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.854$ and on the platform of linear optics the cloning succeeds with probability $P = \frac{1}{3}$. While the limit on fidelity is fundamental in its nature, P depends on the physical platform used in a given implementation and can be arbitrarily close to 1. However, even on the platform of linear optics, it is possible to clone at arbitrarily high values of P but at the expense of reaching lower than optimal fidelity F (see hybrid quantum cloners [141, 158]).

The terminal registers two measurement outcomes per input qubit corresponding to the clones. If the two clones of one input qubit yield identical results, while for the other yield opposite results, the attacker gains information about the encoding. With the probability $P_{\text{tot}} = P_{\text{c}} + P_{\text{e}}$ the attacker eliminates six of the original eight encodings (see Eq. 2.1). One of the two remaining encodings have actually been used by the bank. The probability of obtaining correct information from the attack is $P_{\text{c}} = \frac{1}{2}P^2F^2$, whereas $P_{\text{e}} = \frac{1}{2}P^2(1-F)^2 + P^2F(1-F)$ stands for the probability of getting an erroneous result due to limited cloning fidelity. Similarly, if the two clones of each input qubit yield identical results, the attacker knows that only one of four encodings might have been sent by the bank.

The attacker is able to learn the method of encoding tokens by accumulating measurement results provided that the fidelity is $F \neq \frac{1}{2}$. The cloning operation inherently introduces errors in the measurement outcomes [133, 134]. Hence, the terminal might send to the bank incorrect results. If the error rate surpasses a given limit (25% in Ref. [78]), the bank will reject the payment. Thus, it is necessary to introduce a strategy of attack considering all circumstances of the measurement (i.e., if cloning failed or not) and its outcomes to minimise the error rate. There are generally three distinct strategies: (i) to provide the bank with measurement outcome every time cloning takes place and even if it fails, send a random value, (ii) to send measurement outcome, only if it is registered by the terminal and report a lost qubit when cloning fails and (iii) to measure qubits after their extraction from the credit card in given measurement basis but do not perform cloning at all.

To quantify the correlations between the attacker and the genuine token we use mutual information I_{sec}, which expresses how many bits of information can the attacker obtain upon cloning one qubit pair. The exact value of mutual information depends on the strategy used, cloning success probability P and fidelity F. In case of the third strategy (without cloning), its value is $\frac{1}{2}$. For more details on this strategy refer to section Methods.

Simultaneously, we denote ϵ the probability of an error being reported to the bank. The expressions for error rates ϵ for the two above-mentioned strategies can be obtained by direct calculations based on analysis of probabilities of all possible scenarios and read

$$\begin{aligned} \epsilon_{\text{(i)}} &= \tfrac{1}{2}(1-P) + P(1-F)\,, & (2.2)\\ \epsilon_{\text{(ii)}} &= 1 - F\,. & (2.3) \end{aligned}$$

Equation (2.2) takes into account two situations. In the first case, one or both qubits are lost during cloning and, therefore, random results are reported to the bank (50% chance of error). In the second case, even if cloning succeeds, non-unit fidelity may cause the measurement to yield an incorrect result. The error rate in case of strategy (ii) depends only on imperfect cloning fidelity.

The relation between mutual information I_{sec} (between the bank and the attacker) and the error rate ϵ for all strategies is show in Fig. 2.3. In the figure, quantities

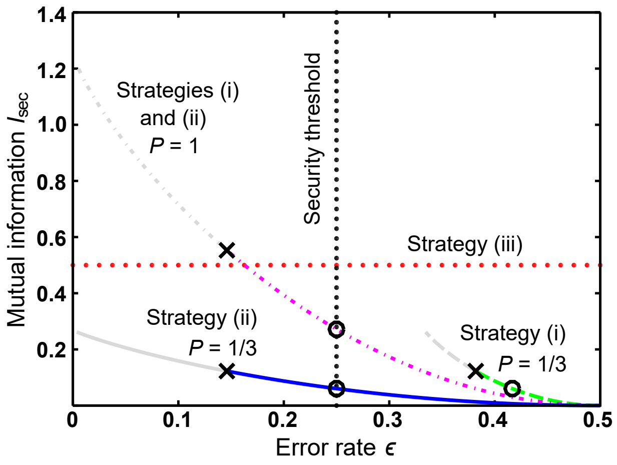


Figure 2.3: Mutual information I_{sec} versus error rate ϵ for two fixed probabilities $P = \left\{\frac{1}{3}; 1\right\}$. Vertical black dotted line represents error rate associated with security threshold discussed in Ref. [146] and [147]. Crosses mark the smallest average error introduced by optimal cloning for a fixed value of P. Error rates below these optimal values cannot be reached by any physical operation (greyed curves). Circles stand for limit of classical copying ($F = 0.75$). Thus, the segments of curves between circles and crosses mark the regime of quantum copying. It follows from Eq. (2.3) that classical copying limit in strategy (ii) always corresponds to intersection between the relevant curve and the security threshold. For more details on strategy (iii) refer to section Methods.

I_{sec} and ϵ are functions of cloning fidelity for $\frac{1}{2} \leq F \leq 1$ for two cloning success rates $P = \frac{1}{3}$ (linear optics limit [39, 108, 158]) and $P = 1$ (deterministic cloning [39, 158–160]). In case of deterministic cloning the two attack strategies coincide, but for probabilistic cloning the second strategy provides better results. It is fair to note that the mutual information of any simple linear-optical cloning strategy is lower in comparison with the no-cloning strategy (iii). On the other hand, with deterministic cloning, one can reach even higher values of mutual information and therefore cloning strategies need to be considered for security implications. Additionally, machine learning-based algorithms may require data with as little noise as possible even at the expense of the overall quantity. Post-selection on successful cloning events allows to distil such sample. Corresponding conditional mutual information yields a significantly higher value when both qubits are successfully cloned than for the no-cloning strategy (iii) (Fig. 2.4).

To prove the working principle of the quantum sniffing attack, let us consider a specific encoding of the quantum tokens and demonstrate the attacker's approach to learning the encoding. Here, we assume that the bank uses a hash function to encode the tokens. Since the hash functions have become a worldwide standard for encryption and basis of many classical cryptosystems they would be easily deployable by the bank. Hash functions are designed to return very distinct results even for similar inputs making their output unique. Another advantages are, for instance: irreversibility, (i.e. impossibility to retrieve original message from a given hash), or their repeatability (they yield the same hash for the same message).

The input can be additionally modified by using a specific secret number (salt). In this case the hash function is often referred to as salted. For simplicity, let us now assume that the hash function is known to the attacker, but the salt is secret. For each token passing through the terminal, the attacker calculates hashes (outputs of the hash function) of its serial number salted by numbers from a certain range. This way the

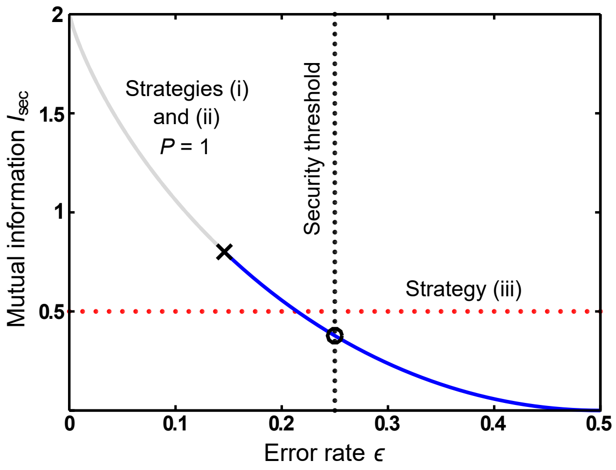


Figure 2.4: Conditional mutual information I_{sec} versus error rate ϵ. Strategies (i) and (ii) are equal in this case.

attacker investigates various encodings each corresponding to one secret number (or salt). Using the information gained by quantum sniffing, the attacker calculates the number of agreements (matching qubit pairs) between the predictions of the tested encoding and the measurement outcomes on real tokens. The encoding with highest number of agreements is most probably the one used by the bank, hence the one corresponding to the correct salt.

To showcase the attack, we have implemented token encoding using several known hash-based functions, i.e. MD5 [161], HMAC-SHA512, HMAC-SHA256, and HMAC-SHA1 (HMAC – Hash-based Message Authentification Code [162]). Typical example of encoding using SHA512 is depicted in Fig. 2.5. In our proof-of-concept experiment, the salt has been sought only among three-digit numbers. To distinguish the secret number from noise originating from random matches, a sample of 4 040 successfully cloned photon pairs (corresponding to 101 serial numbers used in the experiment) has been evaluated. To optimise the computational resources of the attacker, the algorithm gradually refines the set of evaluated secret numbers. Periodically it removes secret numbers with low number of agreements from the list of evaluated numbers. Once the number of agreements for one secret number surpasses the average number of agreements by selected multiple of standard deviation, the algorithm ends and returns that number. Note that due to some error tolerance, the attacker does not necessarily need to recreate the original hash function. It would be enough if they found a function which error rate is below the security threshold.

The size of HMAC output of all used hash functions was set to be 40 bytes. As a consequence, the number of tokens necessary for guessing the secret number was independent on the number of digits of their serial number. For each hash function we have established how many photon pairs need to be successfully cloned in order to reveal the secret number with sufficient certainty. The results are summarised in Tab. 2.1. The number of cloned pairs needed does not scale with the length of the salt. The salt length only increases the classical computing time. According to our numerical simulation, number of photon pairs necessary for correct guess is linearly increasing with the number of output hash bits. However, with the length of output hash the frequency of cloning (number of cloned pairs/total number of transmitted photon pairs) does not change because the length of the token is also increasing. The output hash and the token have to have the same length in order to avoid incidents such as two inputs

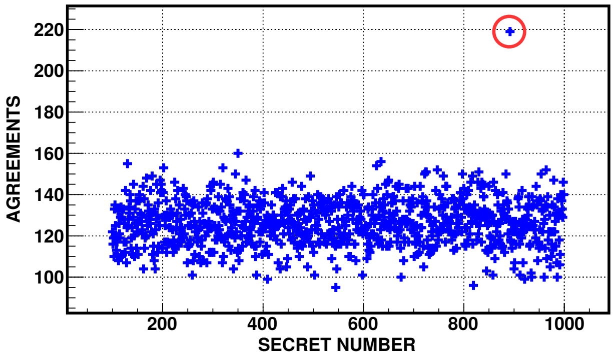


Figure 2.5: Dependence of number of agreements on all possible three-digit secret numbers evaluated for 4 040 successfully cloned photon pairs. The revealed secret number (salt) is marked by a red circle.

Table 2.1: Minimal number of photon pairs cloned for correct guess of the secret number (salt).

hash-based function	number of pairs
HMAC-MD5	1 400 ± 16
HMAC-SHA512	1 192 ± 14
HMAC-SHA256	1 060 ± 14
HMAC-SHA1	1 272 ± 13

to the hash function yielding the same output. Longer hash output would, therefore, result in increase of computer search time, however, it would not prevent the attacker from retrieving the secret number since the searching process is performed in parallel with the cloning attack. Note that these results were obtained using our experimental results where the average cloning fidelity was found to be above 80%.

We have also performed a generalised attack in which the attacker did not know what hash function had been used for encoding. The attacker only assumes the hash function is one from a given set. In this situation, the attacker has to calculate hashes using all hash functions in this set to encode serial numbers and count numbers of agreements as described above. The plot in Fig. 2.6 shows the search for the secret number among four hash functions. The tokens were encoded using MD5. Our results indicate that the correct secret number and hash function can be revealed assuming the hash function is a member of a finite set. The size of which is limited by the available time and computing power.

2.3 Experimental Implementation

Photonic qubits were encoded as four polarisation states located on the equator of Poincaré sphere: $|D\rangle$, $|A\rangle$, $|R\rangle$ and $|L\rangle$ (i.e. diagonal linear, anti-diagonal linear, right-handed and left-handed circular polarisations). Thus, the set of possible qubit pairs (2.1) is given as

$$S' = \{|DR\rangle, |DL\rangle, |AR\rangle, |AL\rangle, |RD\rangle, |LD\rangle, |RA\rangle, |LA\rangle\} . \tag{2.4}$$

Experimental setup used in our experiment is shown in Fig. 2.7. Photon pairs at λ $= 710\,\mathrm{nm}$ are generated in a process of type-I spontaneous parametric down-conversion

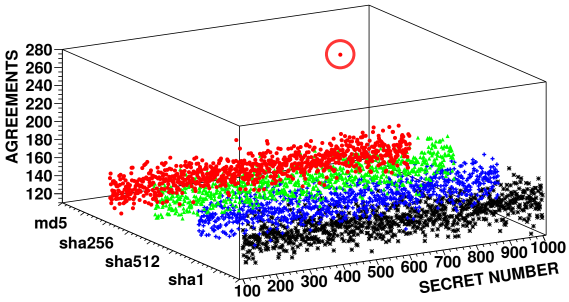


Figure 2.6: Dependence of number of agreements on all three-digit secret numbers. Four different hash functions are tested. The bank used MD5 for encoding. In this plot, 4 040 successfully cloned photon pairs were analysed. The revealed secret number (salt) is marked by a red circle.

(SPDC) in a BBO (β-BaB$_2$O$_4$) crystal. The crystal was pumped by Paladine (Coherent) laser operating at $\lambda = 355\,\mathrm{nm}$. One photon from each SPDC-generated pair served as one qubit of the cloned banknote. We used a sequence of half and quarter wave plates (HWP and QWP, respectively) to implement encoding. The second photon from the SPDC-generated pair was meanwhile used as a cloning ancilla (kept horizontally polarised as it is the theoretically known optimum for SPCC).

Given the nature of the attacked scheme, phase-covariant cloning is the optimal form of cloning attack. It has been used to attack distinguished quantum cryptography protocols such as BB84 [58] or RO4 [163, 164]. The attacked QM scheme uses equatorial qubits in the state

$$|\psi_s\rangle = 1/\sqrt{2}\left(|0\rangle + e^{i\eta}|1\rangle\right) , \tag{2.5}$$

where $|0\rangle$ and $|1\rangle$ denote logical qubit states and η the phase. For this class of states, the phase-covariant cloner reaches fidelity of 0.854. Equatorial states can be unitarily transformed into states laying on the intersection of Bloch sphere and the plain running through the centre of the sphere for which the optimal cloning transformation is defined in Eq. 2.6.

Cloning is performed by an unbalanced polarisation-dependent beam splitter (BS) which implements the optimal SPCC process (for detailed theoretical description see Ref. [108, 157, 165], for experimental implementation see also Ref. [166]). Particular splitting ratio for horizontal and vertical polarisations accounted for 0.21 and 0.79, respectively. During the experiment signal and ancillary photons overlap at the BS which results with success probability of $\frac{1}{3}$ in the cloning transformation:

$$\begin{aligned} |0\rangle_{\mathrm{in}}|\psi_a\rangle &\rightarrow |00\rangle , \\ |1\rangle_{\mathrm{in}}|\psi_a\rangle &\rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) , \end{aligned} \tag{2.6}$$

where $|\psi_a\rangle$ denotes the state of ancilla.

Subsequently, each photon is projected in the D/A or R/L measurement basis as requested by the bank (using HWPs, QWPs, and polarisers). The process of cloning is successful only if each photon leaves BS by different output port. Therefore, we are interested in coincidences between both output arms. The detection is handled by single-photon detectors operating with detection efficiency of around 60% and subsequent electronics. In the experiment, we have registered individual coincident detections one by one thus genuinely implementing the protocol described in the text.

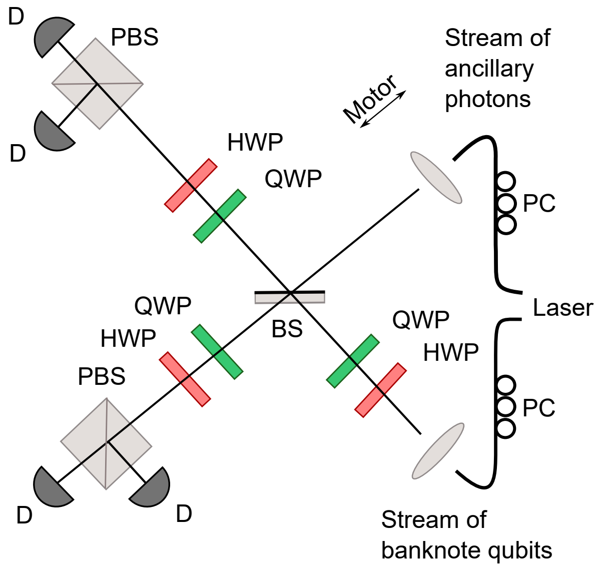


Figure 2.7: Laboratory setup for the quantum sniffing experiment. The setup operates as the compromised terminal from Fig. 2.2. Its components are labelled as follows: BS – partially polarising beam splitter, QWP – quarter-wave plate, HWP – half-wave plate, PBS – polarisation beam splitter, PC – polarisation controller, D – single-photon detector.

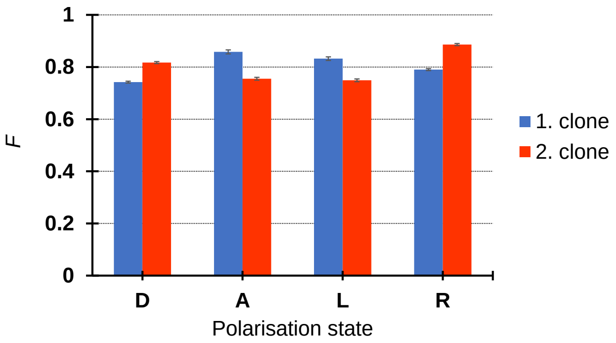


Figure 2.8: Average fidelity of the first and second clone of a qubit from the cloned set measured by projections in appropriate bases.

Quality of the clones was quantified by fidelity for both clones and each possible sequence qubit state (Fig. 2.8) by evaluating statistics of observed individual coincidence events. The average cloning fidelity was calculated to be $(80.3 \pm 0.3)\%$ while some clones in the two output arms had slightly different fidelities. Typical detection rate was 120 pairs per second.

In order to quantify the correlation between the attacker and the information encoded as a pair of qubits, we enter the value of mutual information I. This value determines how many bits of information an attacker can get after cloning one pair of qubits and depends on the strategy used, success probability of cloning P and its fidelity F. Mutual information is calculated as

$$I = \sum_{X,Y=000}^{111} p_{X,Y} \log_2 \frac{p_{X,Y}}{p_X p_Y},$$

where $p_X = \sum_{Y=000}^{111} p_{X,Y}$, $p_Y = \sum_{X=000}^{111} p_{X,Y}$, and X,$Y = 000, 001, 010, 100, 110, 101, 011, 111$. The technical details on calculating probability distributions needed for calculating mutual information for all the considered strategies are given in the Supplement in Appendix A.1. Here we provide a brief introduction into the working principle of strategy (iii). Without performing quantum cloning, the attacker measures the qubits as requested by the bank and simultaneously uses this information to obtain some knowledge about the encoding used. While this approach enables to rule out some of 8 encodings, these eliminated encodings depend on the order of encoding bases. The attacker can assume that the order of encoding bases for the received qubit pair is either Z/X or X/Z, where $Z \in \{0;1\}$ and $X \in \{+;-\}$. This order must be random because there is no way of gaining this information. Thus, maximum information to gain in this strategy is $I_{\max} = 2$ instead of $I_{\max} = 3$ when the order is known. Depending on the measurement outcomes, with probability $\frac{1}{2}$ the attacker can exclude some encodings and can guess the order of bases correctly only in half of the cases. Only if successful, half of 4 encodings can be eliminated. This makes $I_{\text{sec}} = \frac{1}{4} I_{\max} = \frac{1}{2}$.

2.4 Conclusion and Discussion

We have successfully attacked a QM scheme based on QRG [78]. This scheme has been implemented in a form of quantum credit card containing quantum tokens. We retrieved the secret number (salt) used for preparing quantum tokens purely by means of imperfect quantum cloning and computational analysis of measured data (see Fig. 2.5 and 2.6). By learning the exact algorithm for encoding quantum tokens, the attacker is, in principle, able to produce perfect quantum money counterfeits. It is worth noting that the optimal strategy of our attack depends mainly on a particular implementation of bank's security tolerances (e.g., losses) and chosen physical platform for implementing the attack. For instance, if the attacker uses deterministic optimal cloning even less qubit pairs is needed to perform the attack (see Fig. 2.3).

However, the attack was feasible because the bank encoded sufficiently high number of photon pairs using the same secret number (salt) and the same hash function. From the data summarised in Tab. 2.1 we can deduce that if the bank changes, e.g., the secret number after less then 1000 photon pairs, the attacker is not able to reveal the bank's secret with sufficient certainty. This leads to further vital questions regarding tolerance of the bank to noise and threshold value losses.

We hope that our results will stimulate further research on security of QM schemes based on QRG bringing this concept closer to becoming a fully fledged quantum technology. Our results indicate that the correct secret number and hash function can be revealed assuming the hash function is a member of a finite set. The size of which is limited by the available time and computing power. However, this is not a fundamental limitation which might be lifted if more advanced cryptanalysis or more computing power is applied. Our results indicate that while the idea of using hash functions might be tempting, it would be ultimately more secure to store truly random sequences since only these are not vulnerable to the attack described in this Chapter. The recent progress in data storage technologies and quantum computing with its fast searching algorithms (e.g. Deutsch-Jozsa algorithm [167]) may in future enable this. With current technology, the most secure strategy would depend on particular implementation of the protocol by the bank.

Chapter 3

Measuring Concurrence in Qubit Werner States Without an Aligned Reference Frame

Contents of this Chapter is based on the Author's article [A3].

3.1 Introduction

Secure and reliable information exchange is of paramount importance worldwide, hence the practical implementation of quantum communications protocols outside the scientific laboratory has become one of the main focuses of recent studies [168, 169]. Naturally, such advances in quantum communication methods require the ability to perform quantum measurements in an unstable environment, where the strict requirements for alignment and calibration of remote devices are hard to meet (e.g., long-distance quantum communication [73, 170, 171] or satellite-based communications [72, 74, 172, 173]). Specifically, the above-mentioned quantum communications experiments usually rely on quantum optical devices, where qubits are encoded into polarization states of light. However, this necessarily requires a common reference measurement frame to be shared that has to be well aligned and calibrated measurement devices (in a sense of well-defined scale of measurement apparatus such as the rotation angles of wave plates). Furthermore, it also needs to be maintained stable for the entire experiment or communication. From an experimental point of view, this is, however, never achieved without technical difficulties (see, for instance, [174]). Maintaining a common reference frame seems a trivial assumption when confined to a laboratory, but long-distance quantum communications beyond the Earth's surface [72, 74, 172, 173] have already led scientists to re-evaluate the practicality of such an assumption [175, 176].

A possible solution to these problems in free space could be to use rotationally invariant states of light [177]. However, to the best of our knowledge, no one has yet applied these solutions in satellite quantum communication. Instead, much attention has been paid to so-called reference-frame-independent (RFI) protocols [178–185]. For instance, it was proved in Ref. [186] that a RFI quantum key distribution protocol [187] is more robust under reference frame fluctuations than its standard counterpart [58, 59].

Motivated by all these observations, in this Chapter we also investigate the RFI approach. In particular, we focus on quantum entanglement, which is undoubtedly the essence of many quantum information procedures [42, 45, 188]. Therefore, it is necessary to be able to test for the presence of entanglement and, for the reason explained previously, it is practical to manage it in RFI mode [93, 189–192]. Over time, several methods for entanglement detection under these constraints have been proposed. They are based on various approaches, for example, on the violation of a Bell inequality [193, 194], the second moment of the distribution of correlations [195, 196], a geometrical threshold criterion [197], or interference between multiple copies of the investigated state [198]. However, all of them were so far limited to being mere witnesses to entanglement rather than measures. Entanglement quantification is of considerable interest for both theoretical and practical reasons. Our goal is to introduce a device-independent entanglement quantification protocol operating in the RFI approach without calibrating measurement devices, which is of great importance from the experimental point of view. More specifically, we investigate the RFI measure of Bell nonlocality and its relation with entanglement. As Bell nonlocality and entanglement are distinct resources, one cannot establish a direct link between them in the general case, and this is the price paid for the great simplification of the experimental requirements given previously. However, such a relationship can be identified for specific families of states. Because of this, we restrict our attention to two- and three-qubit states which are of practical importance in quantum information processes. One such example is the family of Werner states which have been instrumental for various important advancements in quantum information [199–201]. Moreover, the Werner states are "considered as the paradigmatic example of realistic noisy preparation of a pure entangled state subject to the action of white noise" [202]. Although this family contains examples of states with nonclassical correlations, which nevertheless admit a hidden-variable model, the violation of a local-realistic description is still observed for highly entangled cases which are, in fact, applied in quantum information procedures. We also discuss to what extent the results obtained for the Werner states can be used to estimate the entanglement of other two- and three-qubit states. In other words, we test how precisely one can estimate the entanglement of an unknown state if our RFI approach is applied. Surprisingly, we found that our calculations can be successfully applied to quantify the entanglement of more general states, for example, pure states, Greenberger-Horne-Zeilinger (GHZ) symmetric states. This result also justifies the experimental simplification within which we still obtain an instrument that can find its application in future practical long-distance quantum communications. Finally, we present an experimental verification of our predictions.

3.2 Preliminaries

3.2.1 Entanglement Measure

We now introduce concepts that are relevant to the current investigation. Let us first consider a two-qubit pure state $|\psi\rangle_2$, composed of subsystems A and B. The degree of entanglement between both subsystems is given by so-called *concurrence* [203], $\mathcal{C}(|\psi\rangle_2) = \sqrt{2\,(1 - \mathrm{Tr}(\rho_A^2))}$, where ρ_A denotes the reduced density matrix of subsystem A. For mixed states ρ the concurrence is defined by the convex-roof extension [204], $\mathcal{C}(\rho) = \min_{\text{all decomp.}} \sum_j p_j \mathcal{C}(|\psi_j\rangle)$, where the minimum average concurrence is taken over all possible convex decompositions $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ into pure states. In a special case, when ρ_2 denotes two-qubit mixed state, the mixed-state concurrence is given by

$$\mathcal{C}(\rho_2) = \max\{0, \sqrt{\lambda_1} - \sum_{j=2}^{4} \sqrt{\lambda_j}\} \tag{3.1}$$

with $\{\lambda_j\}$ being the decreasingly ordered eigenvalues of $\rho_2(\sigma^y \otimes \sigma^y)\rho_2^T(\sigma^y \otimes \sigma^y)$, where σ^y denotes the Pauli matrix and the transposition is performed in any product basis.

The measure described previously can be further extended to describe the genuine multipartite entanglement (GME) [205–208], that is, a scenario when a multipartite state has a minimum amount of entanglement in each bipartition. For instance, if the analysed pure state $|\psi\rangle_3$ is composed of three subsystems A, B, and C, one can distinguish three bipartitions $\{\gamma|\gamma'\}$, namely $\{A|BC\}$, $\{B|AC\}$, and $\{C|AB\}$. Then, the GME concurrence is given by [207]

$$\mathcal{C}_{\text{GME}}(|\psi\rangle_3) = \min_{\text{all bipart.}} \sqrt{2\left(1 - \text{Tr}(\rho_\gamma^2)\right)}, \tag{3.2}$$

where the minimum is taken over all possible bipartitions $\{\gamma|\gamma'\}$ and ρ_γ denotes the corresponding reduced density matrix of subsystem γ. The extension of GME concurrence to mixed states also follows the convex-roof extension presented previously [207].

We stress that a general expression for mixed-state GME concurrence still remains unknown. However, it has been successfully evaluated for the so-called X-matrix states [209]. These states are represented by a density matrix written in an orthonormal product basis, the non-zero elements of which are only the diagonal (denoted by a_j and b_j, where $j = \{1, \ldots, 2^{N-1}\}$) and/or anti-diagonal elements (given by z_j and its conjugation). The X-matrix states are positive if $|z_j| \leq \sqrt{a_j b_j}$ and we also expect $\sum_j (a_j + b_j) = 1$ to ensure the normalisation of ρ_{X}. The GME concurrence for these states is given by [210]

$$\mathcal{C}_{\text{GME}}(\rho_{\text{X}}) = 2 \max_i \{0, |z_i| - \chi_i\}, \tag{3.3}$$

where $\chi_i = \sum\limits_{j \neq i} \sqrt{a_j b_j}$.

3.2.2 Bell-Nonlocal Correlations

Next, let us consider an N-partite Bell experiment where each party has a choice over two measurement settings $S_i = \{0, 1\}$ and each measurement results in one of two possible outcomes $r_i = \{0, 1\}$. The corresponding Bell experiment is then fully characterised by the set of joint conditional probability distributions $\mathbf{P} = \{P(\mathbf{r}_N|\mathbf{S}_N)\}$, where $\mathbf{r}_N = (r_1, \ldots, r_N)$ and $\mathbf{S}_N = (S_1, \ldots, S_N)$. When the participants share a quantum state ρ and the correlations are generated by local measurements performed on their respective subsystems, then $\mathbf{P}$ takes the form of $P(\mathbf{r}_N|\mathbf{S}_N) = \text{Tr}\left(\bigotimes\limits_{i=1}^{N} \hat{M}_{r_i|S_i} \rho\right)$, where $\hat{M}_{r_i|S_i}$ is the positive operator-valued measure representing the measurement on the i-th party with measurement settings S_i.

To make it evident whether a given $\mathbf{P}$ can be described by a local realistic description, one can employ a linear function of probabilities called Bell inequality [86]. It can be written as

$$\mathcal{I}(\mathbf{P}) \equiv \sum_{\mathbf{r}_N, \mathbf{S}_N} \mu_{\mathbf{r}_N}^{\mathbf{S}_N} P(\mathbf{r}_N|\mathbf{S}_N) \leq C_{\text{LHV}}, \tag{3.4}$$

where $\{\mu_{\mathbf{r}_N}^{\mathbf{S}_N}\}$ are real coefficients and C_{LHV} refers to the upper threshold of $\mathcal{I}(\mathbf{P})$ for the local realistic description. Consequently, if one observes a value of $\mathcal{I}(\mathbf{P})$ greater than C_{LHV}, the correlations are said to be Bell nonlocal. The value of coefficients $\{\mu_{\mathbf{r}_N}^{\mathbf{S}_N}\}$ solely depends on the analysed model of local realistic description [87, 211–213]. For instance, when $N = 2$ the Bell experiment (Eq. (3.4)) is characterised by the

Clauser-Horne-Shimony-Holt (CHSH) inequality [87]. On the other hand, when $N = 3$ the genuine multipartite nonlocal correlations discussed in this Chapter require the consideration of a set of 185 Bell inequalities defined in Ref. [213].

The presence of Bell-nonlocal correlations clearly certifies the presence of entanglement, and this conclusion follows regardless of how $\mathbf{P}$ is generated from the underlying state and measurements. Therefore, Eq. (3.4) is said to be a device-independent witness for entanglement [214]. To date, the relation between entanglement and Bell nonlocality has been studied intensively. For instance, in Ref. [215] the authors showed that $\mathcal{C}(|\psi\rangle_2) = \sqrt{\beta_2^2 - 1}$, where β_2 denotes the maximal violation of the CHSH inequality [87]. Similar investigations have been performed for three-qubit states (see, for instance, [216, 217] and [218] for an experimental demonstration).

Nevertheless, the previously described demonstration of nonlocal correlations employs carefully chosen measurements the implementation of which requires the spatially separated observers to share a complete reference frame and well-calibrated devices. Although this assumption is typically made implicit in theoretical works, establishing a common reference frame, as well as aligning and calibrating measurement devices in experimental situations are never trivial tasks. Recently, Liang et al. [193] have proposed a reference-frame-independent protocol to circumvent the previously mentioned problem. In their approach, the following quantity is considered [193, 219]

$$p_{\mathrm{V}}(\rho) = \int \omega(\rho, \Omega) d\Omega, \tag{3.5}$$

where the integration comprises a space of measurement parameters Ω according to the Haar measure. The function $\omega(\rho, \Omega)$ is an indicator function that takes the value 1 whenever the generated behaviour is nonlocal and 0 otherwise. Importantly, in this approach the nonlocal correlations are quantified without any prior assumptions about specific Bell inequalities [194, 220, 221]. In other words, the generated behaviour is nonlocal if at least one inequality of the suitable set of Bell inequalities is violated. The quantity p_{V}, if properly normalised, can be interpreted as a probability of violation of local realism for the measurement operators $\hat{M}_{r_i|S_i}$ sampled randomly according to the Haar measure. To avoid confusion, we prefer to use the unique term nonlocal fraction p_{V} we prefer to use the unique term nonlocal fraction [220] to describe the quantity.

3.3 Device-Independent Estimation of Entanglement

In this work we consider a source producing copies of an unknown N-qubit state ρ_{in}, which is transmitted through randomly unitary evolving quantum channels to N local observers. During the j-th transmission the state ρ_{in} is transformed by N random local unitary operators $U_i^{(j)}$ according to

$$\rho_{\mathrm{out}} = \bigotimes_{i=1}^{N} U_i^{(j)} \rho_{\mathrm{in}} \bigotimes_{i=1}^{N} U_i^{(j)\dagger}. \tag{3.6}$$

We assume that the unitary transformation has a timescale that is sufficiently slow to obtain stable measurements for given projections together with their orthogonal counterparts, but the transformation is much faster to apply standard techniques of state analysis [222]. In other words, we can reliably accumulate signal for one particular measurement setting and its orthogonal-projection counterpart, but not for all the measurement settings in a row. As the local unitary transformations remain unknown, it is clear that a common reference frame can be established for the described scenario, nor can local devices be calibrated.

We discuss the entanglement assessment protocol of the input state ρ_{in} based on the nonlocal correlations revealed by the output state ρ_{out}. As the unitary operators during the j-th transmission remain unknown for the observers, the maximal violation of Bell inequalities cannot be determined. Instead, we estimate the nonlocal fraction which is invariant under local unitary transformations applied by each party on the state if one uses the Haar measure for the integration [220]. However, the use of the nonlocal fraction has an important disadvantage which is the lack of analytical solutions [193, 220] and, so, the numerical calculations are used to determine the nonlocal fraction.

3.3.1 Quantifying Bipartite Entanglement

Two-Qubit Werner-Like States

First, we consider the scenario when the input state is given in a form of an arbitrary two-qubit pure state $|\theta\rangle_2 = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ subjected to white noise:

$$\rho_2(\theta, v) = v\,|\theta\rangle_2\,\langle\theta| + \frac{1-v}{4}\mathbb{1}_4, \tag{3.7}$$

where $\mathbb{1}_4$ is the 4×4 identity matrix, v denotes the state visibility ($0 < v \leq 1$), and we assume without loss of generality that $0 < \theta \leq 45°$. The concurrence is given by

$$\mathcal{C}(\rho_2) \;=\; \frac{v\Big(2\sin(2\theta) + 1\Big) - 1}{2}. \tag{3.8}$$

Such states play an important role in quantum information theory as they directly refer to the states generated at the output of the nonlinear process designed in real experiments based on entangled photons [120, 223]. In this context, the white noise which enters Eq. (3.7) is a good approximation of the imperfections occurring in the experimental setup (see, for instance, [224]).

A particular example of the states in Eq. (3.7) is the two-qubit Werner state [98], $\rho_2^{\text{W}}(v) = \rho_2(\theta = 45°, v)$ [45, 199–201]. For the Werner states, concurrence depends only on the visibility, $\mathcal{C}(\rho_2^{\text{W}}) = \frac{3v-1}{2}$. Therefore, the estimation of this parameter is equivalent to the entanglement measurement.

To do that we calculate the nonlocal fraction. Note that the nonlocal correlations of two-qubit states are fully characterised by the CHSH inequality, assuming the freedom in relabelling all measurement settings and/or outcomes and/or parties [225, 226]. By straightforward calculations (see Appendix B.1) one can show that p_{V} of the Werner state is

$$p_{\text{V}}(v) = \frac{2\Big((1-v^2)\arctan\Big(\frac{\sqrt{2v^2-1}}{1-v^2}\Big) - 3\sqrt{2v^2-1}\Big)}{v^2}, \tag{3.9}$$

which is a monotonic function of v. In other words, a direct measurement of p_{V} allows the estimation of visibility and, hence, the value of the concurrence $\mathcal{C}(\rho_2^{\text{W}})$.

Naturally, for general state (Eq. (3.7)) the nonlocal fraction depends on both the visibility v and angle θ (see Fig. 3.1(a)). Although the analytical solution of p_{V} remains unknown in this case, one can always find its approximation. In particular, one can establish the visibility v by

$$v(\theta, p_{\mathrm{V}}) = v_2^{\mathrm{cr}}(\theta) + f_1(\theta)\; p_{\mathrm{V}}^{1/4} + f_2(\theta)\; p_{\mathrm{V}}^{1/2} + f_3(\theta)\; p_{\mathrm{V}}, \tag{3.10}$$

where

$$\begin{aligned} f_1(\theta) &= (0.19674 - 1.3982\;\theta + 4.712274\;\theta^2 \\ &- 6.7193\;\theta^3 + 3.3384\;\theta^4)/\sqrt{10}, \\ f_2(\theta) &= 0.11886 - 0.011544\;\theta^{-1} - 0.363104\;\theta \\ &+ 0.460436\;\theta^2 - 0.204953\;\theta^3, \\ f_3(\theta) &= (0.03848 - 0.011\;\theta^{-1} - 0.02531\;\theta \\ &- 0.018331\;\theta^2 + 0.017373\;\theta^3) \cdot 10^{-2}, \end{aligned}$$

and $v_2^{\mathrm{cr}}(\theta) = 1/\beta_2$ denotes the critical visibility with the maximal violation of the CHSH inequality $\beta_2 = (\sin^2(2\theta) + 1)^{1/2}$ [215].

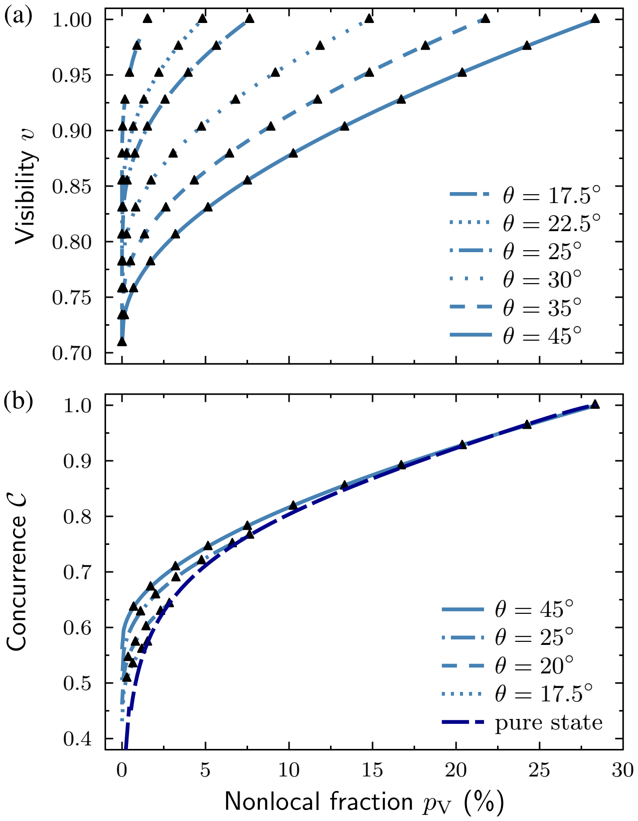


Figure 3.1: (a) Visibility and nonlocal fraction for two-qubit Werner-like states given in Eq. (3.7). Symbols denote numerical results and solid curves correspond to their analytical approximation in Eq. (3.10). (b) Relation between concurrence C and nonlocal fraction p_{V} for two-qubit Werner-like states. As previously, symbols denote numerical results while solid curves correspond to analytical approximation.

As presented in Fig. 3.1(a), this approximation provides a good agreement with our numerical results. Therefore, substituting Eq. (3.10) into Eq. (3.8) one obtains the concurrence $\mathcal{C}(\rho_2)$ depending on the angle θ and the nonlocal fraction p_{V} (see Fig. 3.1(b)). Based on these outcomes, the following remarks can be made:

(i) Whenever an observed $p_{\mathrm{V}} \geq 7\%$, the difference between $\mathcal{C}(\rho_2^{\mathrm{W}})$ and $\mathcal{C}(\rho_2)$ (hereinafter Δ_2^{W}) is no greater than 0.02 and vanishes when p_{V} increases. This means, that the concurrence $\mathcal{C}(\rho_2)$ can be estimated (with precision Δ_2^{W}) assuming that $\rho_2 \equiv \rho_2^{\mathrm{W}}$.

(ii) For $p_{\mathrm{V}} < 7\%$, remark (i) is still valid if $\theta \geq 25^{\circ}$ and $p_{\mathrm{V}} \geq 0.5\%$. In other words, the angle θ is meaningless in such a regime and the concurrence can be estimated on $\mathcal{C}(\rho_2^{\mathrm{W}})$. For other cases, the difference Δ_2^{W} increases for decreasing angle θ.

(iii) Finally, Eq. (3.10) can be used to establish the lower bound of $\mathcal{C}(\rho_2)$ versus p_{V}. Specifically, for a given value of the nonlocal fraction there exists such angle θ_0 so that the visibility $v(\theta_0, p_{\mathrm{V}}) = 1$ in Eq. (3.10). Then, the lower bound is given by $\mathcal{C}(\rho_2) \geq \sin(2\theta_0)$ and the equality is provided by the pure state $|\theta_0\rangle_2$. The lower bound can be approximated by

$$\mathcal{C}(|\theta_0\rangle_2) = \frac{0.6784}{\sqrt{10}}\, p_{\mathrm{V}}^{1/4} - 1.59 \cdot 10^{-2}\, p_{\mathrm{V}}^{1/2} + 10^{-4}\, p_{\mathrm{V}}. \tag{3.11}$$

Based on this result, one can find that the difference $\Delta_2^{\mathrm{W}} < 0.164$ for an arbitrary angle θ and $0.5\% \leq p_{\mathrm{V}} \leq 7\%$.

General Two-Qubit Mixed States

In order to present the usefulness of our entanglement-assessment protocol for a broader range of two-qubit state ρ_{in}, we now consider two examples where we apply our protocol.

Example 1: Two-qubit GHZ symmetric mixed state (GSMS) – These states represent the entire family of two-qubit mixed states with the same symmetry as the two-qubit GHZ state $|45^{\circ}\rangle_2$ [227]. For instance, the Werner states ρ_2^{W} but also the $|45^{\circ}\rangle_2$ state subjected to the local phase-damping or depolarising noise [228]. The GHZ symmetric states are defined as [227]

$$\begin{aligned}\rho_2^{\mathrm{GSMS}}(x,y) &= (\sqrt{2}y + x)\,|45^{\circ}\rangle_2\,\langle 45^{\circ}| \\ &+ (\sqrt{2}y - x)\,|{-45^{\circ}}\rangle_2\,\langle -45^{\circ}| + \frac{1-2\sqrt{2}y}{4}\mathbb{1}_2,\end{aligned}$$

where $|y| \leq (2\sqrt{2})^{-1}$ and $|x| \leq (1 + 2\sqrt{2}y)/4$. Using Eq. (3.1) one obtains the concurrence $\mathcal{C}(\rho_2^{\mathrm{GSMS}}) = \max\{0, 2|x| + \sqrt{2}y - 1/2\}$.

Next, the relation between $\mathcal{C}(x,y)$ and the nonlocal fraction for 10^4 randomly generated GSMS states has been analysed. As a result (Fig. 3.2), we find that the upper bound of such relation is provided by the Werner states $\rho_2^{\mathrm{W}} \equiv \rho_2^{\mathrm{GSMS}}(v/2, v/(2\sqrt{2}))$. The lower bound, on the other hand, is established by the maximally nonlocal mixed states, i.e., Bell diagonal states which produce a maximal value of β_2 for given concurrence [229]. These states are given by $\rho_2^{\mathrm{PhN}}(x) = \frac{1+2x}{2}\,|45^{\circ}\rangle_2\,\langle 45^{\circ}| + \frac{1-2x}{2}\,|{-45^{\circ}}\rangle_2\,\langle -45^{\circ}|$, and describe the $|45^{\circ}\rangle_2$ state subjected to the local phase-damping noise [228]. The relation between the concurrence and the nonlocal fraction in this case is given by $\mathcal{C}(\rho_2^{\mathrm{PhN}}) = \mathcal{C}(|\theta_0\rangle_2)$ written in Eq. (3.11). Therefore, if one knows the nonlocal fraction of an arbitrary GHZ symmetric state, then its concurrence is limited by $\mathcal{C}(|\theta_0\rangle_2) \leq \mathcal{C}(\rho_2^{\mathrm{GSMS}}) \leq \mathcal{C}(\rho_2^{\mathrm{W}})$. This limitation is of great importance if remarks (i)–(iii) are taken into account. That is, the concurrence of an arbitrary GHZ symmetric state can be determined with accuracy not greater than Δ_2^{W} if the measured $p_{\mathrm{V}} \geq 7\%$. Note that, in general, the GSMS may

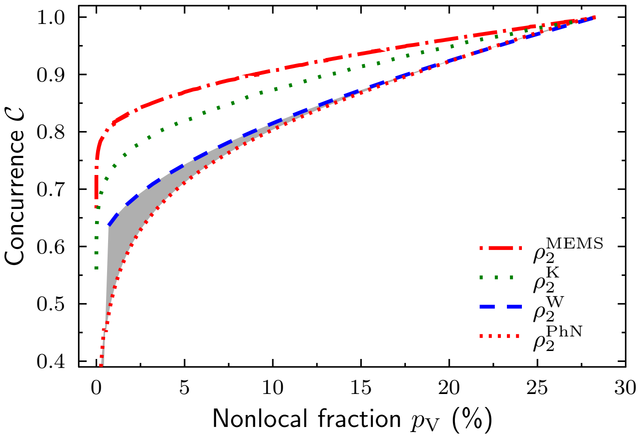


Figure 3.2: The region of possible values of concurrence for given nonlocal fraction. The grey region corresponds to two-qubit GHZ symmetric mixed states and the four curves represent maximally entangled mixed states (red dashed-dotted curve), Kagalwala states [230] (green dotted curve), Werner states (blue dashed curve), two-qubit GHZ state subjected to the local phase-damping noise (red dotted curve).

denote the experimentally generated state $|45°\rangle_2$ subjected to an unknown source of noise if such noise does not change the symmetry of the input state.

Example 2: Maximally entangled mixed state (MEMS) – As a final example we consider the states which maximise the value of the concurrence for a given value of the violation of the CHSH inequality [231, 232]

$$\rho_2^{\rm MEMS}(\gamma) \;\; = \;\; \gamma\,|45°\rangle_2\,\langle 45°| + (1-\gamma)\,|01\rangle\,\langle 01|\,,$$

where $\frac{2}{3} \leq \gamma \leq 1$. Based on numerical calculation we have found that

$$\begin{aligned} \mathcal{C}(\rho_2^{\rm MEMS}) \;\; &= \;\; 1/\sqrt{2} + 0.1125/\sqrt{10}\; p_{\rm V}^{1/4} - 9.0\cdot 10^{-4}\; p_{\rm V}^{1/2} \\ &+ \;\; 2.83\cdot 10^{-5}\; p_{\rm V}. \end{aligned}$$

As we show in Fig. 3.2, the concurrence $\mathcal{C}(\rho_2^{\rm MEMS})$ exceeds $\mathcal{C}(\rho_2^{\rm W})$ in the entire range of $p_{\rm V}$. However, the difference between these two quantities is not greater that 0.173.

Finally, our numerical calculations performed for randomly generated two-qubit mixed states ρ always satisfied the relation

$$\mathcal{C}(|\theta_0\rangle_2) \leq \mathcal{C}(\rho) \leq \mathcal{C}(\rho_2^{\rm MEMS}), \qquad (3.12)$$

if they reveal the same value of $p_{\rm V}$. Therefore, we conjecture that the MEMS and pure states $|\theta\rangle_2$ provide an upper and lower limit for $\mathcal{C}(\rho)$ versus $p_{\rm V}$ for two-qubit states.

3.3.2 Quantifying Genuine Tripartite Entanglement

Three-Qubit Werner-Like States

Now we proceed to estimate the genuine multipartite entanglement. We follow the same procedure as before, that is, we analyse the relationship between the GME-concurrence and nonlocal fraction. First, we concentrate on the three-qubit Werner-like states which serve as a benchmark for the robustness of multipartite entanglement [233]

$$\rho_3(\theta, v) = v\,|\theta\rangle_3\,\langle\theta| + \frac{1-v}{8}\mathbb{1}_8, \qquad (3.13)$$

where $|\theta\rangle_3 = \cos\theta\,|000\rangle + \sin\theta\,|111\rangle$ is the generalised GHZ state (gGHZ) and $\mathbb{1}_8$ is the 8×8 identity matrix denoting the presence of white noise. As previously, v denotes the state visibility ($0 < v \leq 1$) and we assume $0 < \theta \leq 45°$. Using Eq. (3.3) one can find the GME-concurrence as

$$\mathcal{C}_{\text{GME}}(\rho_3) \;=\; \frac{\Big(3\sin(2\theta)+2\Big)v-2}{3}. \tag{3.14}$$

In order to certify the GME, we estimate the nonlocal fraction for the genuine multipartite nonlocal correlations. Such an estimation requires testing all 185 families of Bell inequalities (see [194]). As a result (Fig. 3.3(a)), we find that the visibility v in Eq. (3.13) can be approximated by p_{V} using

$$v(\theta, p_{\text{V}}) = v_3^{\text{cr}}(\theta) + g_1(\theta)\; p_{\text{V}}^{1/6} + g_2(\theta)\; p_{\text{V}}^{1/2} + g_3(\theta)\; p_{\text{V}}, \tag{3.15}$$

where the critical visibility $v_3^{\text{cr}}(\theta) = 1/\beta_3$ and

$$\beta_3 = \begin{cases} 1 + 0.0622\theta + 1.697\theta^2 & \text{for } 0 \leq \theta < 14.94° \\ -3.391\theta^3 + 1.442\theta^4 & \\ \left(1 + 2\sqrt{1+\sin^2(2\theta)}\right)/3 & \text{for } 14.94° \leq \theta < 29.5° \\ \sqrt{2\sin^2(2\theta)} & \text{for } 29.5° \leq \theta < 45° \end{cases}$$

is the maximal strength of Bell-nonlocality for three-qubit Werner-like states (see [42]). The other functions which enter Eq. (3.15) are given by

$$\begin{aligned} g_1(\theta) &= \max\{-0.061297 + 0.55512\;\theta - 0.42815\;\theta^2, \\ &\quad -18.58393 + 57.9917\;\sqrt{\theta} - 50.2727\;\theta \\ &\quad +11.209\;\theta^2\}/10^{1/3}, \\ g_2(\theta) &= \min\{0{,}0.76306 - 4.13852\;\theta + 8.28077\;\theta^2 \\ &\quad -7.2943\;\theta^3 + 2.38884\;\theta^4\}, \\ g_3(\theta) &= \max\{0.0001151 - 0.0004063\;\theta + 0.0004321\;\theta^2, \\ &\quad -0.015237 + 0.084803\;\theta - 0.17408\;\theta^2 \\ &\quad +0.15723\;\theta^3 - 0.052804\;\theta^4\}. \end{aligned}$$

Based on Eq. (3.14) and (3.15), the GME concurrence has been obtained as a function of p_{V}. As we see in Fig. 3.3(b), in contrast to $\rho_2(\theta, v)$, here the angle θ is meaningful in the entire range of attainable p_{V}. For instance, if one takes $\theta_1 = 45°$ (i.e., the three-qubit Werner state) and $\theta_2 = 35°$, the GME concurrence is explicitly written as

$$\begin{aligned} \mathcal{C}_{\text{GME}}(\theta_1) &= 0.512 + 0.186\; p_{\text{V}}^{1/6} - 7.1 \cdot 10^{-3}\; p_{\text{V}}^{1/2} \\ &\quad +1.12 \cdot 10^{-4}\; p_{\text{V}}, \\ \mathcal{C}_{\text{GME}}(\theta_2) &= 0.542 + 0.155\; p_{\text{V}}^{1/6} - 8.2 \cdot 10^{-3}\; p_{\text{V}}^{1/2} \\ &\quad +1.52 \cdot 10^{-4}\; p_{\text{V}}. \end{aligned} \tag{3.16}$$

Using these equations one can easily find the difference $\Delta_3^{\text{W}} = \mathcal{C}_{\text{GME}}(\theta_1) - \mathcal{C}_{\text{GME}}(\theta_2)$ belongs to $(0.032, 0.048)$ when $p_{\text{V}} > 1\%$. Therefore, in order to establish GME concurrence $\mathcal{C}_{\text{GME}}(\rho_3)$, we need to evaluate not only the value of p_{V} but also the underlying angle θ. Without prior knowledge of the angle θ, its value can be determined from the distribution of the strength of violation for random measurements (Appendix B.2). This requires the accumulation of data on the strength of violation of local realism for a sequence of randomly chosen measurements. In a typical experimental investigation of p_V [93, 194, 221], such a set is known without any additional effort and, hence, one can establish the value of GME concurrence.

On the other hand, by inserting $v(\theta, p_\mathrm{V}) = 1$ into Eq. (3.15) one can derive the GME concurrence for pure states $|\theta\rangle_3$. It can be approximated by [194]

$$\mathcal{C}_\mathrm{GME}(|\theta\rangle_3) \;=\; \left(0.068\; p_\mathrm{V} + 0.06\; p_\mathrm{V}^{1/2}\right)^{1/2}, \tag{3.17}$$

which denotes the lower bound of $\mathcal{C}_\mathrm{GME}(\rho_3)$ with given p_V.

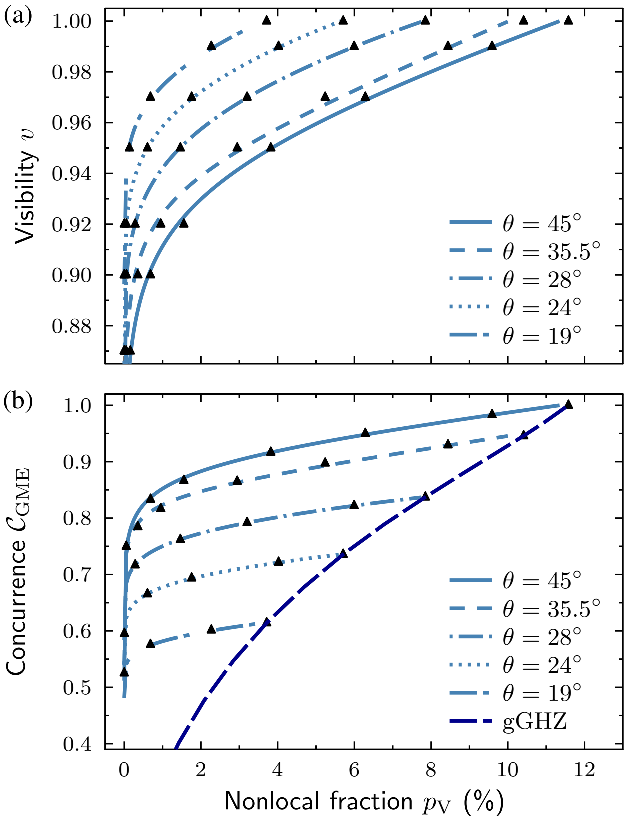


Figure 3.3: (a) Visibility and nonlocal fraction for three-qubit Werner-like states given in Eq. (3.13). Symbols denote numerical results and solid curves correspond to their analytical approximation in Eq. (3.15). (b) Relation between genuine concurrence $\mathcal{C}_\mathrm{GME}$ and nonlocal fraction p_V for three-qubit Werner-like states. As previously, symbols denote numerical results whereas solid curves correspond to analytical approximation.

Other Examples of States

We note that the general analysis of the three-qubit mixed states is beyond the scope of our research, as there is no general analytical formula of the genuine concurrence. Therefore, we examine a few examples which illustrate the usefulness of our approach.

Example 3: Three-qubit GHZ symmetric mixed state (GSMS) – A natural extension of the three-qubit Werner-like states is the family of GHZ symmetric states. In the three-qubit case, they are given by

$$\begin{aligned}\rho_3^{\mathrm{GSMS}}(x,y) &= \left(\frac{2\sqrt{3}}{3}y+x\right)|45°\rangle_3\langle 45°| \\ &+\left(\frac{2\sqrt{3}}{3}y \;-\; x\right)|{-45°}\rangle_3\langle{-45°}|+\frac{3-4\sqrt{3}y}{24}\mathbb{1}_8,\end{aligned} \tag{3.18}$$

where $\frac{-1}{4\sqrt{3}} \leq y \leq \frac{\sqrt{3}}{4}$, $|x| \leq (1+4\sqrt{3}y)/8$ and the GME concurrence $\mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{GSMS}}) = \max\{0, 2|x|+\sqrt{3}y-3/4\}$.

For these states, similar remarks can be drawn as in *Example 1.* Specifically, the upper bound of the GME concurrence for a given value of p_{V} is provided by the three-qubit Werner state ρ_3^{W} (Fig. 3.4). The lower bound is observed for $\rho_3^{\mathrm{PhN}}(x) = \left(\frac{1}{2}+x\right)|45°\rangle_3\langle 45°| + \left(\frac{1}{2}-x\right)|{-45°}\rangle_3\langle{-45°}|$, i.e., the GHZ state subjected to the local phase-damping noise [228]. The GME concurrence is approximated by:

$$\mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{PhN}}) = 0.4012\, p_{\mathrm{V}}^{1/6} - 0.0118\, p_{\mathrm{V}}^{1/2} + 9.0\cdot 10^{-5}\, p_{\mathrm{V}},$$

and, hence, the difference $\Delta_3^{\mathrm{W}} \leq 0.14$. Interestingly, results obtained for ρ_3^{PhN} are significantly different with respect to those of $|\theta\rangle_3$, as opposed to the case of two-qubit states. In summary, for all ρ_3^{GSMS} states, the following relation is observed

$$\mathcal{C}_{\mathrm{GME}}(|\theta\rangle_3) < \mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{PhN}}) \leq \mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{GSMS}}) \leq \mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{W}}),$$

where we assume that each state reveals the same value of the nonlocal fraction.

Example 4: GHZ state under the amplitude-damping noise (AD) – Let us recall that the GHZ-symmetric states describe two basic examples of the noisy GHZ state, that is, affected by local phase-damping and depolarising noise. Here we investigate another important example, namely the GHZ state subjected to the local amplitude-damping noise [228]

$$\rho_3^{\mathrm{AD}}(\alpha) = \sum_{i,j,k=1}^{2} \mathcal{K}_{i,j,k}(\alpha)\,|45°\rangle_3\langle 45°|\,\mathcal{K}_{i,j,k}^{\dagger}(\alpha), \tag{3.19}$$

where $\mathcal{K}_{i,j,k}(\alpha) = \mathcal{K}_i(\alpha)\otimes\mathcal{K}_j(\alpha)\otimes\mathcal{K}_k(\alpha)$ denotes the tensor product of the appropriate Kraus operators [228] and $0 \leq \alpha \leq 1$. Our calculations reveal that the genuine concurrence $\mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{AD}}) \geq \mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{W}})$ in the entire range of p_{V} (Fig. 3.4). Furthermore, the calculation has been repeated for the bit flip noise, providing results slightly smaller than these of the Werner states. This means that if the GHZ state is transmitted via one of the basic quantum channels (unknown in principle), then the genuine concurrence of the output state is greater than or equal to that of ρ_3^{PhN}.

Example 5: Three-qubit pure states – Finally, we analyse the relationship between the genuine concurrence and the nonlocal fraction for other examples of three-qubit pure state that are important for quantum communication protocols [234], namely the tetrahedral (T) states [217, 235], the generalised W states [236], and the maximal slice (MS) states [237]

$$\begin{aligned}|\psi_{\mathrm{T}}\rangle &= t_0\left(|001\rangle+|010\rangle+|100\rangle\right)+\sqrt{1-3t_0^2}\,|111\rangle\,, \\ |\psi_{\mathrm{W}}\rangle &= \frac{w_0}{\sqrt{2}}\left(|001\rangle+|010\rangle\right)+w_1\,|100\rangle\,, \\ |\psi_{\mathrm{MS}}\rangle &= \frac{1}{\sqrt{2}}\left(|000\rangle+m_0\,|110\rangle+m_1\,|111\rangle\right), \end{aligned} \tag{3.20}$$

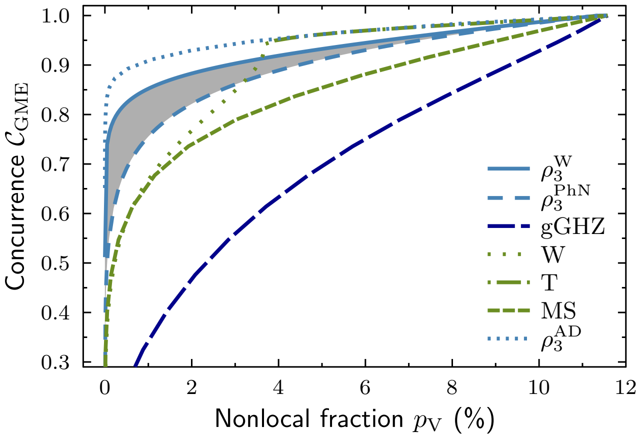


Figure 3.4: The region of possible values of genuine concurrence for given nonlocal fraction. The grey region corresponds to three-qubit GHZ symmetric mixed states and the four blue curves represent Werner states (solid curve), three-qubit GHZ state subjected to the local phase-damping noise (short dashed curve), three-qubit GHZ state subjected to the local amplitude-damping noise (dotted curve), and generalised GHZ states (blue dashed curve). Furthermore, the three green curves show the tetrahedral states (dot-dashed curve), generalised W states (dotted curve), and maximal slice states (short dashed curve).

where the standard normalisation condition is assumed. As we show in Fig. 3.4 in all these cases the relationship between the genuine concurrence and the nonlocal fraction satisfy the relation

$$\mathcal{C}_{\mathrm{GME}}(|\theta\rangle_3) < \mathcal{C}_{\mathrm{GME}}(|\psi_{\mathrm{T,W,MS}}\rangle) \leq \mathcal{C}_{\mathrm{GME}}(\rho_3^{\mathrm{AD}}).$$

In other words, if one assumes that the state under the question remains unknown, then its genuine concurrence can be estimated from the bottom using $\mathcal{C}_{\mathrm{GME}}(|\theta\rangle_3)$.

3.4 Experimental Implementation

3.4.1 Experimental Setup

We have constructed the experimental setup depicted in Fig. 3.5 to produce and characterise three-qubit states. Our experiment is implemented on the platform of linear optics and it encodes qubits into spatial and polarisation states of single photons. The setup utilises entangled photon pairs generated using Type-I parametric down-conversion in a β-BBO crystal cascade (referred to as Kwiat source [121]) at $\lambda = 710$ nm. A laser beam of a wavelength of $\lambda = 355$ nm pumps two identically cut non-linear crystals, with optical axis in mutually perpendicular planes defining horizontal and vertical basis. If pumped by horizontally (vertically) polarised pump beam, pairs of vertically (horizontally) polarised photons are generated. By setting half-wave plate HWP$_{\mathrm{Z}}$ at angle $\frac{\theta}{2}$ both crystals are coherently pumped and generate photons in a state of the form of

$$\cos\theta\,|HH\rangle + \sin\theta\,|VV\rangle\ . \tag{3.21}$$

The first (second) position in the ket stands for polarisation of the first (second) photon, respectively. Probability of generating two pairs simultaneously is negligible.

In order to generate the three-qubit states, we incorporate spatial mode encoding to be used in addition to polarisation encoding. For this purpose, the first photon is

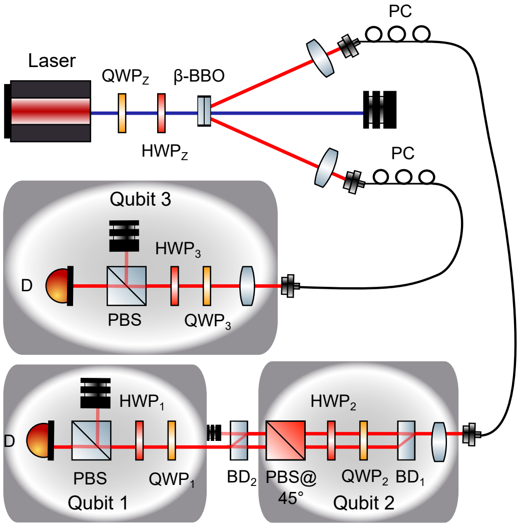


Figure 3.5: Experimental setup. Legend: PBS – polarisation beam splitter, BD – beam displacer, PC – polarisation controller, β-BBO – non-linear crystal β-barium borate, D – detector, HWP – half-wave plate, QWP – quarter wave-plate.

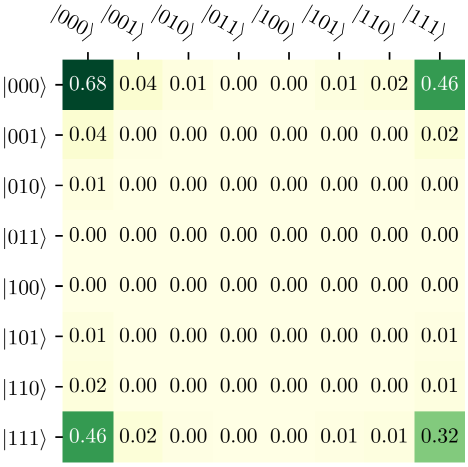
subjected to the beam displacer (BD$_1$). Here BD$_1$ deviates vertically polarised photons upwards whereas horizontally polarised photons continue straightforward. Therefore, one can denote by $|0\rangle$ ($|1\rangle$) spatial mode of photons in the upper (lower) arm. At the same time by associating H (V) polarisation with logical states $|0\rangle$ ($|1\rangle$) one can immediately identify that by the action of BD$_1$ the original two-qubit state (3.21) becomes a generalised GHZ state in its canonical form

$$|\theta\rangle_3 = \cos\theta\,|000\rangle + \sin\theta\,|111\rangle\ . \tag{3.22}$$

Here the first qubit in the ket denotes first photon's spatial mode and second (third) qubit stands for first (second) photon's polarisation state.

Having the desired state prepared, all 3 qubits are subjected to local projections (hereafter $|\hat{\Pi}_1 \otimes \hat{\Pi}_2 \otimes \hat{\Pi}_3\rangle$). The third qubit is projected simply by using a combination of quarter and half wave plates (QWP$_3$ and HWP$_3$) accompanied by polarising beam splitter (PBS). The remaining two qubits are encoded into the spatial and polarisation state of the first photon. Using a similar sequence (QWP$_2$, HWP$_2$ and PBS) spreading over both spatial modes of this photon, we achieve projection of the second qubit. At this stage, a BD$_2$ is used to convert the spatial encoding of the first qubit to polarisation encoding. Once polarisationally encoded, the sequence of QWP$_1$, HWP$_1$ and PBS is used to perform first qubit's projection. At the end of the setup, both photons are led to single-photon detectors and the rate of coincident detections is measured for every projection setting.

For the purposes of this experiment, we require the setup to prepare and characterise all pure computational basis states, i.e., $|\text{basis}\rangle = \{|000\rangle\,,\ |001\rangle\,,\ldots,\ |111\rangle\}$. This is simply achieved by setting $\theta = 0°$ resulting in generation of the $|000\rangle$ state and imposing single-qubit NOT gates in the modes where the qubit is required in the $|1\rangle$ state. These NOT gates are implemented by adding a 45° bias to the HWP associated with this qubit. All these states were later used to synthesise white noise. Then, various quasi-pure GHZ states were also prepared. All experimental data accumulated in this experiment are available on CD-ROM (see Appendix E) enclosed with the printed version of this Thesis.



	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
$\|000\rangle$	0.68	0.04	0.01	0.00	0.00	0.01	0.02	0.46
$\|001\rangle$	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.02
$\|010\rangle$	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00
$\|011\rangle$	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
$\|100\rangle$	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
$\|101\rangle$	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.01
$\|110\rangle$	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.01
$\|111\rangle$	0.46	0.02	0.00	0.00	0.00	0.01	0.01	0.32

Figure 3.6: Visualisation of the real part of the density matrix ρ^{expt} $\theta = 35°$. All values of the imaginary part of ρ^{expt} are less than 0.025.

The experiment is carried out in three steps. First, we generate the desired gGHZ states and verify their quality using standard state tomography (Sec. 3.4.2). For such verification, it is necessary to align the reference frame. Having the reconstructed density matrix, one can estimate experimental imperfections and also test the concept of nonlocal fraction by simulating 10^8 random projections imposed to this matrix. The second experimental step is the truly RFI scenario involving 8000 random projections directly imposed to the generated photons. This constitutes the main result of this Chapter (Sec. 3.4.3). Finally, in Sec. 3.4.4, we also perform experimental estimation of GME concurrence measurement on arbitrarily mixed Werner states by adding white noise as explained previously.

3.4.2 Nonlocal Fraction Measurements - Aligned Reference Frames

First, we consider a scenario when the observers share common reference frames. The experimental setup has been adjusted in such a way to generate the gGHZ states, $|\theta\rangle_3$, for two different angles accounting for 35° and 45°. Note that the later case denotes the prototype GHZ state. For each adjustment of θ, the output-state density matrix, $\rho_\theta^{\text{expt}} \equiv \rho_3^{\text{expt}}(\theta)$, is reconstructed by evaluating the quantum state tomography and maximum-likelihood estimation [132, 238]. An exemplary result is shown in Fig. 3.6. Then, we determined the fidelity F of $\rho_\theta^{\text{expt}}$ with respect to the ideal pure state $|\theta\rangle_3$, $F(\rho_\theta^{\text{expt}}) = \text{Tr}(\rho_\theta^{\text{expt}}|\theta\rangle_3\langle\theta|)$. As a result, we find that $F(\rho_\theta^{\text{expt}})$ is always greater than 0.980 ± 0.002 for all values of θ confirming the good quality of our source. The uncertainty of the fidelity has been determined by Monte Carlo simulations of Poissonian noise distribution.

The fact that $F(\rho_\theta^{\text{expt}}) < 1$ is naturally caused by the presence of experimental imperfections such as the improper setting of individual components or depolarisation effects. Consequently, an effective form of the generated state should be considered as the three-qubit Werner-like state $\rho_3(\theta, v_\theta)$ in Eq. (3.13), where v_θ is associated with the strength of the effective noise inherently present during the experiment. The presence of such noise is certified by a reduction in purity, $P(\rho) = \text{Tr}(\rho^2)$, of the output state. By straightforward calculations we have found that $P(\rho^{\text{expt}}_{35^\circ}) = 0.982 \pm 0.005$ and $P(\rho^{\text{expt}}_{45^\circ}) = 0.976 \pm 0.005$. Then, using the relation $P(\rho) = \frac{1+7v_0^2}{8}$ [95] the visibility v_0 has been estimated. In our case the visibility is equal to $v_{35^\circ} = 0.990 \pm 0.003$ and $v_{45^\circ} = 0.986 \pm 0.003$. These values are further utilised to establish an appropriate reference point of theoretical predictions.

Next, using the reconstructed output state, $\rho^{\text{expt}}_\theta$, and numerical procedure described in Sec. 3.2.2, the nonlocal fraction has been evaluated

$$\begin{aligned} p_{\mathrm{V}}(\rho^{\text{expt}}_{45^\circ}) &= 9.0 \pm 0.9\%, \\ p_{\mathrm{V}}(\rho^{\text{expt}}_{35^\circ}) &= 8.2 \pm 0.7\%. \end{aligned} \tag{3.23}$$

For each state 10^8 different settings have been examined numerically. Although the density matrix was obtained via tomography in an aligned reference frame scenario, processing of probabilities corresponding to these random projection settings is identical to the RFI situation. Comparing these results with theoretical prediction, $p_{\mathrm{V}}(45^\circ, v_{45^\circ}) = 8.830\%$ and $p_{\mathrm{V}}(35^\circ, v_{35^\circ}) = 8.279\%$, we see a very good agreement between both sets of outcomes.

3.4.3 Nonlocal Fraction Measurements - Reference Frames Independent Approach

In the second step, we relax the experimental requirements and consider the reference-frame-independent approach. In this case, all three qubits of the desired $\rho^{\text{expt}}_\theta$ state are subjected to randomly chosen local projections $|\hat{\Pi}_1 \otimes \hat{\Pi}_2 \otimes \hat{\Pi}_3\rangle$. Note that, by the definition of the nonlocal fraction, their actual value is not important and, so, there is no need to calibrate the experimental devices. The whole process includes $n = 8000$ projection settings. For each adjustment of θ and $|\hat{\Pi}_1 \otimes \hat{\Pi}_2 \otimes \hat{\Pi}_3\rangle$, we measure coincidence detections (CC) over approximately 20 s and we registered one value of CC per projection. The values of CC are used to determine all correlation coefficient (see [95, 194]) and, then, to test all 185 Bell inequalities relevant for the genuine multipartite nonlocal correlations [213]. Note that in this test all possible relabelling of parties, inputs, and outputs has been taken into account. The value of the Bell inequality is determined with precision ±0.015. Dividing the number of projection setting which provide violation of local realism by the total number of setting n, the nonlocal fraction has been estimated. We obtain the following results:

$$\begin{aligned} p^{\mathrm{CC}}_{\mathrm{V}}(45^\circ) &= 8.6 \pm 1.6\%, \\ p^{\mathrm{CC}}_{\mathrm{V}}(35^\circ) &= 8.7 \pm 1.2\%. \end{aligned} \tag{3.24}$$

As we show in Fig. 3.7, our results in Eq. (3.24) match correctly to the attainable range of theoretical predictions if the precision of v_0 is included. Specifically, for the error bar of v_0 equal to ± 0.003, one obtains $8.302\% \leq p_{\mathrm{V}}(45^\circ, v_{45^\circ}) \leq 9.377\%$ and $7.735\% \leq p_{\mathrm{V}}(35^\circ, v_{35^\circ}) \leq 8.848\%$. However, the values of $p^{\mathrm{CC}}_{\mathrm{V}}(\theta)$ slightly differ from $p_{\mathrm{V}}(\rho^{\text{expt}}_\theta)$ in Eq. (3.23). In particular, $p^{\mathrm{CC}}_{\mathrm{V}}(45^\circ) < p^{\mathrm{CC}}_{\mathrm{V}}(35^\circ)$. To explain such difference, we emphasise that owing to inherent experimental fluctuation, the generated state slightly varies over the course of the entire data acquisition time (about two days). For that reason, one may expect some fluctuations of the inherent noise arising due to, e.g., dephasing and depolarisation.

In order to verify this conclusion, the distribution of the strength of violation for random measurements has been analysed. In other words, we simulate a robustness of

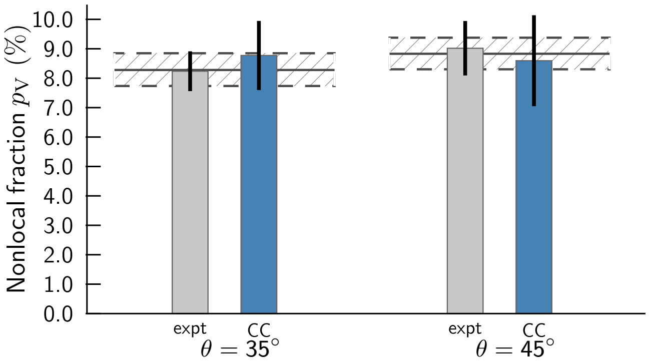


Figure 3.7: Comparison of the nonlocal fraction estimated for the reconstructed density matrix $p_{\mathrm{V}}(\rho_\theta^{\mathrm{expt}})$ (gray bar) and measured coincidence detections $p_{\mathrm{V}}^{\mathrm{CC}}(\theta)$ (blue bar) for angle $\theta = 35°, 45°$. Horizontal hatched areas show theoretical predictions, solid lines correspond to $p_{\mathrm{V}}(\theta, v_\theta)$, and dashes lines denote $p_{\mathrm{V}}(\theta, v_\theta \pm 0.03)$.

the nonlocal fraction $p_{\mathrm{V}}^{\mathrm{CC}}$ using the accumulated data for random sampling. As we see in Fig. 3.8, for both values of angle θ the simulated relationship between $p_{\mathrm{V}}^{\mathrm{CC}}$ and $\mathcal{I}_{\min}$ has a similar shape as its theoretical counterpart (see Appendix B.2). Furthermore, by fitting our experimental data with Eq. (B7) we have found the following results $\{\theta,\ v_{45°}\} \approx \{44.7°,\ 0.984\}$ and $\{\theta,\ v_{35°}\} \approx \{36.0°,\ 0.996\}$ which is in line with our previous observations. Note that these fitted values are sufficient to establish the GME concurrence using Eq. (3.14) without prior knowledge about the generated state.

3.4.4 Genuine Concurrence Measure - Reference-Frame-Independent Approach

The final stage of our experiment is to measure the GME concurrence for the Werner-like states. In order to do that, the Werner-like states $\rho_3^{\mathrm{expt}}(\theta, v)$ were synthesised with controlled visibility v in the range $[0.9;\ v_\theta]$. This is accomplished by controlled mixing (with probability v_{c}) the output state $\rho_\theta^{\mathrm{expt}}$ and white noise, i.e., $v_{\mathrm{c}}\rho_\theta^{\mathrm{expt}} + (1 - v_{\mathrm{c}})\rho_{\text{white noise}}$. As a result, one has

$$\begin{aligned} \rho_3^{\mathrm{expt}}(\theta,v) &= v_{\mathrm{c}} v_\theta\ |\theta\rangle_3 \langle\theta| + \\ &+ \sum_{\text{basis}} \frac{1 - v_{\mathrm{c}} v_\theta}{8} |\text{basis}\rangle \langle\text{basis}|\,, \end{aligned} \tag{3.25}$$

where the total visibility $v \equiv v_{\mathrm{c}} v_\theta$ with v_θ being a constant value defined above and controlled parameter v_{c} varying with a step $\delta_{\mathrm{v}} = 0.01$.

Now, to synthesise projection results CC for any mixed state in Eq. (3.25), the experimental setup was set to gradually generate 8 basis states $|\text{basis}\rangle$. Similarly as in Sec. 3.4.3, each of the states is subjected to the same set of random projections $|\hat{\Pi}_1 \otimes \hat{\Pi}_2 \otimes \hat{\Pi}_3\rangle$ as those of ρ^{expt} (including tomography projections). Finally, values of CC are probabilistically mixed according to the following routine (Fig. 3.9)

$$CC_i(\theta, v) = v_{\mathrm{c}}\, CC_i(\rho_\theta^{\mathrm{expt}}) + \sum_{\text{basis}} \frac{1 - v_{\mathrm{c}}}{8} CC_i(|\text{basis}\rangle), \tag{3.26}$$

where $CC_i(\theta, v) \equiv CC_i(\rho_3^{\mathrm{expt}}(\theta, v))$ and $CC_i(\rho)$ denotes the values of CC for the state ρ and the i-th projector $|\hat{\Pi}_1^{(i)} \otimes \hat{\Pi}_2^{(i)} \otimes \hat{\Pi}_3^{(i)}\rangle$. This procedure results in 8000 values of

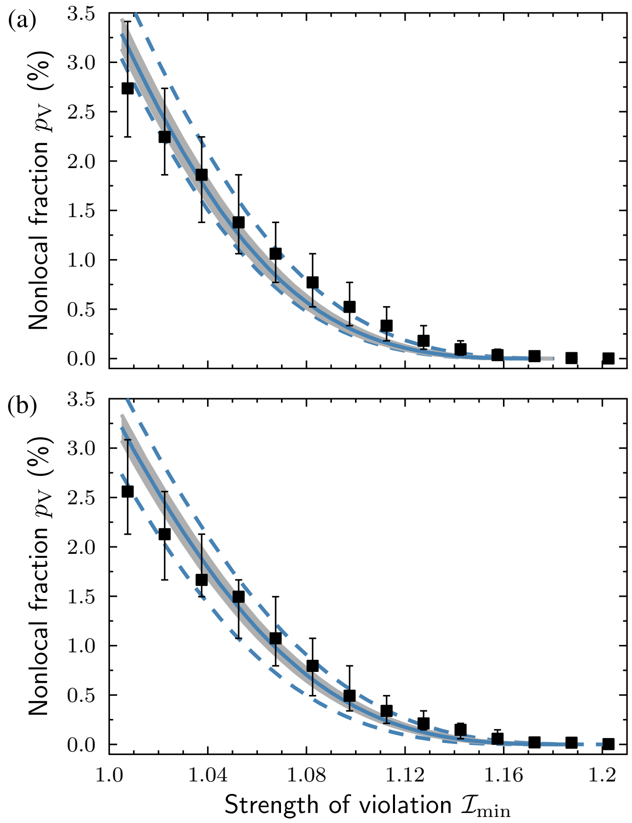
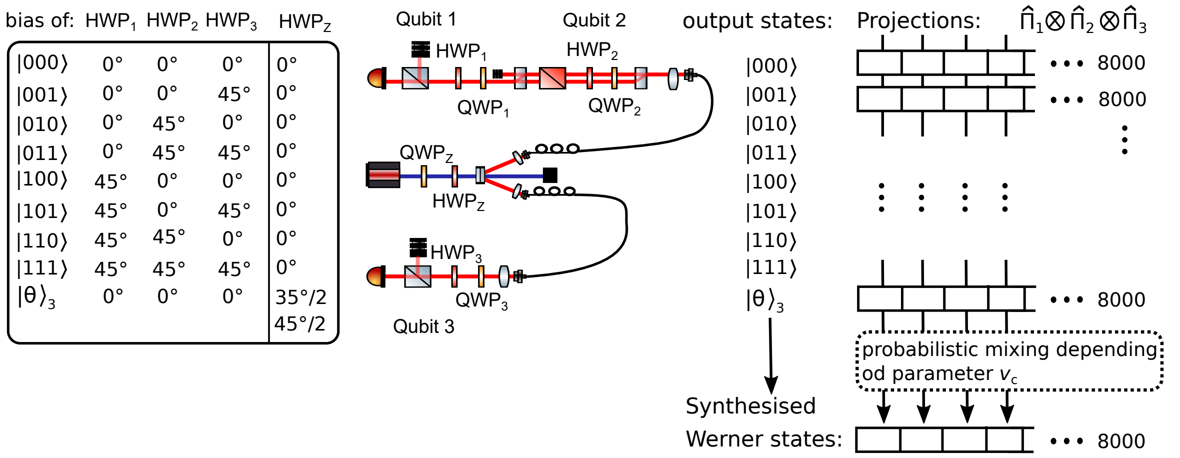


Figure 3.8: Distribution of the strength of violation for randomly sampled measurements for (a) $\theta = 35°$ and (b) $\theta = 45°$. In both panels, symbols denote experimental results whereas gray areas depict theoretical predictions for $\rho_3(\theta, v_\theta \pm 0.003)$. Dashed lines correspond to theoretical calculations for (a) $\rho_3(35°, 1)$ and $\rho_3(35°, 0.985)$ (b) $\rho_3(45°, 0.990)$ and $\rho_3(45°, 0.975)$.



bias of:	HWP$_1$	HWP$_2$	HWP$_3$	HWP$_Z$
$\|000\rangle$	0°	0°	0°	0°
$\|001\rangle$	0°	0°	45°	0°
$\|010\rangle$	0°	45°	0°	0°
$\|011\rangle$	0°	45°	45°	0°
$\|100\rangle$	45°	0°	0°	0°
$\|101\rangle$	45°	0°	45°	0°
$\|110\rangle$	45°	45°	0°	0°
$\|111\rangle$	45°	45°	45°	0°
$\|\theta\rangle_3$	0°	0°	0°	35°/2 45°/2

Figure 3.9: Scheme of the synthesising procedure for all 8 000 random projections $|\hat{\Pi}_1 \otimes \hat{\Pi}_2 \otimes \hat{\Pi}_3\rangle$. On the left-hand side of this scheme we provide HWP settings for each three-qubit state. The final state $\hat{\rho}_{\mathrm{W}}$ is mixed according to a prescription given in Eq. (3.25).

CC for each generated state $\rho_3^{\text{expt}}(\theta, v)$ that can be further analysed. Note that for every state, all CC_i are normalised with respect to the overall generation rate for the particular state.

Based on these results, the nonlocal fraction of $\rho_3^{\text{expt}}(\theta, v)$ has been determined. As we see in Fig. 3.10(a), our measurements are in good agreement with theoretical predictions given in Eq. (3.15). Finally, using Eq. (3.16) the GME concurrence for the Werner-like states has been established and the accomplished results are in perfect agreement with theory (Fig. 3.10(b)). Specifically, for the exemplary states discussed in previous subsections, we obtain

$$\begin{aligned} \mathcal{C}_{\text{GME}}(45^\circ) &= 0.97 \pm 0.01, \\ \mathcal{C}_{\text{GME}}(35^\circ) &= 0.93 \pm 0.01, \end{aligned} \tag{3.27}$$

whereas theoretical predictions yield $\mathcal{C}_{\text{GME}}(45^\circ, v_{45^\circ}) = 0.977$ and $\mathcal{C}_{\text{GME}}(45^\circ, v_{45^\circ}) = 0.924$.

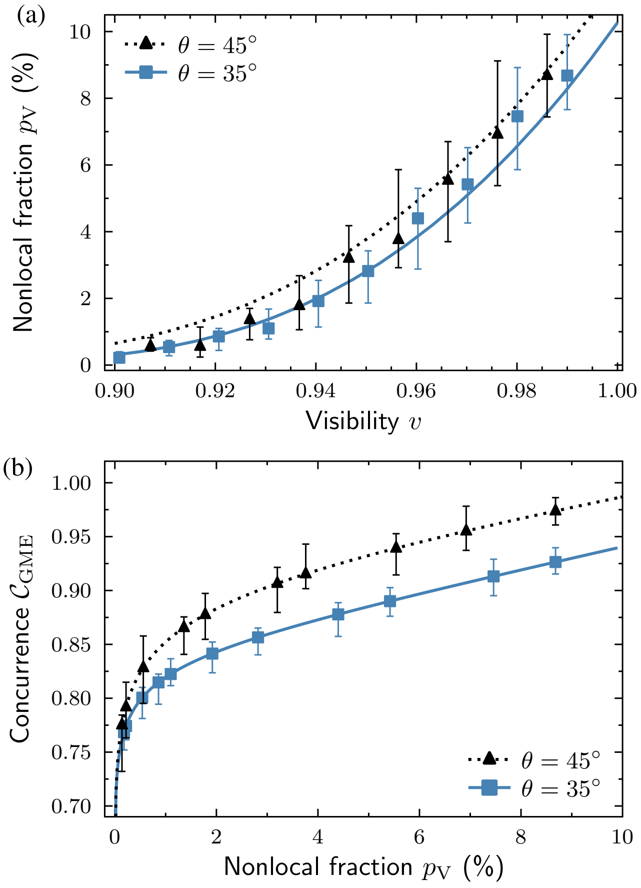


Figure 3.10: (a) Dependence of the nonlocal fraction on the visibility and (b) the relation between genuine concurrence and nonlocal fraction for three-qubit Werner-like states. In both panels, symbols denote experimental measurements for $\theta = 35^\circ$ (triangles) and $\theta = 45^\circ$ (squares) while curves depict theoretical predictions.

3.5 Conclusions

In conclusion, we have theoretically and experimentally investigated the entanglement-assessment protocol for two- and three-qubit Werner-like states. Our proposal is based on the concept of the nonlocal fraction which denotes the probability of detection of nonlocal correlation under random measurements. Using numerical calculations, we have found the relationship between the degree of entanglement and nonlocal fraction. Then, our method has been successfully applied to the experimental measurements of the GME concurrence of the three-qubit Werner-like state, revealing perfect agreement with theoretical predictions.

The advantage of using random sampling in our protocol is a great simplification of experimental procedures as the alignment and calibration of remote devices are no longer necessary. Therefore, our protocol can be applied in an unstable environment, where the previously mentioned requirements are hard to meet.

Although in this Chapter we focus on the Werner-like states, our protocol can also be used for an arbitrary mixed state. In this broader context, the protocol can operate as an indicator of a lower bound of entanglement for the state under considerations. From the point of view of quantum communications, such finding is of great importance as it allows the characterisation of a minimal efficiency on the communication protocol. One should also emphasise that Werner states are considered as the paradigmatic examples of experimental noise. This fact justifies the choice of Werner-like states as a test bed for our protocol.

Chapter 4

Experimental Hierarchy and Optimal Robustness of Quantum Correlations of Two-Qubit States With Controllable White Noise

Contents of this Chapter is based on the Author's article [A4].

4.1 Introduction

4.1.1 Entanglement, Steering, and Bell Nonlocality

Quantum entanglement [79] and its generalizations, i.e., quantum steering [239, 240] and Bell nonlocality [86], are fundamental types of quantum correlations between spatially separated systems (parties). These effects reveal the disparity between classical and quantum physics from a fundamental point of view, but also play a pivotal role in quantum information and its applications in quantum technologies of second generation [45, 241–243]. (i) Quantum entanglement (or quantum inseparability) occurs when the state of one party cannot be described independently of the state of the other party [45]. (ii) Quantum steering, also referred to as Einstein-Podolsky-Rosen (EPR) steering, refers to the ability of one party (say, Alice) to affect the state of the other party (say, Bob) through the choice of her measurement basis, which cannot be explained by any local hidden state (LHS) models [242, 243]. Moreover, (iii) quantum nonlocality can be defined as the effect detectable by the violation of the Bell inequality and, thus, which cannot be explained by any local hidden variable (LHV) models. Here we limit our interest to the two-qubit Bell inequality in the Clauser-Horne- Shimony-Holt (CHSH) form [87]. Thus, we refer to this effect as Bell(-CHSH) nonlocality, having in mind that quantum nonlocality can also be understood in a much broader sense [241].

The distinction between these effects is fundamental, and their intuitive operational interpretation can be given from a measurement perspective, i.e., by referring to their detection using two types of measuring devices, which can be perfect or imperfect from physical and technological points of view, or trusted or untrusted from a cryptographic perspective, i.e., with or without prior knowledge about the devices [244]. Specifically, (i) quantum entanglement between two systems can be detected using trusted devices for both systems, (ii) EPR steering can be tested by trusted devices for one system and untrusted ones for the other, while (iii) quantum nonlocality can be detected by untrusted devices on both sides. Such interpretation has direct applications for quantum cryptology, including secure communication. In the same measurement scenarios, Bell nonlocality implies steering, and steering implies entanglement, but not vice versa, in general. Indeed, there exist entangled [98] and steerable states which do not violate Bell inequalities as well as do exist unsteerable entangled states [242, 243].

4.1.2 Werner States and Their Experimental Generation

Mixtures of a Bell state and a maximally mixed state (i.e., white noise) are prototypal examples of states revealing the non-equivalence of entanglement and Bell nonlocality, which was first demonstrated by Werner over 30 years ago [98]. The Werner states have been later used to show a hierarchy of criteria and a hierarchy of some classes of correlations (CC) (which for short is here refereed to as *CC hierarchy*), including quantum steering (see, e.g., reviews in [45, 241–243] and the very recent Ref. [245] with references therein). The effect of white noise on Bell states has also been studied theoretically to reveal a hierarchy of the following classes of temporal quantum correlations [246]: temporal inseparability [247], violations of temporal Bell-CHSH inequalities [248], and temporal steering [249, 250].

We stress that we only consider von Neumann's projective measurements in this work. Note that the quantum-correlation regimes of states assumed for projective measurements are different from those based on positive-operator-valued measures (POVMs). However, the same hierarchy relations, as studied here, still hold assuming POVMs.

Generation of mixed states of discrete photons has been investigated both theoretically [251–253] and experimentally [254–267]. Temporal decoherence of optical polarization modes in a birefringent material seems to be a rather widely used technique in a number of experiments such as those reported in Refs. [258, 267]. This technique has also enabled the experimental generation of maximally entangled mixed states (MEMSs) [268] by Peters *et al.* [265] and later by Aiello *et al.* [263]. Recently, Liu *et al.* incorporated a tunable decoherence channel [269] to generate the Werner states [256]. Alternative methods to generate or simulate temporal decoherence include the generation of mixed states by exploiting a particular geometry of a spontaneous parametric down-conversion (SPDC) source [254, 264]. In 2004, Barbieri *et al.* [266] and Cinelli *et al.* [260] reported their refined two-photon sources capable of preparing a broad range of mixed quantum states, including MEMSs. A highly birefringent material, together with a wide momentum spectrum of generated photon pairs (resulting in effective spatial decoherence), was also used as an alternative method to generate temporal decoherence [258]. Puentes *et al.* applied wedge depolarisers and bucket detectors [257], and later utilized scattering in various media [262]. Moreover, Zhang *et al.* incoherently combined photons generated in two separate SPDC sources to create mixed quantum states [259], while Caminati *et al.* reported an experiment, where mixed states were generated by attenuating a high-gain SPDC source [261]. The idea of using a wide-temporal detection window, such that a detected state appeared to be mixed, was also implemented in several experiments [255, 270]. It is also possible to use an experimental setup that can be tuned (to change properties of generated states) in times shorter than the measurement integration time [271].

In this work we report experimental generation of both Werner states and their generalizations, i.e., partially entangled pure states affected by white noise, which we refer to as generalised Werner states (GWSs). These states were not in the focus of the above-reviewed experiments. Some of the experimental setups cannot generate these generalised states (e.g., Ref. [263]), some could be used after specific improvements (e.g., Ref. [256]) and the others, possibly, might have such capabilities, but these (e.g., Ref. [259]) have not been used so far for demonstrating the CC hierarchy of the Werner states or their generalizations. In this research, our experimentally generated and reconstructed states are applied to reveal a CC hierarchy.

The remainder of this Chapter is organised as follows. Two approaches to study hierarchies of correlations are specified in Sec. 4.2. Measures of quantum correlations of general two-qubit states are recalled in Sec. 4.3. These include popular measures of entanglement, steering, and Bell nonlocality. Moreover, steering in the two-, three-, and multi-measurement scenarios is explicitly discussed in Appendices C.3, C.2, and C.4, respectively. In Sec. 4.4 we define GWSs. Because GWSs are a direct generalization of the usual Werner states based on a Bell state, we refer to them as Bell-non-diagonal GWSs. Our experiment is described in Sec. 4.4.1. We compare various predictions of the quantum correlations for the theoretical and experimental GWSs with those for the Werner states in Sec. 4.5. We also discuss fundamental differences in a CC hierarchy for the Bell-diagonal and -non-diagonal GWSs in this section. In Sec. 4.6 we present our most counterintuitive theoretical results. Specifically, we show in Sec. 4.6.1 that there exist GWSs, which are steerable in a two-measurement scenario (2MS) but still admit LHV models. Such a regime cannot be observed for the standard Werner states. In Sec. 4.6.2 we show that some Bell-non-diagonal GWSs are more robust against white noise than the diagonal GWSs, i.e., the Werner states. In Sec. 4.6.3, we analyse lower and upper bounds on steering for a large number of measurements. We show better robustness against white noise of unsteerable entangled Bell-non-diagonal GWSs compared to the diagonal ones. An example of a hierarchy of entanglement criteria is discussed in Appendix C.5 in comparison with the CC hierarchy for the GWSs. We conclude in Sec. 4.7.

4.2 Two Approaches to Study a Hierarchy of Quantum Correlations

Here we study a CC hierarchy, which is the hierarchy of *states* with different correlation properties rather than types of probability distributions, as in the case of certain research in quantum information. We use the term correlation of a state by referring to its entanglement, steering, and Bell nonlocality. For clarity, we recall that: (a) an entangled (separable) state is a state that cannot (can) be factored into individual states belonging to separate subspaces, (b) an EPR steerable (unsteerable) state is the one described by the statistics which cannot (can) be reproduced by an LHS model for a given measurement set (see Sec. 4.3.2 for more details), and (c) a quantum nonlocal (local) state is the one described by the statistics which cannot (can) be reproduced by an LHV model, which in turn implies the violation (fulfillment) of a Bell inequality. Since we are focused on analysing two-qubit states, the Bell inequalities can be limited to the CHSH inequality. Moreover, the steerability of states can be considered in the limit of an infinite number of measurements, but it is usually limited to practical resources, including a finite number of measurements. In our research we focus on the GWSs which are steerable or unsteerable in two- and three-measurement scenarios (2MS and 3MS), corresponding to measuring two (three) Pauli operators. Thus, we can consider subclasses of steerable states depending on the number of performed measurements. In what follows, we study in detail the hierarchy of correlation classes limited to analysing the states which are: (i) separable, (ii) entangled but unsteerable in 3MSs, (iii) steerable in 3MSs but not in 2MSs, (iv) 2MS steerable but local, and (v) nonlocal. The hierarchy is extended in Sec. 4.6.3 to include the analysis of the GWSs which are steerable for a larger number n of measurements (i.e., $n = 136$).

In general, a hierarchy of quantum correlations can be understood in several ways including: (i) a hierarchy of conditions (or criteria) for the observation of a given class of quantum correlations and (ii) a hierarchy of different classes of quantum correlations (i.e., a CC hierarchy). This division is also closely related to experimental demonstrations of a hierarchy by measuring (nonuniversal or universal) witnesses of quantum correlations corresponding to performing partial or full quantum state tomography (QST), respectively.

In this work, we focus on analysing a CC hierarchy of the GWSs. We demonstrate different kinds of quantum correlations in question by performing full QST and then calculating the corresponding measures on the reconstructed states.

Below we explain the main differences between the two approaches to study a hierarchy of quantum correlations and explain why a complete experimental demonstration of the studied CC hierarchy. To our knowledge, this seems to be unfeasible within the present state of the art.

Hierarchy of Criteria for a Given Class of Quantum Correlations

Experimental demonstrations of Bell nonlocality via the violations of the CHSH inequalities have been at the heart of quantum information since its early days starting from the pioneering experiments of Aspect *et al.* in the 1980s [272] and then refined in hundreds of experiments, including significant-loophole-free tests (see, e.g., [273–275] and the review in [241] for references).

Thus, if one talks about "demonstrating" the nonlocality of a quantum state, one would normally expect to see a violation of a Bell inequality, rather than QST.

However, this approach usually reveals only a hierarchy of criteria (i.e., either sufficient or necessary conditions) for the observation of a specific class of quantum correlations. This is because it is usually based on measuring nonuniversal witnesses of quantum correlations by testing the violation of specific inequalities. Note that nonuniversal witnesses correspond usually to *sufficient but not necessary conditions* of a specific quantum (temporal or spatial) correlation effect. Thus, such a witness can usually be determined *without* a complete QST.

Within this hierarchy approach, one can analyse a hierarchy of, e.g., different Bell inequalities or even the Bell-CHSH inequalities but for different angles of polarisers in a description of Bell nonlocality, specifically, by choosing different angles ϕ_1, ϕ_2, ϕ_1', and ϕ_2' as described in Eq. (4.5). By having *a priori* information about a given generated state, one can choose optimally angles of the polarisers to maximize the violation of the Bell-CHSH inequalities and thus to be able to quantify Bell nonlocality (i.e., to determine a nonlocality measure) for the state. However, without knowing *a priori* a given state, one has to measure many copies of the state at different angles of the polarisers, to find their optimal rotation. Such scanning of the angles corresponds to (complete or partial) QST.

The hierarchy of criteria has also been studied based on the matrices of the moments of, e.g., the annihilation and creation operators of bosonic or fermionic states of any dimension. Indeed, a number of works demonstrated: (i) a hierarchy of sufficient conditions for observing entanglement (i.e., entanglement witnesses). These include the conditions based on the Shchukin-Vogel criterion [276, 277] which are related to the Peres-Horodecki criterion and its generalised versions using positive maps beyond partial transpose [278], (ii) a hierarchy of sufficient conditions for observing quantum steering (i.e., steering witnesses) [279], (iii) a hierarchy of necessary conditions for revealing Bell nonlocality (i.e., nonlocality requirements) [280], and (iv) a hierarchy of sufficient conditions for observing spatial [281] and spatio-temporal nonclassicality (i.e., nonclassicality witnesses) [282, 283].

An illustrative detailed example of a hierarchy of entanglement criteria is discussed in Appendix C.5.

Note that the upper and lower bounds of measures of quantum correlations, which correspond to their sufficient and necessary conditions, can be determined using such a hierarchy of matrices of moments without a complete QST. However, for an unknown state, to make these bounds tight to a true measure, one needs to increase the number of moments to be detected. This in turn leads to a partial moment-based QST, which approaches more and more a complete QST as explained in Appendix C.5.3.

In conclusion, this approach, in general, enables a direct but partial demonstration of a hierarchy, which is discussed below.

Hierarchy of Various Classes of Correlations

A hierarchy of various classes of correlations can be revealed by their measures or by the conditions, which are both necessary and sufficient for their observation. It should be stressed that we are focused on demonstrating such a CC hierarchy in this Chapter.

Indeed, experimental methods for a complete demonstration of a CC hierarchy can be based on experimentally reconstructed density matrices (in the case of standard single-time spatial correlations) or the Choi-Jamiołkowski matrices (in the case of temporal correlations) for a given system via quantum state or process tomographies, respectively. This approach enables the calculation of necessary and sufficient conditions for observing and quantifying the amount of any class of quantum temporal or spatial correlations for a given state or process.

Experimental demonstration of such a CC hierarchy has usually been done using a complete QST, although it can also be done with an incomplete QST, as discussed in Appendix C.1.

Here we apply an indirect approach based on experimental detecting and reconstructing states via a full QST and only then calculating their correlation measures on the reconstructed states. This approach has important fundamental and experimental advantages, which include the following (in addition to the above-mentioned ones):

(i) We want to test the above-mentioned five classes of quantum correlations on the same footing (preferably using the same setup) based on either complete or incomplete tomography. However, it is seen that we can determine experimentally the Horodecki nonlocality measure without QST, but detecting the negativity and the steerable weights (or, equivalently, steering robustness) can be done effectively only via a complete QST.

(ii) We want to use the same experimental states for testing different quantum properties. The problem is that we do not have perfect control of especially the mixing parameter determining the amount of white noise in a pure state. Thus, we cannot generate the same GWSs even using the same setup. Such a state generation would be even more demanding using different setups for testing different classes of correlations. However, this is feasible using a full QST to reconstruct a state, which is only then numerically studied for its quantum correlations.

4.3 Measures of Quantum Correlations of General Two-Qubit States

As a part of our introduction, we shortly recall standard measures of quantum correlations for general two-qubit states ρ, which can be written in the Bloch representation as follows:

$$\rho = \frac{1}{4}\Big(I \otimes I + \boldsymbol{u}\cdot\boldsymbol{\sigma} \otimes I + I \otimes \boldsymbol{v}\cdot\boldsymbol{\sigma} + \sum_{n,m=1}^{3} T_{nm}\,\sigma_n \otimes \sigma_m\Big), \tag{4.1}$$

where $u_i = \mathrm{Tr}[\rho(\sigma_i \otimes I)]$ and $v_i = \mathrm{Tr}[\rho(I \otimes \sigma_i)]$ are the elements of the Bloch vectors $\boldsymbol{u} = [u_1, u_2, u_3]$ and $\boldsymbol{v} = [v_1, v_2, v_3]$ of the first and second qubits, respectively, and I is the single-qubit identity operator. Moreover, the correlation matrix $T_{ij} = \mathrm{Tr}[\rho(\sigma_i \otimes \sigma_j)]$ and $\boldsymbol{\sigma} = [\sigma_1, \sigma_2, \sigma_3] \equiv [X, Y, Z]$ are expressed via the Pauli matrices.

4.3.1 Entanglement Measures

Here we recall the standard definitions and physical meaning of the two most popular measures of two-qubit entanglement, i.e., the negativity and concurrence, which are in the following sections compared with the measures of steering and Bell nonlocality.

The negativity is defined as $N(\rho) = \max\{0, -2\mu_{\min}\}$, where $\mu_{\min} = \min \mathrm{eig}(\rho^\Gamma)$ and ρ^Γ denotes a partial transpose of ρ. It was first introduced in Ref. [284] as a quantitative version of the Peres-Horodecki entanglement criterion [285]. The two-qubit negativity (or, more directly, the logarithmic negativity $\log_2[N(\rho) + 1]$) has various quantum-information interpretations. Specifically: (i) it is a measure of the entanglement cost under operations preserving the positivity of the partial transpose for two-qubit systems [286, 287], (ii) it gives an upper bound of distillable entanglement [45], and (iii) it determines the dimensionality of entanglement, i.e., the number of the degrees of freedom of entangled subsystems [288].

The Wootters concurrence [289], which is monotonically related to the entanglement of formation, is given by $C(\rho) = \max\{0, 2\lambda_{\max} - \sum_j \lambda_j\}$, where

$$\lambda_j^2 = \mathrm{eig}[\rho(\sigma_2 \otimes \sigma_2)\rho^*(\sigma_2 \otimes \sigma_2)]_j\,, \tag{4.2}$$

with σ_2 denoting the Pauli Y-operator, and $\lambda_{\max} = \max_j \lambda_j$.

Note that both measures have been applied in quantifying not only entanglement but also, e.g., nonclassicality (quantumness) of single-qubit (or single-qudit) states [290–292]. These two related measures reach unity for the Bell states and vanish for separable states. For the brevity of our presentation, we have plotted the negativity as the only entanglement measure.

These entanglement measures of various two-qubit states have been typically determined experimentally only indirectly, based on a full QST, which is also the case in this work. Note that an experimental universal test of entanglement without a complete QST was proposed in Ref. [293] (see Appendix C.1). This test is a necessary and sufficient criterion of two-photon polarization entanglement. It is based on measuring a collective universal witness of Ref. [294], which gives tight lower and upper bounds for the negativity and concurrence, and can be used as an entanglement measure on its own. However, since its quantum-information interpretation and applications are limited, we prefer to use the standard entanglement measures, even if they are determined indirectly using experimental density matrices.

4.3.2 Steerable Weight

The steerable weight [295] and the steering robustness [296] are arguably the most popular measures of EPR steering [242, 243, 297]. They can be applied for quantifying not only standard spatial steering, but also (after a minor modification) to quantify temporal [246, 249, 250, 298, 299] and spatio-temporal [300] steering.

An intuitive and general idea behind the steerable weight, according to Skrzypczyk *et al.* [295], is based on the decomposition of a given assemblage of Alice, $\sigma_{a|x}$, into its steerable ($\sigma^{\mathrm{S}}_{a|x}$) and unsteerable ($\sigma^{\mathrm{US}}_{a|x}$) parts, for the values of a and x specified in Appendices C.2 and C.3, i.e.,

$$\sigma_{a|x} \;=\; \mu\sigma^{\mathrm{US}}_{a|x} + (1-\mu)\sigma^{\mathrm{S}}_{a|x}, \tag{4.3}$$

for $\mu \in [0,\, 1]$. Note that the unsteerable assemblages $\sigma^{\mathrm{US}}_{a|x}$ can be created via classical strategies, and a model based on $\sigma^{\mathrm{US}}_{a|x}$ can be referred to as an LHS model. The steerable weight $S = 1-\mu^*$ is defined as the maximum amount of unsteerable assemblage $\sigma^{\mathrm{US}}_{a|x}$ necessary to reproduce Alice's assemblage $\sigma_{a|x}$. This general definition can be formulated as solutions of semidefinite programs (SDPs) as demonstrated in Refs. [242, 295] and are given explicitly in Appendices C.2 and C.3 for the 3MS and 2MS, respectively. Moreover, sufficient and necessary conditions for observing steering in multi-measurement scenarios are discussed in Appendix C.4.

The LHS models are relevant to quantum steering as follows [244]: A given state ρ is referred to as quantum (EPR) *unsteerable* (in the communication from Alice to Bob) for Alice's measurement set $\{M_{a|x}\}$ if one can find a variable λ allowing for the following Bell local decomposition [242, 243]

$$p(ab|xy) \;=\; \int d\lambda\, \pi(\lambda)\, p_A(a|x,\lambda)\ \mathrm{Tr}\big(M_{b|y}\sigma_\lambda\big), \tag{4.4}$$

where σ_λ is the local (hidden) quantum state of Bob and $p_A(a|x,\lambda)$ is Alice's response distribution. Otherwise a given state for the measurement set $\{M_{a|x}\}$ is referred to as quantum (EPR) *steerable*, i.e., when its statistics cannot by reproduced by an LHS model. Note that Eq. (4.8), which defines a Bell local state, reduces in the special case to Eq. (4.4) by setting $p_B(b|y,\lambda) = \mathrm{Tr}\big(M_{b|y}\sigma_\lambda\big)$. It is usually assumed that Bob's measurements $M_{b|y}$ enable a complete QST of his qubit. The collection of Bob's states $\sigma_{a|x} = \mathrm{Tr}_A(M_{a|x} \otimes \mathbb{1}\,\rho)$, conditioned on Alice's measurements, is called an assemblage.

The steerable weight and, equivalently, the steering robustness of Ref. [296] are defined via necessary and sufficient conditions for quantum-information characterization of quantum steering in the specified measurement scenarios. Thus, a spatially separated two-qubit state ρ is referred to as steerable (or more precisely S_n-steerable) in the discussed n-measurement scenarios if there exists a set of measurements such that the steerable weight is nonvanishing, $S_n(\rho) > 0$. Otherwise it is referred to as unsteerable (or S_n-unsteerable).

The question arises why our interest is focused on analysing steering in two- and three- measurement scenarios only, except in Sec. 4.6.3 and Appendix C.4. In principle, one could also consider steering in the limit of an infinite number (of the types) of measurements. But this would require knowing universal criteria (i.e., which are both sufficient and necessary) for detecting this type of steering. Unfortunately, such universal criteria are not known for the GWSs. Note that the upper and lower bounds for steering have only been calculated numerically so far for large but still finite numbers n of measurements (i.e., at most for $n = 136$, as shown in Fig. 4.8(a) based on the results of Refs. [301, 302]). Moreover, our analysis of steering includes not only criteria but also steering measures, as shown in Figs. 4.2–4.5. Unfortunately, the calculations of the steerable weight and the steering robustness are much more involved beyond 3MS. Finally, we remark that our experimentally generated states are not exactly GWSs, so the calculations of their measures or even universal criteria of steering beyond the 3MS are even more complicated compared to those for the perfect GWSs.

4.3.3 Horodecki Measure of Bell Nonlocality

Here we recall the Horodecki measure [303, 304] of quantum nonlocality for two-qubit states.

Note that quantum nonlocality is usually studied and interpreted in the context of Bell inequalities (including the CHSH inequality) and then it is often referred to as Bell(-CHSH) nonlocality [241]. A Bell inequality violation (BIV) demonstrates the impossibility of any LHV models to fully reproduce quantum-mechanical predictions [86]. For convenience, we use the terms BIV and Bell(-CHSH) nonlocality interchangeably, in the context of our two-qubit experiments. Note that BIV implies a violation of local realism. So BIV can in principle be explained by *nonlocal* (non)realistic theories, but also by *local* nonrealistic ones. Moreover, quantum nonlocality can be defined without referring to BIV. In addition, such (generalised) quantum nonlocality can occur without quantum entanglement in, e.g., three qubits or two qutrits (three-level systems) [305]. Thus, it should be stressed that, in general, neither BIV implies quantum nonlocality nor quantum nonlocality implies BIV (see, e.g., Refs. [241, 306]).

The Horodecki measure of Bell nonlocality for a two-qubit state ρ quantifies the amount of the maximal violation of the Bell-CHSH inequality [87],

$$|\langle\mathscr{B}\rangle| = |\mathscr{E}(\phi_1,\phi_2) + \mathscr{E}(\phi_1',\phi_2) + \mathscr{E}(\phi_1,\phi_2') - \mathscr{E}(\phi_1',\phi_2')| \leq 2, \tag{4.5}$$

which is given in terms of the Bell-CHSH operator $\mathscr{B} = \boldsymbol{a}\cdot\boldsymbol{\sigma}\otimes(\boldsymbol{b}+\boldsymbol{b}')\cdot\boldsymbol{\sigma}+\boldsymbol{a}'\cdot\boldsymbol{\sigma}\otimes(\boldsymbol{b}-\boldsymbol{b}')\cdot\boldsymbol{\sigma}$. Moreover, ϕ_i and ϕ_i' are two dichotomic variables of the i-th ($i = 1, 2$) qubit corresponding to the rotations of a polariser in typical optical implementations; while $\mathscr{E}(\phi_1,\phi_2)$ is the expectation value of the joint measurement of ϕ_1 and ϕ_2, and, analogously, for the other expectation values. For a given two-qubit state ρ, the expected value of the Bell-CHSH operator $\mathscr{B}$, which is maximized over real-valued three-dimensional unit vectors $\boldsymbol{a}$, $\boldsymbol{a}'$, $\boldsymbol{b}$, and $\boldsymbol{b}'$, reads [303, 304]:

$$\max_{\mathscr{B}} \mathrm{Tr}\,(\rho\mathscr{B}_{\mathrm{CHSH}}) = 2\sqrt{M(\rho)}, \tag{4.6}$$

where $M(\rho) = \max_{j<k}\,\{h_j + h_k\} \leq 2$, and h_j ($j = 1, 2, 3$) are the eigenvalues of $U = T^{\mathrm{T}}\,T$, which is the real symmetric matrix constructed from the correlation matrix T (and its transpose T^{T}) defined below Eq. (4.1). Thus, the Bell-CHSH inequality is violated if $M(\rho) > 1$ [303, 304]. To quantify the degree of BIV and Bell nonlocality we apply the parameter [307]:

$$B(\rho) \equiv \sqrt{\max\,[0,\, M(\rho) - 1]}. \tag{4.7}$$

Note that this nonlocality measure is exactly equal to the concurrence and negativity for two-qubit *pure* states. For a given state ρ, the Bell-CHSH inequality in Eq. (4.5) is satisfied if and only if $B(\rho) = 0$. If $B(\rho) = 1$ then the inequality is maximally violated, which is the case for Bell states. We refer to $B(\rho)$ as a Bell nonlocality measure.

In this work we refer to Bell nonlocal and local states with the following meaning. Usually, a spatially separated state is referred to as Bell local if local measurements and classical communication can generate a correlation admitting an LHV model [86, 241]. Otherwise, the state is referred to as Bell nonlocal.

More specifically, an LHS model can be introduced by considering two distant observers (Alice and Bob) who share an entangled two-qubit state ρ. Assume that Alice (Bob) performs a set of measurements $\{M_{a|x}\}$ ($\{M_{b|y}\}$) satisfying $M_{a|x}, M_{b|y} \geq 0$ and $\sum_a M_{a|x} = \sum_b M_{b|y} = \mathbb{1}$, where x and y label measurements and $a$and b are their outcomes. The resulting statistics $p(ab|xy) = \mathrm{Tr}\big(M_{a|x} \otimes M_{b|y}\,\rho\big)$ is referred to as Bell *local* (with respect to the measurement sets $\{M_{a|x}\}$ and $\{M_{b|y}\}$) if they allow for a Bell local decomposition [241]:

$$p(ab|xy) \;=\; \int d\lambda\; \pi(\lambda)\; p_A(a|x,\lambda)\; p_B(b|y,\lambda), \tag{4.8}$$

where λ is a shared local hidden variable distributed with density $\pi(\lambda)$, while $p_A(a|x,\lambda)$ and $p_B(b|y,\lambda)$ are local response distributions. Thus, a state is called Bell *local* if it can be reproduced by an LHV model with properly chosen $\{\lambda,\, \pi(\lambda),\, p_A(a|x,\lambda),\, p_B(b|y,\lambda)\}$. Otherwise, the state is referred to as Bell *nonlocal* for the measurement sets $\{M_{a|x}\}$ and $\{M_{b|y}\}$. This Bell nonlocality can be witnessed by the violation of a Bell inequality, which reduces to testing the Bell-CHSH inequality in the case of two-qubit states. So, in terms of the Horodecki measure, a given two-qubit state is Bell local (nonlocal) if and only if $B(\rho) = 0$ ($B(\rho) > 0$).

The Horodecki measure of Bell nonlocality can be determined *without* a complete QST, which was experimentally demonstrated in an entanglement-swapping device in [308] (see Appendix C.1). However, here, we apply a full QST for determining ρ^{E}_{GW} and then calculating $B(\rho^{E}_{\mathrm{GW}})$.

Note that various alternative approaches to quantifying nonlocality have been proposed [241]. These include a nonlocality measure introduced by Elitzur *et al.* in Ref. [309], which can be interpreted as a fraction of a given ensemble that cannot be expressed via local correlations. Thus, this quantifier has been referred to as a fraction of nonlocality [310, 311].

4.4 Generalised Werner States and Their Experimental Generation

In this work we focus on comparing quantum correlations of experimental states, which are special cases of those in Eq. (4.1). Specifically, we directly generated Werner(-like) states (also referred to as isotropic states or Bell states with white noise) [98]:

$$\rho_{\mathrm{W}} \;=\; p\,|\phi^+\rangle\,\langle\phi^+| + \frac{1-p}{4} I \otimes I, \tag{4.9}$$

which are mixtures of any Bell state [say, $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$)] and the maximally mixed state for various values of the mixing parameter $p \in [0,1]$. Note that the original definition of the Werner state is based on the singlet state [98], instead of $|\phi^+\rangle$. However, this local change does not effect measures of entanglement, steering, and nonlocality. Thus, the state defined in Eq. (4.9) is also often referred to as a Werner state (see, e.g, Refs. [268, 302, 307, 312, 313]). This terminology is used in this Chapter.

We are also interested in partially entangled states with white noise, which we call GWSs, which are obtained from Eq. (4.9) by replacing $|\phi^+\rangle$ by a general two-qubit pure state $|\phi_q\rangle = \sqrt{q}\,|00\rangle + \sqrt{1-q}\,|11\rangle$ with the superposition coefficient $q \in [0,1]$. Thus, the GWSs can be defined as

$$\rho_{\mathrm{GW}}(p,q) \quad = \quad p\,|\phi_q\rangle\langle\phi_q| + \frac{1-p}{4} I \otimes I. \tag{4.10}$$

These states for $q = \frac{1}{2}$ can be referred to as the Bell-diagonal GWSs corresponding to the Werner states $\rho_{\mathrm{W}}(p)$, which are diagonal in the Bell basis. While for $q \neq \frac{1}{2}$ we refer to them as the Bell-non-diagonal GWSs. These states have been generated by us in the experimental setup described below.

4.4.1 Experimental Setup

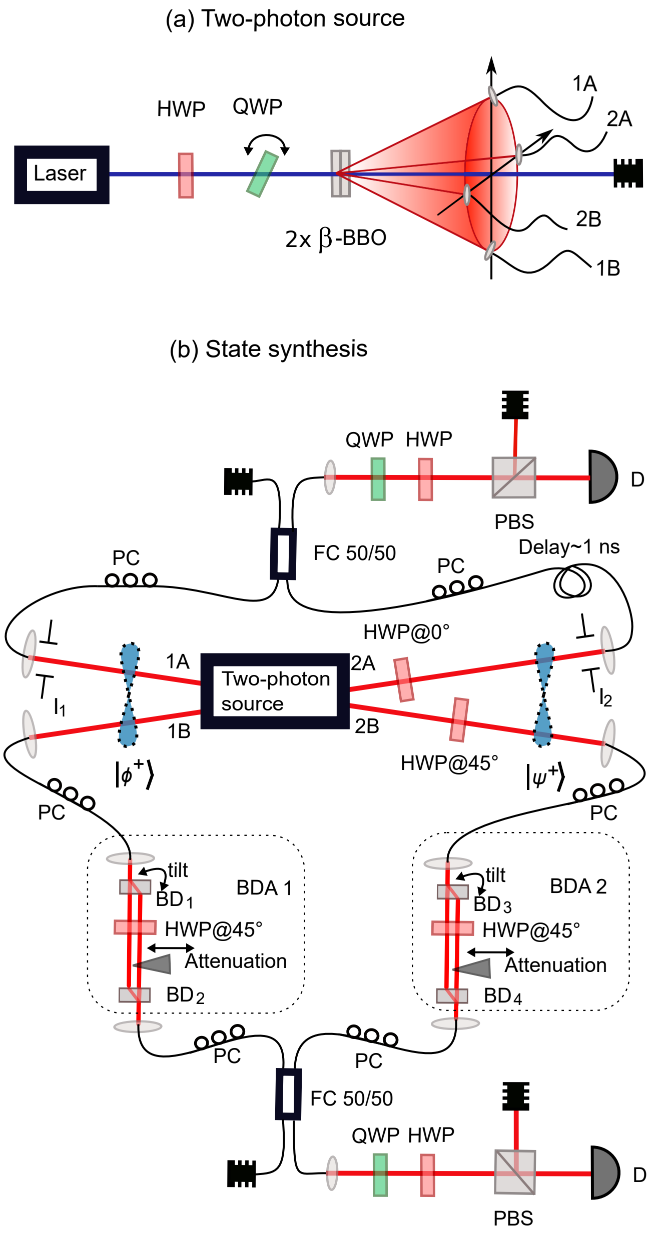
Here we describe our experimental setup, which is designed to be as much versatile as possible, being capable of generating a broad class of mixed quantum states in the form of

$$\rho = \begin{pmatrix} A & 0 & 0 & E \\ 0 & B & F & 0 \\ 0 & F^* & C & 0 \\ E^* & 0 & 0 & D \end{pmatrix}. \tag{4.11}$$

This class of states includes (i) the Werner [98] and Werner-like states, (ii) the Horodecki states, which are mixtures of a Bell state and a separable state orthogonal to it [285], (iii) Bell-diagonal states [including the Werner states], and (iv) various types of MEMSs, e.g., those defined in [268]. Moreover, capabilities of our method are not limited to the Werner or Horodecki states based on a "balanced" Bell state, but also allow for (v) their generalised forms based on unbalanced entangled states $\sqrt{1-q}\,|00\rangle + \sqrt{q}\,|11\rangle$ for any $q \in [0,1]$ instead of considering only $q = \frac{1}{2}$.

In this work we focus on experimental generation of the Werner states and GWSs, which are prepared on a platform of quantum linear optics using the experimental setup depicted in Fig. 4.1. Qubits were encoded into polarization states of single photons. The process of type-I spontaneous parametric down-conversion (SPDC) occurring in a cascade of two nonlinear β-BBO crystals, served as a source of entangled photons [121]. When pumped by a beam at a wavelength of $\lambda = 355$ nm, the source generated two polarization-entangled photons in mutually different spatial modes at $\lambda = 710$ nm [Fig. 4.1(a)]. The state of these photons can be expressed in the form of $|\phi^+\rangle = (|00\rangle +$ $+\,|11\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ denote horizontally (H) and vertically (V) polarized photons, respectively. Due to the geometry of type-I SPDC, photons are generated in symmetrically opposite directions on the surface of a cone with its axis coincidental with the pump beam. We choose to couple photon pairs propagating in the vertical and horizontal planes, denoting them by (1A,1B) and (2A,2B), respectively [see Fig. 4.1(a)]. Assuming that only two photons were generated (so higher-photon-number processes are negligible), these photons are simultaneously in either modes (1A,1B) or (2A,2B). Employing a half-wave plate (HWP) at 45° in the 2B mode, the state $|\phi^+\rangle$ is transformed into the Bell state $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. Thus, we obtained states spanning the two subspaces $|\phi^+\rangle$ and $|\psi^+\rangle$.

Our goal is to prepare the Werner states and their generalizations for various values of the mixing parameter p. The main idea behind the design of our setup is to decrease temporal coherence of the states $|\phi^+\rangle$ (in the modes 1A and 1B) and $|\psi^+\rangle$ (in the modes 2A and 2B) using beam displacer assemblies (BDAs). A BDA consists of a pair of beam displacers (BDs) with an HWP inserted between them. This allows us



(a) Two-photon source

(b) State synthesis

Figure 4.1: Our experimental setups for (a) photon-pairs generation and (b) state synthesis. Legend: 1A and 1B (2A and 2B) stand for photons propagating in vertical (horizontal) planes, BD – a beam displacer, BDA – a beam displacer assembly, D – a detector, FC – a fiber coupler, HWP – a half-wave plate, PBS – a polarization beam splitter, PC – a polarization controller, QWP – a quarter-wave plate, I_1,I_2 – irises 1, 2, and β-BBO stands for a nonlinear crystal (β-barium borate).

to split and subsequently rejoin the horizontal and vertical components of a photon polarization state. By introducing a difference in the propagation time between these two components (which is done by tilting one BD) we can achieve their mutual phase difference (by fine tilting) and tunable distinguishability (by coarse tilting). Polarization-sensitive losses can easily be implemented by partially blocking one of the polarization paths. Subsequently, the modes (1A,2A) and (1B,2B) are incoherently mixed in fiber couplers (FCs).

Firstly, the subspace $|\phi^+\rangle$ was adjusted while arms 2A and 2B (belonging to the subspace $|\psi^+\rangle$) were blocked. By means of the polarization-sensitive losses in BDA_1, we regulated the intensity ratio of the matrix elements A and D [see Eq. (4.11)] in the computational basis, i.e., $|00\rangle$ and $|11\rangle$ (or $|HH\rangle$ and $|VV\rangle$ in the polarization terms). The ratio accounts for

$$R_{\mathrm{A,D}} = \frac{4pq + 1 - p}{4p(1-q) + 1 - p}\,, \tag{4.12}$$

where p and q are both tuned parameters. The next step consists of tuning the decoherence by observing coincidence counts in the projections $|{+}{+}\rangle$ and $|{+}{-}\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ stand for diagonal and anti-diagonal polarization states, respectively. We found such a coarse tilt of BD_1 so that the visibility accounts for

$$\nu = \frac{2E}{A + D}, \tag{4.13}$$

while the phase is set by fine-tuning, the tilt using a piezo-actuator, which minimizes the signal in the $|{+}{-}\rangle$ projection by setting the effective value of E to be real.

Secondly, when adjusting the subspace $|\psi^+\rangle$ in turn, the arms 1A and 1B were blocked. In analogy with the adjustment of the $|\phi^+\rangle$ subspace, the same two steps were performed. This time, however, the target intensity ratio $R_{\mathrm{B,C}}$ is equal to 1 because $B = C$. The coarse tilt of BD_3 needs to be sufficient to decrease the coherence of the state completely since $\nu = 0$, resulting in $F = 0$. The phase becomes meaningless.

Finally, all arms were unblocked and both subspaces were balanced to adjust the ratio between the matrix elements A and B. While having the projection $|00\rangle$ and $|01\rangle$, the required ratio was

$$R_{\mathrm{A,B}} = \frac{4pq + 1 - p}{1 - p}\,. \tag{4.14}$$

For this purpose, we partially closed the irises in the 1A and 2A couplers, which are depicted in Fig. 4.1(b) by labels I_1 and I_2, respectively.

After all the adjustments were implemented, the measurement itself was carried out and it consisted of a standard full QST [238]. Polarization projection was performed on both photons utilizing a set of quarter- and half-wave plates, as well as polarisers and single-photons detectors. Coincidence detections within 2 ns window were detected under all 36 two-fold combinations of single-photon projections onto the basis states: $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, and $(|0\rangle \pm i\,|1\rangle)/\sqrt{2}$, where the latter states are the right- and left-hand circularly polarized states, respectively. Density matrices were estimated via a maximum likelihood method [132, 314–317].

Because of experimental imperfections, the setup produces states with the p and q parameters slightly different from those targeted by the above-described procedure. To observe better agreement with theoretical predictions, we have estimated the best-fitting parameters p_{est} and q_{est} by finding such a $\rho_{\mathrm{GW}}(p_{\mathrm{est}}, q_{\mathrm{est}})$ that its fidelity with the experimentally reconstructed density matrix is maximized. We find that the deviations of the estimated value of the mixing parameter p_{est} from the value of p, which was set with a limit precision in our experiment, are on average equal to 0.01 for the Werner states and 0.03 for the GWSs. For the estimated value of the superposition parameter q_{est}, the observed parameter deviations from a given value of q are equal on average to 0.02. The maximal deviation values are 0.03 for both Werner states and GWSs. Note that the superposition parameter q was manually set by an HWP in the source part of the setup shown in Fig. 4.1(a). Experimental data as well as the estimated density matrices are provided on the CD-ROM attached to the printed version of this Thesis (Appendix E).

The states ρ_{W} and ρ_{GW} can also be expressed by Eq. (4.11) with $F = 0$. In this matrix, the subspace spanned by the states $|\phi_q\rangle$ for $q \in [0,\, 1]$ is represented by the elements A, D, E, and E^*, while the corresponding subspace for the white-noise term corresponds to only diagonal elements (A, B, C, D). For the reasons specified below, we set, in our experiments, the superposition coefficient at $q = 0.9$, in addition to $q = 0.5$.

Note that it is irrelevant to replace $|\phi_q\rangle$ by a four-term superposition state $|\phi_{abcd}\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$ at least in the analysis of nonclassical correlations. This is because $|\phi_{abcd}\rangle$ can be reduced to $|\phi_q\rangle$ solely by local rotations, so the studied two-qubit quantum correlations are unchanged. As mentioned above, the GWSs are not diagonal in the Bell basis, except $q = 0,\, \frac{1}{2},\, 1$. This property greatly complicates analytical calculations of correlation measures. So, for the Bell-non-diagonal GWSs, we present analytical formulas of the entanglement and nonlocality measures only, contrary to the corresponding results for the Werner states, which include also our formulas for the steerable weights.

We begin our detailed comparative analysis by presenting various theoretical relations between chosen correlation measures for the Werner states and GWSs showed in Figs. 4.2 and 4.3, respectively. These curves show the negativity N (or equivalently the concurrence C), the steerable weights S_2 and S_3, and the Bell nonlocality measure B as a function of the mixing parameter p. Each coloured region starts where a given correlation measure becomes non-zero with an increasing value of the mixing parameter p. We refer to these regions as quantum correlation regimes, which are also listed in Tables 4.1 and 4.2.

Table 4.1: Hierarchy of classes of correlations for the Werner states $\rho_{\text{W}}(p)$ depending on the mixing parameter p. The four regimes of vanishing or nonvanishing different classes of quantum correlations correspond to the regimes shown in Figs. 4.2 and 4.4.

Regime	B	$S_2 \equiv S_2^{ij}$	S_3	N	p	experiment
#1	$B = 0$	$S_2 = 0$	$S_3 = 0$	$N = 0$	$p \in [0,\, \frac{1}{3}]$	direct
#2	$B = 0$	$S_2 = 0$	$S_3 = 0$	$N > 0$	$p \in (\frac{1}{3},\, \frac{1}{\sqrt{3}}]$	direct
#3	$B = 0$	$S_2 = 0$	$S_3 > 0$	$N > 0$	$p \in (\frac{1}{\sqrt{3}},\, \frac{1}{\sqrt{2}}]$	direct
#4	$B = 0$	$S_2 > 0$	$S_3 > 0$	$N > 0$	$p \in \emptyset$	impossible
#5	$B > 0$	$S_2 > 0$	$S_3 > 0$	$N > 0$	$p \in (\frac{1}{\sqrt{2}},\, 1]$	direct

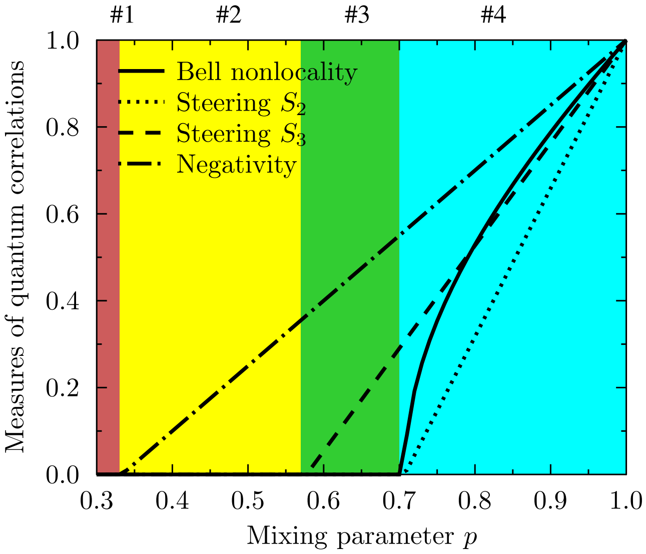


Figure 4.2: Four correlation regimes of the Werner states corresponding to those listed in Table 4.1. Note that regime #4 is missing. Theoretical plots for the negativity N (or, equivalently, the concurrence C), the steerable weights S_2 and S_3, and the Bell nonlocality measure B are shown as a function of the mixing parameter p. Exact definitions of the depicted quantum correlation measures are given in Sec. 4.5.

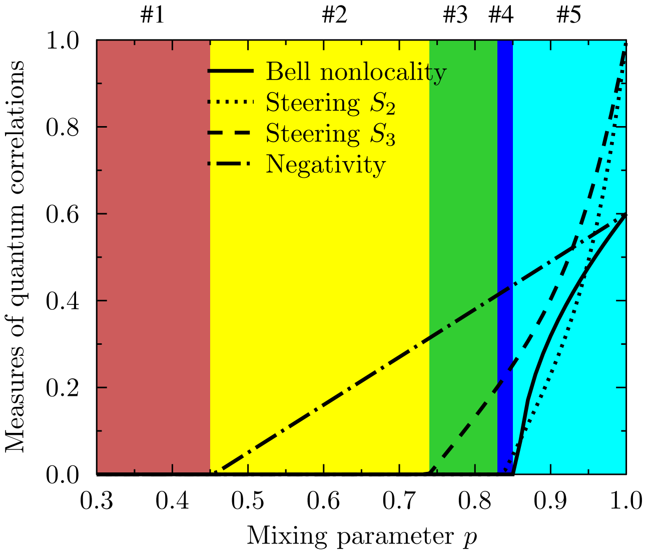


Figure 4.3: Five correlation regimes of the GWSs corresponding to the regimes in Table 4.2. Curves are analogous to those in Fig. 4.2, but for the superposition parameter $q = 0.9$ or, equivalently, $q = 0.1$.

Table 4.2: Hierarchy of classes of correlations exhibited by the Bell-non-diagonal GWSs $\rho_{\mathrm{GW}}(p,q)$ for different values of the mixing parameter p and a fixed value of the superposition parameter at $q=0.9$ or, equivalently, $q=0.1$. This table lists the five regimes shown in Figs. 4.3, 4.5, and 4.6(a). The threshold values read: $p'_N \equiv p_N(q) = 5/11 = 0.45(45)$ and $p'_B \equiv p_B(q) = 5/\sqrt{32} = 0.8574\cdots$, are given by Eqs. (4.17) and (4.22) for $q=0.9$ (or 0.1), respectively, while $p'_{S_3} \equiv p_{S_3}(q) = 0.7390\cdots$ and $p'_{S_2} \equiv p_{S_2}(q) = 0.8370\cdots$ were obtained numerically. The term *hybrid* experiment refers to averaging of two directly generated experimental states according to Eq. (4.24). 2MS and 3MS stand for two- and three-measurement scenarios, respectively.

Regime	states	B	S_2^{XY}	$S_2 \equiv S_2^{XZ} = S_2^{YZ}$	S_3	N	p	experiment
#1	separable	$B=0$	$S_2^{XY}=0$	$S_2=0$	$S_3=0$	$N=0$	$p\in[0,p'_N]$	direct
#2	3MS – unsteerablebutentangled	$B=0$	$S_2^{XY}=0$	$S_2=0$	$S_3=0$	$N>0$	$p\in(p'_N,p'_{S_3}]$	direct
#3	steerablein3MSbutnotin2MS	$B=0$	$S_2^{XY}=0$	$S_2=0$	$S_3>0$	$N>0$	$p\in(p'_{S_3},p'_{S_2}]$	direct
#4	Belllocalbut2MS – steerable	$B=0$	$S_2^{XY}=0$	$S_2>0$	$S_3>0$	$N>0$	$p\in(p'_{S_2},p'_B]$	hybrid
#5	Bellnonlocal	$B>0$	$S_2^{XY}>0$	$S_2>0$	$S_3>0$	$N>0$	$p\in(p'_B,1]$	direct

4.5 Hierarchy of the Classes of Correlations for Werner-Like States

4.5.1 Entanglement of Werner-Like States

It is well known that, for Werner states, the concurrence and negativity, which were defined in Sec. 4.3.1, are equal to each other and are given by a linear function of the mixing parameter p, i.e.,

$$N(\rho_{\rm W}) = C(\rho_{\rm W}) \;\;=\;\; \max\left[0,\,(3p-1)/2\right], \tag{4.15}$$

as shown in Fig. 4.2 by the dot-dashed curve. The good agreement of the negativities calculated for the theoretical and experimental Werner states is shown in Fig. 4.4(a).

We find that the negativity and concurrence for the GWSs read:

$$N(\rho_{\rm GW}) = C(\rho_{\rm GW}) = \max\left\{0,\,\tfrac{1}{2}\left[p(1+4\sqrt{x})-1\right]\right\}, \tag{4.16}$$

with $x = q(1-q)$, which is plotted in Fig. 4.3 by the dot-dashed curve. Figure 4.5(a) demonstrates the good fit of the negativities calculated for the theoretical and experimental GWSs for different values of the superposition parameter q. Note that not only $N(\rho_{\rm W})$ but also $N(\rho_{\rm GW})$ is a linear function of the mixing parameter p for a fixed value of the superposition coefficient q. In a special case for a pure state $|\phi_q\rangle$ (i.e., when $p=1$), Eq. (4.16) reduces to $N(|\phi_q\rangle) = C(|\phi_q\rangle) = 2\sqrt{q(1-q)}$.

Equation (4.16) vanishes for $p \in [0,\,p_N(q)]$ at the threshold value given by

$$p_N(q) = 1/\left[1+4\sqrt{q(1-q)}\right], \tag{4.17}$$

which is plotted in Fig. 4.6. It is seen that $N[\rho_{\rm W}(p)] > 0$ if $p > \frac{1}{3}$ and $N[\rho_{\rm GW}(p, 0.9)] > 0$ if $p > p'_N = \frac{5}{11}$. These threshold values are below compared with those for the other measures of quantum correlations and also marked in Figs. 4.6 and 4.7.

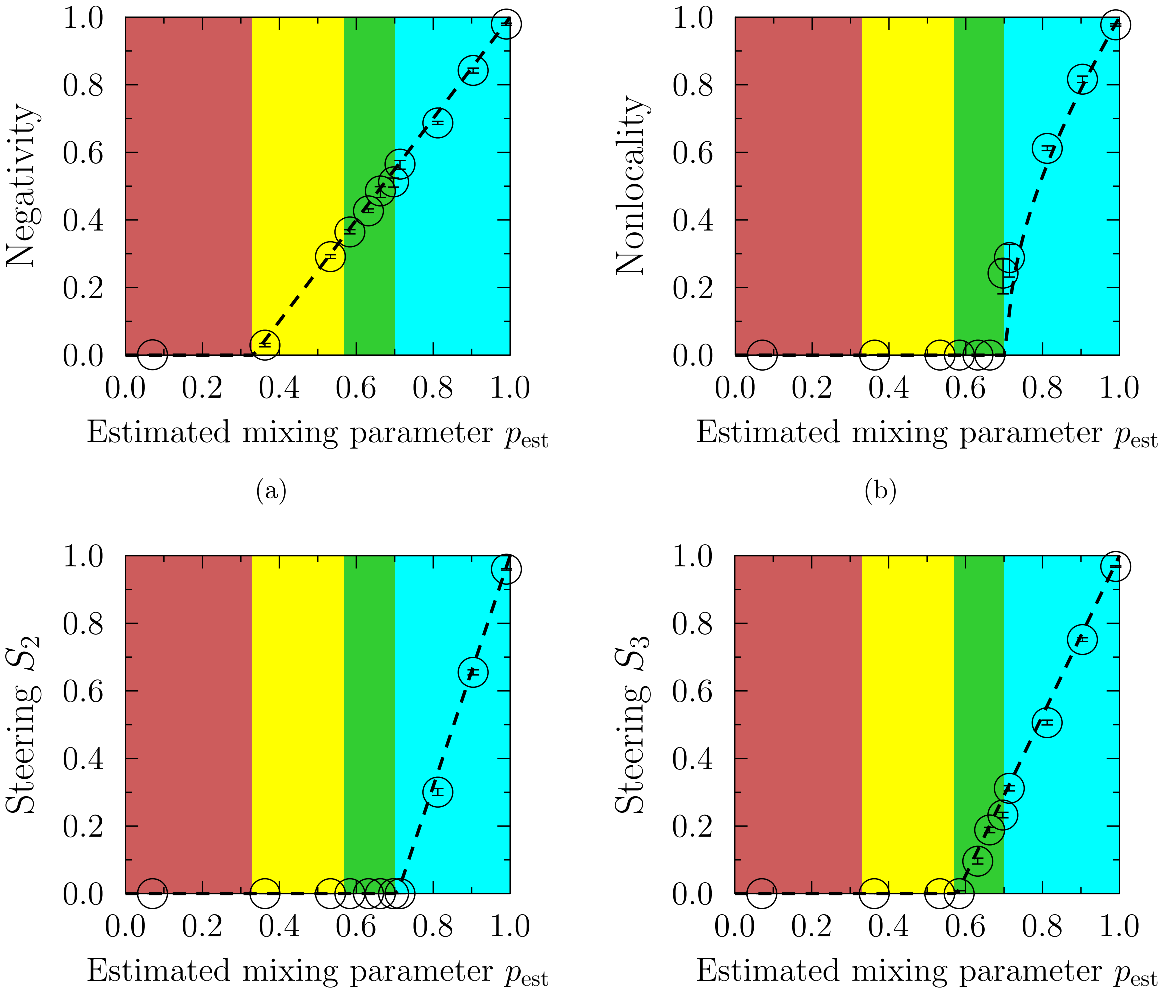
Note that $N(\rho_{\rm GW}) = C(\rho_{\rm GW})$ should hold for the ideal GWSs, including the Werner states. However, our experimental GWSs do not exactly satisfy this condition. Thus, we calculated both measures, because their difference shows how much our experimental states deviate from the ideal Werner states. These deviations quantify also the precision of our measurements. Specifically, the observed experimental differences between the negativity and concurrence were on the average 0.02% for the Werner states and 0.06% for the GWSs. Thus, on the scale of Figs. 4.4(a) and 4.5(a) one could not see any differences between $N(\rho^E_{\rm GW})$ and $C(\rho^E_{\rm GW})$.

4.5.2 Steering of Werner-Like States in the Three-Measurement Scenario

Steering in a 3MS on Alice's side can be quantified by the steerable weight S_3 of Ref. [295], as defined as an SDP in Appendix C.2. We find that this steerable weight S_3 for the Werner states is a *linear* function of the mixing parameter p, specifically,

$$S_3(\rho_{\rm W}) = \max\left(0,\,\frac{\sqrt{3}p-1}{\sqrt{3}-1}\right), \tag{4.18}$$

which means that the state $\rho_{\rm W}(p)$ is steerable in the 3MS if $p > \frac{1}{\sqrt{3}}$ [see Fig. 4.4(d) and Table 4.1]. By contrast to this, the steerable weight S_3 for the GWSs is a *nonlinear*



(a)

(b)

(c)

(d)

Figure 4.4: Quantum correlations for the theoretical and experimental Werner states as a function of the estimated mixing parameter p_{est}: (a) negativity N, (b) Bell nonlocality measure B, as well as the steerable weights (c) S_2 and (d) S_3.

function of the mixing parameter p for $q \neq \frac{1}{2}$. This is shown for $q = 0.9$ in Fig. 4.5(d). It can be seen that these GWSs are steerable for $p > p_{S_3} = 0.7390$ (see also Table 4.2). This means that $\rho_{\mathrm{GW}}(p, 0.9)$ is steerable for a much shorter range of the mixing parameter p than that for $\rho_{\mathrm{W}}(p) \equiv \rho_{\mathrm{GW}}(p, \frac{1}{2})$. Figures 4.4(d) and 4.5(d) show the weight S_3 for our experimental states compared to those for the theoretical states. These results show good agreement of the theory with our experimental results.

4.5.3 Steering of Werner-like States in Two-Measurement Scenarios

To quantify steering of the Werner states and GWSs in 2MSs on Alice's side, we apply the steerable weights S_2^{ij} of Ref. [295] defined in Appendix C.3.

We find that the weights S_2^{ij} for the Werner states are equal to each other, $S_2(\rho_{\mathrm{W}}) \equiv S_2^{XY}(\rho_{\mathrm{W}}) = S_2^{XZ}(\rho_{\mathrm{W}}) = S_2^{YZ}(\rho_{\mathrm{W}})$, being a *linear* function of the mixing parameter p,

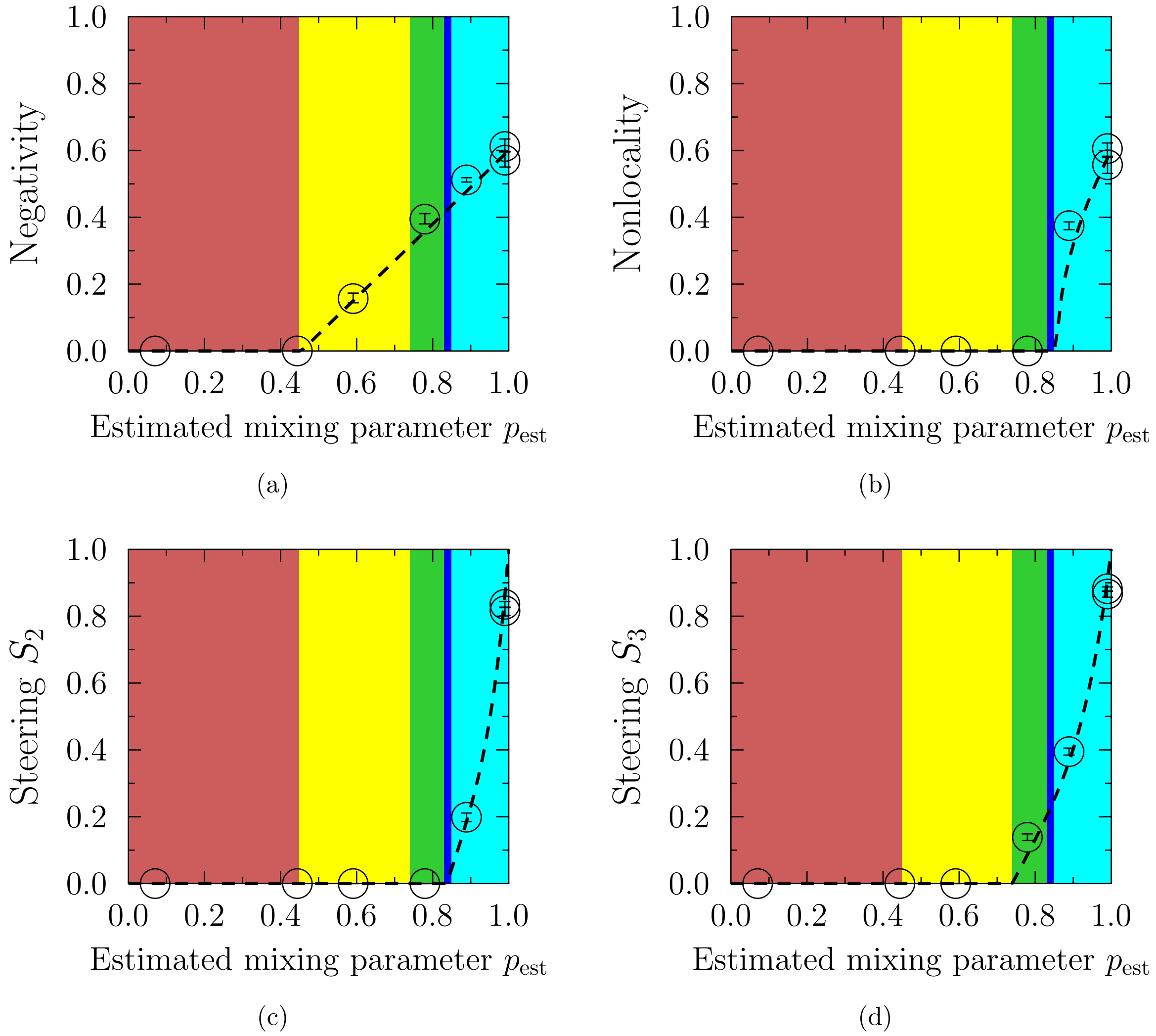
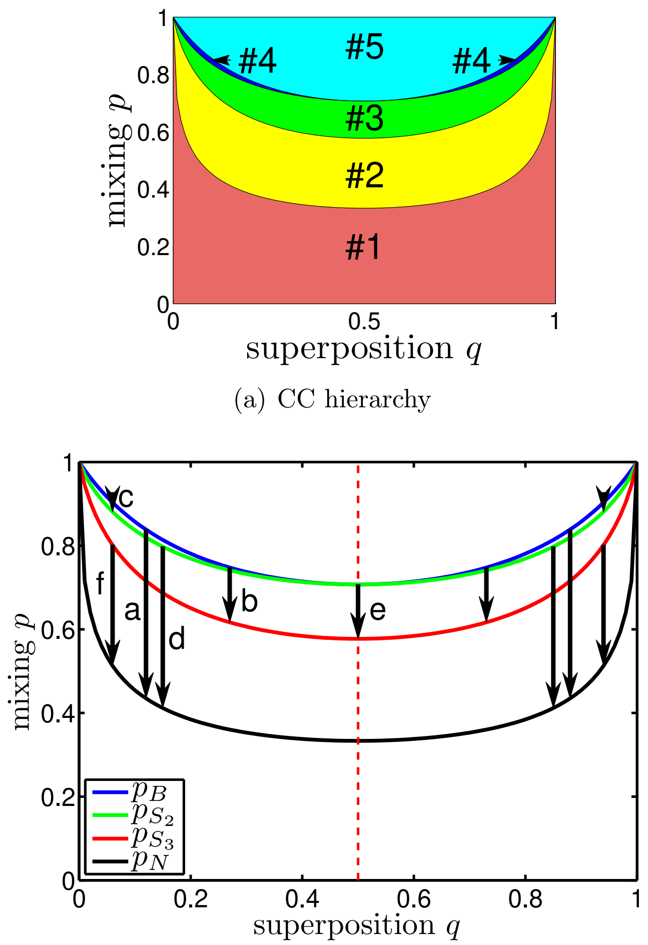


Figure 4.5: Same as in Fig. 4.4 but for the GWSs for the estimated superposition coefficient $q_{\rm est} \approx q = 0.9$ (see the text for details).

i.e.,

$$S_2(\rho_{\rm W}) = \max\left(0, \frac{\sqrt{2}p - 1}{\sqrt{2} - 1}\right). \tag{4.19}$$

This implies the steerability of the states in the 2MS if $p > \frac{1}{\sqrt{2}}$ [see Fig. 4.4(c) and Table 4.1]. However, the steerable weights for the GWSs become much more complicated. We find that $S_2^{XY}(\rho_{\rm GW}) \leq S_2^{XZ}(\rho_{\rm GW}) = S_2^{YZ}(\rho_{\rm GW}) \equiv S_2(\rho_{\rm GW})$, and there exist two threshold values p'_{S_2} and p'_B, as listed in Table 4.2. Specifically, (i) $S_2^{XZ}(\rho_{\rm GW}) = S_2^{YZ}(\rho_{\rm GW}) > 0$ if $p > p'_{S_2} = 0.8370\cdots$ and (ii) $S_2^{XY}(\rho_{\rm GW}) > 0$ if $p > p'_B = \frac{5}{\sqrt{32}}$, which is the same threshold parameter as that for the Bell nonlocality measure $B > 0$, as discussed above. Moreover, the dependence of $S_2^{ij}(\rho_{\rm GW})$ on the mixing parameter p becomes nonlinear for $q \neq \frac{1}{2}$. Different values of the threshold parameters for p'_B and p'_{S_2} imply the occurrence of the region #4 for the GWSs, which is shown in Figs. 4.3, 4.6(a), and 4.7(c), and explained in detail in Sec. 4.6.1.



(a) CC hierarchy

(b) Optimal robustness

Figure 4.6: Threshold mixing parameters $p_i(q)$ versus the superposition parameter q for the GWSs. (a) The threshold curves separate the five regimes in the hierarchy of the classes of quantum correlations, which are listed in Table 4.2. (b) Transitions between various curves, requiring the largest amount of white noise, are indicated by arrows. It is seen that the only arrow e for the Werner states (i.e., the GWSs at $q = 1/2$) is marked for the transition between the curves $p_{S_2}(q)$ and $p_{S_3}(q)$. All the other arrows are plotted at $q \neq 1/2$. This explains the meaning of enhanced robustness of the Bell-non-diagonal GWSs against white noise compared to that of the Werner states. The locations at q_{opt} and lengths of the labelled arrows are listed in Table 4.3. The unlabelled arrows are located at $q'_{\text{opt}} = 1 - q_{\text{opt}}$.

4.5.4 Nonlocality of Werner-Like States

To estimate the degree of quantum nonlocality or, equivalently, to quantify the violation of the Bell-CHSH inequality for two-qubit states [87], we use the Horodecki measure [303, 304], which is as defined in Sec. 4.3.3.

The Bell nonlocality measure for the Werner states reads as

$$B(\rho_{\text{W}}) = \sqrt{\max(0,\, 2p^2 - 1)}, \tag{4.20}$$

which instantly implies a standard result that the Werner states are nonlocal if $p > \frac{1}{\sqrt{2}}$ (see also Table 4.1). However, if $p \in (\frac{1}{3}, \frac{1}{\sqrt{2}})$, the Werner states are entangled without BIV (admitting an LHV model), as already demonstrated by Werner in 1989 in [98].

We find that the Bell nonlocality measure for the GWSs is given by

$$B(\rho_{\rm GW}) = \max\left\{0,\ \sqrt{p^2[1+4q(1-q)]-1}\right\}, \tag{4.21}$$

Note that for pure states ($p=1$), Eq. (4.21) reduces to the standard result $B(|\phi_q\rangle) = N(|\phi_q\rangle) = 2\sqrt{q(1-q)}$. It can be seen that $B(\rho_{\rm GW})$ is zero for the values of the mixing parameter in the range $p \in [0, p_B(q)]$ with the threshold value given by

$$p_B(q) = 1/\sqrt{1+4q(1-q)}, \tag{4.22}$$

which is plotted in Fig. 4.6. For the diagonal GWSs (with $q=\frac{1}{2}$), we can reproduce the well-known threshold value $p_B(\frac{1}{2}) = \frac{1}{\sqrt{2}}$ for the Werner states. In another special case for $q = 0.9$, which was set in our experiments, we have the threshold value $p'_B \equiv p_B(q = 0.9) = p_B(q = 0.1) = \frac{5}{\sqrt{32}}$. Thus, the GWSs $\rho_{\rm GW}(p, 0.9)$ for $p \in (p'_N,\, p'_B) = (\frac{5}{11},\, \frac{5}{\sqrt{32}})$ are entangled without Bell nonlocality, which occurs for a wider range of the mixing parameter p compared to that for the Werner states, i.e., $p'_B - p'_N \approx 0.4029 > \frac{1}{\sqrt{2}} - \frac{1}{3} \approx 0.3738$, as it is explained in detail in Sec. 4.6.2.

In Fig. 4.4(b) we plotted $B(\rho_{\rm W})$ in comparison to the numerically calculated $B(\rho^E_{\rm W})$ for the experimental Werner states $\rho^E_{\rm W}(p)$ for various values of the mixing parameter p and fixed $q = 0.9$. Analogous results for the Bell nonlocality measure $B(\rho_{\rm GW})$ for the GWSs generated experimentally, $\rho^E_{\rm GW}(p; q = 0.9)$, are shown in Fig. 4.5(b) in comparison to those for the ideal GWSs, $\rho_{\rm GW}(p; q = 0.9)$. Note that $B(\rho_{\rm GW}) > 0$ if $p > p'_B$ (see also Table 4.2), assuming $q = 0.9$ or 0.1, which is clearly larger than the corresponding threshold value $\frac{1}{\sqrt{2}}$ for the Werner states. Both Figs. 4.4(b) and 4.5(b) show relatively good agreement of our experimental results compared to the corresponding theoretical predictions. More details about the accuracy of our experimental results were given in Sec. 4.4.1.

4.6 Counterintuitive results

Here we present, arguably, the most interesting theoretical results of our research for the states generated experimentally (either directly or in a hybrid way).

4.6.1 Steerability S_2 Without Bell Nonlocality

Here we show that Bell-non-diagonal GWSs are steerable in 2MSs on Alice's side but still admit an LHV model. So the existence of such quantum correlations cannot be revealed by the violation of the Bell-CHSH inequality. The GWSs exhibiting the S_2-steerability without Bell nonlocality correspond to the regime #4 in Table 4.2 and are shown in Figs. 4.3, 4.6(a), and 4.7(c).

Our analytical and numerical results clearly demonstrate that the regime #4 cannot be observed for the Werner states, for which $p_B(\frac{1}{2}) = p_{S_2}(\frac{1}{2})$ holds, as can be seen in Fig. 4.3. However, this degeneracy is broken for the GWSs with $q \neq 0,\, \frac{1}{2},\, 1$.

We find this result interesting, although the amount of the required white noise destroying the correlations is small [i.e., $\max_q \Delta_{B,S_2}(q) = 0.023$] compared to all the other cases shown in Fig. 4.7, except Fig. 4.7(e).

Moreover, the regime #4 can be observed for the mixing parameter p limited to a very narrow range $[p'_{S_2},\, p'_B] \approx [0.837,\, 0.857]$ assuming $q = 0.9$ (or, equivalently, 0.1), as shown in Figs. 4.5(b) and 4.5(c). We have experimentally generated the GWSs for $p = 0.8$ and $p = 0.9$, but unfortunately they are outside the desired range $[p'_{S_2},\, p'_B]$.

To solve this problem, we recall that mixtures of any two GWSs, say $\rho_{\mathrm{GW}}(p_1,\, q)$ and $\rho_{\mathrm{GW}}(p_2,\, q)$ for a fixed value of q, are also GWSs. Specifically,

$$\rho^{E}_{\mathrm{GW}}(p,q) = \frac{p_2 - p}{p_2 - p_1}\rho_{\mathrm{GW}}(p_1,q) + \frac{p - p_1}{p_2 - p_1}\rho_{\mathrm{GW}}(p_2,q). \tag{4.23}$$

Thus, we can use this property to produce (or simulate) a GWS, which was not measured directly in our experiment, e.g.,

$$\rho_{\mathrm{GW}}(0.85{,}q) = \frac{1}{2}[\rho^{E}_{\mathrm{GW}}(0.8,q) + \rho^{E}_{\mathrm{GW}}(0.9,q)], \tag{4.24}$$

simply by balanced post-measurement numerical mixing of the two experimental GWSs $\rho^{E}_{\mathrm{GW}}(p,q)$ for $p = 0.8$ and 0.9 assuming $q = 0.9$. We refer to this method as a *hybrid* experimental generation, as written in Table 4.2 for the regime #4. By contrast to this regime, we have *directly* generated experimental states in all other regimes listed in Tables 4.1 and 4.2. Moreover, all the states plotted in our figures correspond to those *directly* generated experimentally without using any post-measurement numerical mixing.

Our prediction of the existence of states in the regime #4 is a surprising result and our experiment has just confirmed it. This prediction seems to be especially counterintuitive in the context of the Girdhar-Cavalcanti article on "All two-qubit states that are steerable via CHSH-type correlations are Bell nonlocal" [318] (see also Refs. [319, 320]), which seemingly implies the impossibility of generating states in this regime. However, the Girdhar-Cavalcanti theorem is valid in 2-2 measurement scenario only, i.e., for "a scenario employing only correlations between two arbitrary dichotomic measurements on each party" [318]. Our steering measures S_2 and S_3 refer to a 2-3 and 3-3 measurement scenarios, respectively. Indeed, we always assume a full tomography on Bob's side corresponding to the measurement of the three Stokes parameters: $\langle\sigma_x\rangle$, $\langle\sigma_y\rangle$, and $\langle\sigma_z\rangle$, while the projective measurements on Alice's side can be limited to 2MS or 3MS. It is seen that our and Girdhar and Cavalcanti's steering results refer to different measurement scenarios. Thus, the observation of the regime #4 in our steering scenarios does not imply the violation of the Girdhar-Cavalcanti theorem.

4.6.2 Increased Robustness Against White Noise of Bell-Non-diagonal Generalised Werner States

Even a quick analysis of Figs. 4.6(b) and 4.7, and Table 4.3 shows one of the main theoretical results of this Chapter, i.e., increased robustness against white noise of Bell-non-diagonal GWSs compared to the standard (Bell-diagonal) Werner states. Below we give a more intuitive and detailed explanation of this result.

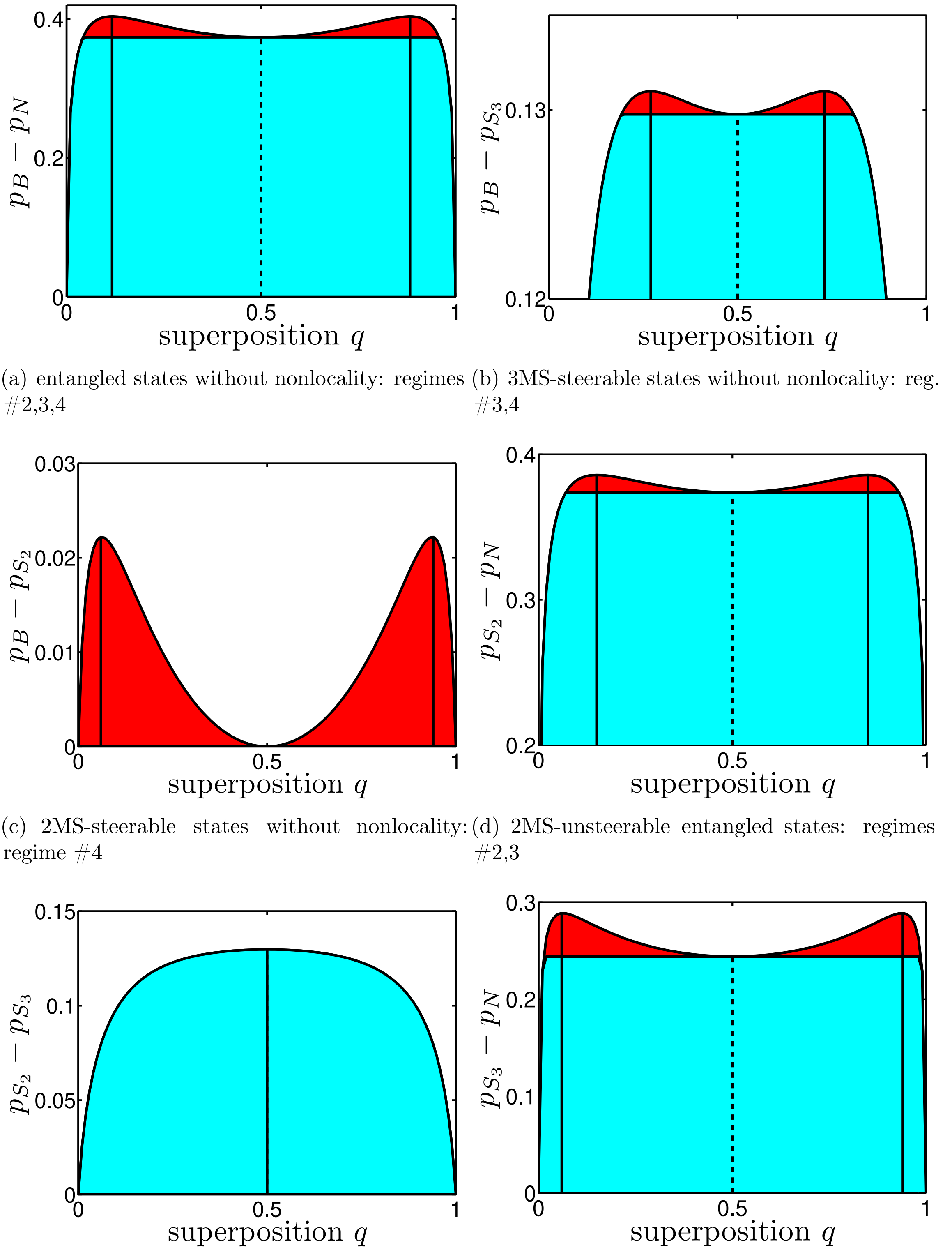
We recall that Bell diagonal (non-diagonal) GWSs are the maximally (partially) entangled states affected by white noise. Let us analyse the amount of white noise (i.e., $1 - p$), which is necessary to make the transition of a GWS from one threshold value, say $p_i(q)$, to another (final) value, $p_f(q)$, for a given value of the superposition parameter q. Thus, the required white noise can be quantified by

$$\Delta_{if}(q) \equiv p_i(q) - p_f(q) \tag{4.25}$$

for $i \neq f \in \{N,\, S_3,\, S_2,\, B\}$, which is plotted in Fig. 4.7 and numerically given in Table 4.3.

Table 4.3: Transitions between the threshold values of different correlations of the GWSs for the optimal superposition parameter q_{opt}, which maximizes the white-noise robustness, $\Delta_{if}(q_{\text{opt}}) = p_i(q_{\text{opt}}) - p_f(q_{\text{opt}})$ for $i \neq f \in \{N,\, S_2,\, S_3,\, N\}$. These transitions correspond to the arrows shown in Fig. 4.6(b), and the length of a given arrow is given by $\Delta_{if}(q_{\text{opt}})$. The parameter p_i (p_f) is the threshold value of the mixing parameter p for the initial (final) class of correlations, or, equivalently, the position of the beginning (end) of the corresponding arrow. The last column shows the relative robustness with respect to the standard Werner states (i.e., the GWS for $q = 1/2$). Note that, for every q_{opt}, there is a second optimal value of the superposition parameter, $q'_{\text{opt}} = 1 - q_{\text{opt}}$, exhibiting the same quantum correlation properties.

Transition	q_{opt}	$p_i(q_{\text{opt}})$	$p_f(q_{\text{opt}})$	$\Delta_{if}(q_{\text{opt}})$	$\Delta_{if}(\frac{1}{2})$	$\Delta_{if}(q_{\text{opt}}) - \Delta_{if}(\frac{1}{2})$
(a) $p_B \to p_N$	0.1170	$p_B = 0.8412$	$p_N = 0.4375$	0.4037	0.3738	0.0299
(b) $p_B \to p_{S_3}$	0.2692	$p_B = 0.7481$	$p_{S_3} = 0.6171$	0.1310	0.1298	0.0012
(c) $p_B \to p_{S_2}$	0.0625	$p_B = 0.9001$	$p_{S_2} = 0.8779$	0.0222	0	0.0222
(d) $p_{S_2} \to p_N$	0.1508	$p_{S_2} = 0.7971$	$p_N = 0.4113$	0.3858	0.3738	0.0120
(e) $p_{S_2} \to p_{S_3}$	0.5000	$p_{S_2} = 0.7071$	$p_{S_3} = 0.5774$	0.1298	0.1298	0
(f) $p_{S_3} \to p_N$	0.0630	$p_{S_3} = 0.7959$	$p_N = 0.5071$	0.2888	0.2440	0.0448



(a) entangled states without nonlocality: regimes #2,3,4

(b) 3MS-steerable states without nonlocality: reg. #3,4

(c) 2MS-steerable states without nonlocality: regime #4

(d) 2MS-unsteerable entangled states: regimes #2,3

(e) steerable states in 3MS but not in 2MS: regime #3

(f) 3MS-unsteerable entangled states: regime #2

Figure 4.7: Differences $\Delta_{ij}(q) = p_i(q) - p_j(q)$ of the threshold mixing parameters versus the superposition parameter q for the GWSs corresponding to the transitions shown by the red arrows in Fig. 4.6. The red-coloured regions show explicitly the improved robustness against white noise of the Bell-non-diagonal GWSs compared to the diagonal ones in the Bell basis (i.e., the standard Werner states), except the case shown in panel (e). Combined red and cyan regions correspond to the regimes indicated in the captions of all these panels and those listed in Table 4.2.

For example, let us consider the maximally entangled Werner state admitting an LHV model, i.e., $\rho_{\mathrm{W}}(p_B)$. Our question is about the minimum amount of white noise which should be added to this state to make it separable, i.e., $\rho_{\mathrm{W}}(p_N)$. The answer is $\Delta_{BN}(q=\frac{1}{2}) = \frac{1}{\sqrt{2}} - \frac{1}{3} \approx 0.3738$. However, in the case of the GWSs, the minimum amount of white noise needed to convert the maximally entangled GWS $\rho_{\mathrm{GW}}(p_B(q),q)$, admitting an LHV model, to the closest separable state $\rho_{\mathrm{GW}}(p_N(q),q)$ can be larger than that for the Werner states, $\Delta_{BN}(q) > \Delta_{BN}(\frac{1}{2})$, for some values of the superposition parameter q corresponding to the red regions in Fig. 4.7(a). Assuming that $q = 0.9$ (as set in our experiments), we obtain $\Delta_{BN}(0.9) = 0.4029 > 0.3738$. Actually, the largest value $\max_q \Delta_{BN}(q) = \Delta_{BN}(q') = 0.4037$ can be achieved for $q' = 0.8829$ and $1-q'$, which can be calculated by solving the following sixth-order equation $(1+4x^2)^3 = x^2(1+ + 4x)^4$ with $x = \sqrt{q'(1-q')}$.

The same conclusion about higher robustness of the Bell-non-diagonal GWSs against white noise compared to that of the Werner states can also be drawn for other transitions, indicated by the arrows in Figs. 4.6(b) and 4.7 and also listed in Table 4.3. The only exception is observed for the transition corresponding to $\Delta_{S_2,S_3}(q)$, which reaches the largest value for the Werner states, as shown in Fig. 4.7(e).

More white noise should be added to a Bell state to reach any threshold value p_j compared to that for any partially entangled state, because $1 - p_j(\frac{1}{2}) > 1 - p_j(q)$ for $q \neq \frac{1}{2}$ and $j \in \{N,\ S_3,\ S_2,\ B\}$, i.e., the amount of white noise destroying completely any quantum properties of the states, including entanglement, steering, and nonlocality. So, in that sense, the Werner states are more robust against white noise than the non-diagonal GWSs. However, by choosing proper reference states or proper transitions, one can draw the opposite conclusion, as we have demonstrated in this section and it is clearly visualized in Figs. 4.6(b) and 4.7.

4.6.3 Increased Robustness of Steering for a Larger Number of Measurements

Our research is focused on analysing steering in only the two- and three-measurement scenarios. Nevertheless, in Appendix C.4 we also discuss steering in multi-measurement scenarios including the case of steering in the limit of an infinite number of types of available measurements.

Specifically, we analyse lower and upper bounds on steering for a much larger number n of measurements (even $n = 136$). We demonstrate that entangled GWSs, which are unsteerable for a very large (or in principle infinite) number of measurements, can be more robust against white noise if they are non-diagonal in the Bell-state basis compared to the diagonal ones (i.e., the Werner states).

First, we recall that, while the analysed entanglement measures reveal the property of a given state independent of its measurements, the measures for steerability and Bell nonlocality additionally depend on the available measurements.

Thus, one can raise the following questions: (i) whether a larger spread (corresponding to higher robustness) between different classes of correlations in the GWSs is an artefact stemming from the fact that the considered steering and Bell-nonlocality measures perform better on less entangled states? This question can also be rephrased differently: (ii) Can one expect to find the same robustness behaviour for some tight bounds for Bell nonlocal states and steerable states (taking into account any measurement scenario)?

We answer these questions by calculating tight upper (p_S^{up}) and lower (p_S^{low}) bounds on steering for the GWSs for a large number of measurements. These numerical bounds strongly suggest that the hierarchy also holds for an arbitrary number of measurements. Indeed, similar analysis can be performed for Bell nonlocality of the GWSs, as discussed in [301], to show that the Horodecki measure fully describes the nonlocality in two-qubit states with no restriction on the number of measurements.

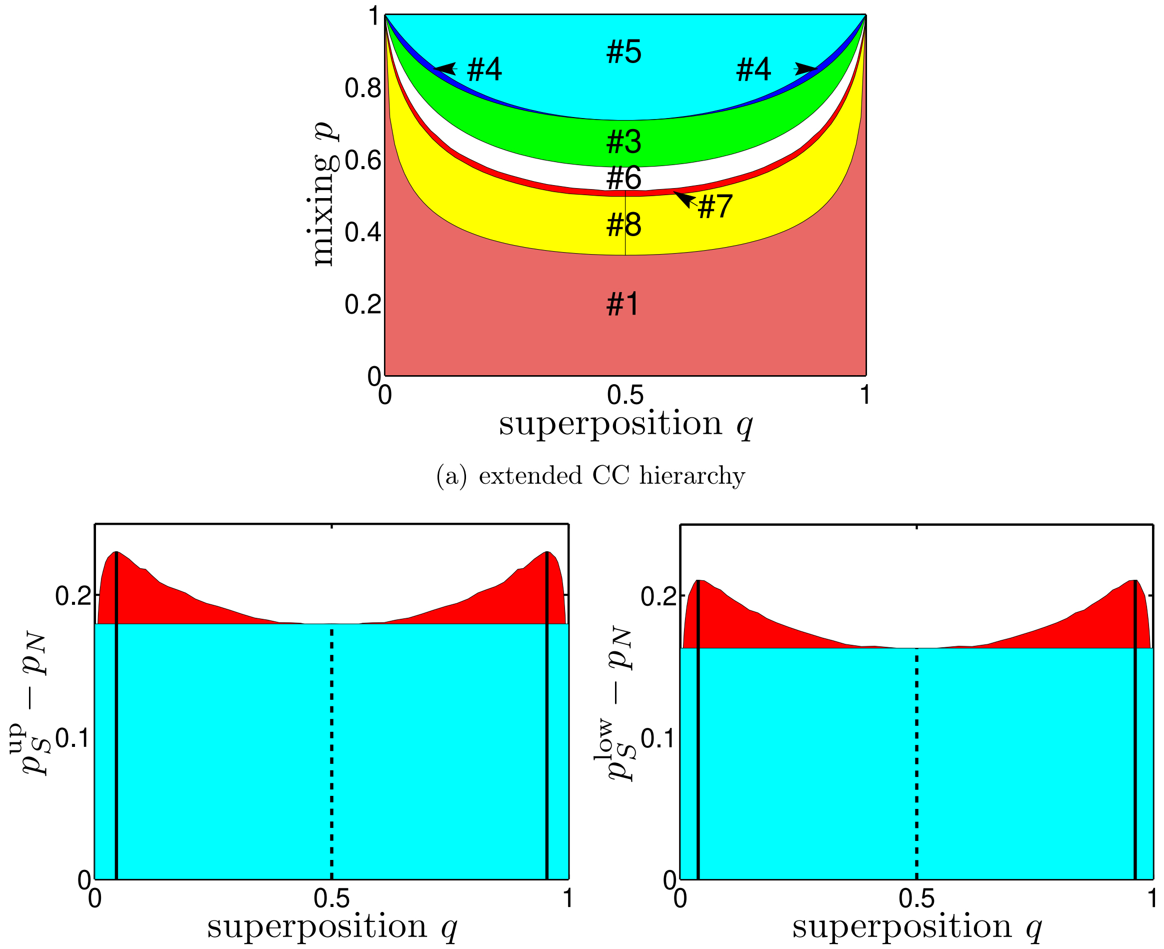
Two bounds on multi-measurement steering are shown in Fig. 4.8. Specifically, the upper bound $p_S^{\rm up}$, which corresponds to the border curve between the regimes #6 and #7 in Fig. 4.8(a), is a sufficient condition for the steerability of the GWSs. This bound was obtained numerically in Refs. [301, 302] from a criterion of Ref. [242] using an SDP technique for 13 measurements on the Bloch sphere. Moreover, the lower bound $p_S^{\rm low}$, which is shown by the curve between the regimes #7 and #8, corresponds to a sufficient condition of the unsteerability of the GWSs based on the algorithm of Refs. [301, 302] for constructing LHS models assuming 136 projective optimal (or almost optimal) measurements corresponding to the fourth level of their algorithm. The curves for both $p_S^{\rm low}$ and $p_S^{\rm up}$ are plotted using the numerical data of Ref. [302]. Thus, any GWS above the $p_S^{\rm up}$ curve in Fig. 4.8(a) is steerable, while any state below the $p_S^{\rm low}$ curve is unsteerable. The unsteerability of some of the states in the regime #7 (lying close to the border curve $p_S^{\rm low}$) can be tested by applying the algorithm of Refs. [301, 302] for higher levels, which corresponds to analysing a larger number of measurements ($n \gg 136$). However, it is unclear whether any GWSs lying inside the regime #7 can be steerable in the limit of $n \to \infty$.

Figure 4.8(a) shows that by including the criteria for steering in multi-measurement scenarios, in addition to S_2 and S_3, one can study a CC hierarchy which is more refined than that in Fig. 4.6(a). Note that the regime #2 in Fig. 4.6(a) corresponds to the sum of the regimes #6, #7, and #8 shown in Fig. 4.8(a).

To answer the questions raised above, we plotted the differences $p_S^{\rm up}-p_N$ and $p_S^{\rm low}-p_N$ in Figs. 4.8(b) and 4.8(c), respectively. Both figures are quite similar and show that the optimal robustness against noise is observed for the Bell *non-diagonal* GWSs with the superposition parameter $q \neq \frac{1}{2}$ (denoted by black solid lines). Thus, even without knowing the exact threshold values between the steerability and unsteerability of the GWSs in the limit of an infinite number of measurements, one can conclude that the predicted optimal robustness is *not* an artefact, at least for the cases shown in Figs. 4.8(b) and 4.8(c). This is the answer to question (i). Concerning the above-mentioned question (ii), the robustness behaviour is different for different $p_i = p_S^{\rm up}$, $p_S^{\rm low}$, p_{S_2}, p_{S_3}. Indeed, the optimal values of the superposition parameter q maximizing $p_i - p_N$ depend on i. However, this property does not weaken our conclusion about higher robustness against white noise of some Bell non-diagonal GWSs compared to that of the Werner states.

4.7 Conclusions

The main purpose of this work was to analyse a CC hierarchy of theoretical and experimental Werner states and their generalization, i.e., the Bell-non-diagonal GWSs. We recall that the considered GWSs are the mixtures of partially entangled two-qubit pure states (not only of a Bell state) and the maximally mixed state (white noise). We have shown that the Bell-non-diagonal GWSs exhibit a more refined CC hierarchy compared to that of the Bell-diagonal GWSs, i.e., the Werner states.



(a) extended CC hierarchy

(b) supremum of unsteerable entangled states: reg. #7,8

(c) unsteerable entangled states: regime #8

Figure 4.8: (a) Same as in Fig. 4.6(a) but with additional regions (regimes) #6, #7, and #8 of steerability in the limit of a large number of measurements. Also shown are the differences (b) $p_S^{\rm up} - p_N$ and (c) $p_S^{\rm low} - p_N$, where p_N is given by Eq. (4.17). The curve $p_S^{\rm up}$ is the border between the regimes #6 and #7, which corresponds to a sufficient condition for steerability of Ref. [242], while the curve $p_S^{\rm low}$ is the border between the regimes #7 and #8, which corresponds to a sufficient condition of unsteerability based on the algorithm and numerical data of Refs. [301, 302] assuming 136 projective measurements. Panels (b,c) show, analogously to those in Fig. 4.7, that the optimal robustness of steering assuming a large number of measurements compared to the entanglement of the GWSs is observed for the Bell non-diagonal GWSs with the superposition parameter $q \neq 1/2$ (as denoted by solid blue lines).

By tuning the mixing and superposition parameters of the GWSs, we have experimentally generated and tomographically reconstructed such GWSs, which reveal the hierarchy of the following classes of correlations: #1 separability, #2 entanglement without steerability in 3MS, #3 steerability in the 3MS but not steerable in the 2MS, #4 steerability in the 2MS without violating the Bell-CHSH inequality (so admitting LHV models), and #5 Bell nonlocality, which cannot be explained within LHV models. Note that the case of steering is a little more subtle since the measures assume specific measurements. Thus, we have also analysed a sufficient condition for unsteerability assuming a very large number (i.e., 136) of measurements.

In particular, we found five different parameter regimes of the GWSs, including the states which are steerable in a 2MS without violating Bell inequalities and thus corresponding to the regime #4. This is a counterintuitive result, especially when compared with the Girdhar-Cavalcanti theorem [318], which states that: "All two-qubit states that are steerable via CHSH-type correlations are Bell nonlocal" [318]. In Sec. 4.6.1 we have explained why the observation of the regime #4 in our steering scenarios does not imply the violation of the Girdhar-Cavalcanti theorem. We also demonstrated that the regime #4 cannot be observed for the usual Werner states.

Moreover, we have shown that the robustness against the white noise for, e.g., steerable states admitting LHV models can be stronger for some Bell-non-diagonal GWSs than that for the diagonal GWSs (i.e., the Werner states). This can be achieved by properly choosing the value of the superposition coefficient q, as shown in Figs. 4.6(b) and 4.7. Thus, we addressed the problem of optimal robustness of states against white noise. Specifically, we analysed threshold values (curves) separating the five regimes of quantum correlations. Then we could find optimal transitions between various curves corresponding to the largest amount of white noise or, in other words, to the largest spread in the hierarchy. Thus, we discovered the optimal Bell-non-diagonal GWSs which are more robust against white noise than the Werner states.

Furthermore, we considered lower and upper bounds on steering in multi-measurement scenarios. Again we demonstrated better robustness against white noise of some unsteerable entangled Bell-non-diagonal GWSs compared to the diagonal ones. Thus, such enhanced robustness is not limited to only the two- and three-measurement steering scenarios; it can also be observed for steering in the limit of a large number of measurements.

Possible applications of the discovered optimal robustness against white noise can be found for quantum cryptography. For instance, imagine that legitimate users of some secure quantum communications system want to use steering (or entanglement) such that it should not be detected by the violations of Bell inequalities by others. Thus, assuming that the communication is via a depolarizing channel, it is convenient to use partially steerable (or partially entangled) states which are Bell local and are the most robust against white noise. Such optimal states are indicated by arrows in Fig. 4.6(b).

Our study of the hierarchy of the classes of spatial quantum correlations can be generalised to analyse a hierarchy of their temporal or spatio-temporal analogues. Indeed, the concepts of spatial and temporal quantum correlations are closely related. Formally, it is enough to replace two-qubit measurements for testing spatial correlations by measurements on a single qubit, followed by transmission through a channel, to reveal temporal correlations, as explained in the example of spatial and temporal steering in Ref. [298]. Thus, many of the results discussed here for spatial correlations can also be generalised to temporal correlations. We explicitly indicated such relations in various sections of this Chapter. Analyses of CC hierarchies of temporal correlations can lead to a deeper understanding of, e.g., quantum causality [321] or enable designing new types of quantum cryptosystems and finding new methods of breaking the standard ones.

We believe that analysing such CC hierarchies is interesting concerning both fundamental aspects of quantum mechanics and possible cryptographic applications for, e.g., secure communication, secure information retrieval, or zero-knowledge proofs of (quantum) identity.

Conclusion

> “God makes everything happen at the right time. Yet none of us can ever fully understand all he has done, and he puts questions in our minds about the past and the future.”
> *Ecclesiastes 3:11 in translation of Contemporary English Version*
>
> “On ve svém čase učinil všechno krásné a do srdce jim vložil touhu po věčnosti, jenže člověk není schopen pochopit ani počátek ani konec toho, co Bůh koná.”
> *Kazatel 3:11 v překladu Slovo na Cestu*

Nowadays, increasing number of companies has recognised that quantum physics is no longer a subject of academic discussions among physicists but rather it opens up unprecedented opportunities for solving intricate issues and tasks. They invest strenuous efforts and considerable funds to jump on the bandwagon of a very promising field, quantum computing, hoping to find solutions to, e.g., industrial, analytical and other practical tasks that have been difficult to tackle before. Quantum communications is another field that has found its application in practice, especially for the prospect of security warranted by laws of Nature. Thus, quantum technologies are gradually becoming part of our lives.

Since it was formulated more than 80 years ago, a phenomenon of quantum entanglement has become an indispensable part of quantum physics and in time it found its application (among others) in those above mentioned fields of significance. Thus, its detailed study is an imperative for further development of any practical application of quantum technologies. Additionally, entanglement is of interest even to theoretical perspective.

The goal of this doctoral Thesis is to present three experiments aim of which is either to improve a quantum money protocol or to study quantum correlations and their hierarchy on Werner states made up of two and three qubits subjected to controllable white noise. The common feature of the two remaining experiments is the investigation of generalised Werner states, i.e., gGHZ states influenced by white noise. This family of states realistically showcases deterioration of entanglement during, e.g., quantum communication caused by presence of noise in the communications channel. Since two- and three-qubit Werner states are widely used to model quantum information transmissions through realistic channels, results of our research might eventually find its practical usage. All presented experiments were implemented on the platform of linear optics and information was encoded into polarisation and spatial modes of single photons. Therefore, the main components used for building of these experiments are described in the Chapter 1 along with source of photons and procedures of encoding and analysis of qubits.

A successful attack on a quantum money (QM) scheme, which is based on quantum retrieval games, is presented within the scope of the Chapter 2. This attack was realised by means of imperfect cloning on a beam splitter with the frequency of cloning deliberately lowered in order to hide the eavesdropping in noise. We expected that the bank uses an unknown secret function, like for instance hash function, and a secret number – salt, to encode all issued banknotes. The main result of this experiment is that despite using hash function, the secret number has been guessed. Even though quantum physics possesses fundamental means (such as no-cloning theorem) to provide security of quantum communication, protection is not guaranteed unconditionally. Security of quantum communication is affected by several factors, such as the noise threshold, which the bank still considers safe. Further assessment of security has to take place before this type of QM protocol becomes a viable quantum technology. It is worth stressing that entangled states are present even in this experiment, although it may not be immediately obvious. The reason being that during the cloning transformation entangled states are inherently created (Eq. (2.6)) as signal and ancillary photons overlap on beam splitter.

In the remainder of this Thesis, i.e., in Chapters 3 and 4, we addressed experimental preparation of Werner states and also their generalised form (in the later Chapter). We measured concurrence and nonlocal fraction (Chapter 3) on these states and demonstrated hierarchy of several classes of quantum correlations (Chapter 4). Specifically, the aim of the third Chapter is to show how quantification of multipartite entanglement can be made more accessible for practical quantum communications where alignment and calibration of laboratory devices cannot be guaranteed due to, e.g., an unstable conditions. To implement it, the measurements were carried out in reference-frame independent regime, i.e. by means of random sampling, instead of standard quantum tomography. Under these relaxed conditions we focused on quantification of entanglement (by means of concurrence) via detection of nonlocal fraction. Both connection between entanglement and nonlocality and quantification of entanglement are of particular interest. All our results are well in agreement with the theory.

Demonstration of hierarchy of separability, entanglement, steering (2- and 3-measurement scenario) and Bell nonlocality is discussed in the fourth Chapter. It turned out that this hierarchy reveals that generalised Werner states display fundamentally new features of quantum correlations. Particularly, unlike Werner state, their generalised form does not break Bell inequality (i.e. they are Bell local), yet they retain steerability in a 2-measurement scenario. Further, it was discovered, by means of both experiment and theoretical analysis, that some optimally prepared generalised Werner states exhibit increased robustness against white noise. To put it another way, quantum correlations of these optimal states are not disrupted upon addition of larger amount of white noise. Increased robustness also makes these states being an suitable tool for applications in secure quantum communications and cryptography.

The Author has firm believe that the research presented within this Thesis meaningfully contributed to better understanding of such a thrilling feature of quantum physics which entanglement certainly is. The Author is also particularly pleased that our results were published in journals with IF, namely Scientific Reports, Physical Review Applied and Physical Review A. Even though entanglement has found its stable role within the context of several fields of quantum physics its study has not been completed, yet. There are some open fundamental questions still waiting to be satisfactorily answered, such as: “What is the relation between entanglement and nonlocality?” or “How to reliably quantify and detect entanglement?”. This provides an opportunity for new discoveries. Nonetheless, it is a well-known truth that research brings actually more questions than answers which is in line with the quote above. This has a positive effect that there will always be something to research, as ongoing studies widen our view and insight into quantum mechanics and bring out new possibilities. Still, under no circumstances should this quote be viewed as a pessimistic view of the future of science. Quite the contrary: it means that the profession of physicist will always find employment.

❦

Author’s Publications

[A1] K. Jiráková, K. Bartkiewicz, A. Černoch, and K. Lemr, “Experimentally attacking quantum money schemes based on quantum retrieval games”, Scientific Reports **9** (2019).

[A2] K. Bartkiewicz, C. Gneiting, K. Jiráková, A. Černoch, K. Lemr, and F. Nori, “Experimental kernel-based quantum machine learning in finite feature space”, Scientific Reports **10**, 12356 (2020).

[A3] K. Jiráková, A. Barasiński, A. Černoch, K. Lemr, and J. Soubusta, “Measuring concurrence in qubit Werner states without an aligned reference frame”, Phys. Rev. Applied **16**, 054042 (2021).

[A4] K. Jiráková, A. Černoch, K. Lemr, K. Bartkiewicz, and A. Miranowicz, “Experimental hierarchy and optimal robustness of quantum correlations of two-qubit states with controllable white noise”, Phys. Rev. A **104**, 062436 (2021).

[A5] J. Jašek, K. Jiráková, K. Bartkiewicz, A. Černoch, T. Fürst, and K. Lemr, “Experimental hybrid quantum-classical reinforcement learning by boson sampling: how to train a quantum cloner”, Opt. Express **27**, 32454–32464 (2019).

[A6] J. Lange, L. Adamczyk, G. Avoni, E. Banas, A. Brandt, M. Bruschi, P. Buglewicz, E. Cavallaro, D. Caforio, G. Chiodini, L. Chytka, K. Cieśla, P. Davis, M. Dyndal, S. Grinstein, K. Janas, K. Jiráková, M. Kocian, K. Korcyl, I. L. Paz, D. Northacker, L. Nozka, M. Rijssenbeek, L. Seabra, R. Staszewski, P. Świerska, and T. Sykora, “Beam tests of an integrated prototype of the ATLAS Forward Proton detector”, Journal of Instrumentation **11**, P09005 (2016).

[A7] L. Nozka, L. Adamczyk, G. Avoni, A. Brandt, P. Buglewicz, E. Cavallaro, G. Chiodini, L. Chytka, K. Ciesla, P. Davis, M. Dyndal, S. Grinstein, P. Hamal, M. Hrabovsky, K. Janas, K. Jiráková, M. Kocian, T. Komarek, K. Korcyl, J. Lange, D. Mandat, V. Michalek, I. L. Paz, D. Northacker, M. Rijssenbeek, L. Seabra, P. Schovanek, R. Staszewski, P. Świerska, and T. Sykora, “Construction of the optical part of a time-of-flight detector prototype for the AFP detector”, Opt. Express **24**, 27951–27960 (2016).

[A8] L. Chytka, G. Avoni, A. Brandt, E. Cavallaro, P. M. Davis, F. Förster, M. Hrabovsky, Y. Huang, K. Jiráková, M. Kocian, T. Komarek, K. Korcyl, J. Lange, V. Michalek, L. Nozka, I. L. Paz, M. Rijssenbeek, P. Schovanek, T. Sykora, and V. Urbasek, “Timing resolution studies of the optical part of the AFP Time-of-flight detector”, Opt. Express **26**, 8028–8039 (2018).

[A9] V. Peřinová, A. Lukš, J. Křepelka, and K. Jiráková, “Stimulated and spontaneous down-conversion in layered media”, Optics Communications **441**, 96–105, ISSN: 0030-4018 (2019).

Bibliography

[1] M. Dušek, *Koncepční otázky kvantové teorie* (UPOL, Olomouc, 2002), ISBN: 8024404494.

[2] S. Weinberg, *Lectures on Quantum Mechanics*, 2nd edition (Cambridge University Press, 2015).

[3] P. Ehrenfest, "Welche Züge der Lichtquantenhypothese spielen in der Theorie der Wärmestrahlung eine wesentliche Rolle?", Annalen der Physik **341**, 91–118 (1911).

[4] P. Lenard, "Ueber die lichtelektrische Wirkung", Annalen der Physik **313**, 149–198 (1902).

[5] J. Thomson, "XXIV. On the structure of the atom: an investigation of the stability and periods of oscillation of a number of corpuscles arranged at equal intervals around the circumference of a circle; with application of the results to the theory of atomic structure", The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **7**, 237–265 (1904).

[6] E. Rutherford, "LXXIX. The scattering of α and β particles by matter and the structure of the atom", The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **21**, 669–688 (1911).

[7] N. Bohr, "XXXVII. On the constitution of atoms and molecules", The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **26**, 476–502 (1913).

[8] G. Kirchhoff, "I. On the relation between the radiating and absorbing powers of different bodies for light and heat", The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **20**, 1–21 (1860).

[9] M. Planck, "The theory of heat radiation", in, page 10, [Translated by Morton Masius from German original: "Vorlesungen über die Theorie der Wärmestrahlung" (1906).] (Philadelphia, P. Blakiston's Son & Co., 1914).

[10] J. Stefan, "ÜBER DIE BEZIEHUNG ZWISCHEN DER WÄRMESTRAHLUNG UND DER TEMPERATUR, [ON THE RELATION BETWEEN HEAT RADIATION AND TEMPERATURE]", in Sitzungsberichte der kaiserlichen akademie der wissenschaften. mathematisch-naturwissenschaftliche classe. abt. 2, mathematik, physik, chemie, mechanik, meteorologie und astronomie. 79 (1879), pages 391–428.

[11] L. Boltzmann, "Ableitung des Stefan'schen Gesetzes, betreffend die Abhängigkeit der Wärmestrahlung von der Temperatur aus der electromagnetischen Lichttheorie, [Derivation of Stefan's law, concerning the dependency of heat radiation on temperature, from the electromagnetic theory of light]", Annalen der Physik **258**, 291–294 (1884).

[12] J. W. S. Rayleigh, “LIII. Remarks upon the law of complete radiation”, The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **49**, 539–540 (1900).

[13] J. W. S. Rayleigh, “The Dynamical Theory of Gases and of Radiation”, Nature **72**, 54–55, ISSN: 1476-4687 (1905).

[14] J. H. Jeans, “A Comparison between Two Theories of Radiation”, Nature **72**, 293–294, ISSN: 1476-4687 (1905).

[15] J. H. Jeans and J. Larmor, “On the laws of radiation”, Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character **76**, 545–552 (1905).

[16] M. Planck, “Faksimile aus den Verhandlungen der Deutschen Physikalischen Gesellschaft 2 (1900) S. 237: Zur Theorie des Gesetzes der Energieverteilung im Normalspectrum”, Physikalische Blätter **4**, 146–151 (1948).

[17] G. N. Lewis, “The Conservation of Photons”, Nature **118**, 874–875, ISSN: 1476-4687 (1926).

[18] A. H. Compton, “A Quantum Theory of the Scattering of X-rays by Light Elements”, Phys. Rev. **21**, 483–502 (1923).

[19] De Broglie, Louis, “On the Theory of Quanta”, Ann. Phys. **10**, [Translated by A.F. Kracklauer from French original: "Recherches sur la théorie des Quanta" (1925).], 22–128 (1925).

[20] E. Schrödinger, “An Undulatory Theory of the Mechanics of Atoms and Molecules”, Phys. Rev. **28**, 1049–1070 (1926).

[21] M. Born, “Zur Quantenmechanik der Stoßvorgänge”, Zeitschrift für Physik **37**, 863–867, ISSN: 0044-3328 (1926).

[22] J. Griffiths, D., *Introduction to Quantum Mechanics* (Pearson Education, Inc., 2005), ISBN: 0131911759.

[23] J. J. Napolitano, J.; Sakurai, *Modern quantum mechanics*, 2nd (Addison-Wesley, San Francisco, CA, 2011), ISBN: 0805382917.

[24] P. A. M. Dirac, *The Principles Of Quantum Mechanics* (Oxford at the Clarenden Press, 1930).

[25] J. Von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin [u.a.], 1932).

[26] R. Shankar, “Chapter 4: The Postulates–a General Discussion”, in *Principles of Quantum Mechanics* (Springer Nature, New York, NY, 1994), pages 115–143.

[27] R. E. Christoffersen, “Postulates of Quantum Mechanics and Initial Considerations”, in *Basic Principles and Techniques of Molecular Quantum Mechanics* (Springer Nature, New York, NY, 1989).

[28] B. Zwiebach, *Key Features of Quantum Mechanics. Quantum Physics I. Massachusetts Institute of Technology: MIT OpenCourseWare*, `https://ocw.mit.edu/courses/physics/8-04-quantum-physics-i-spring-2013/index.htm`, [Accessed: 2021-05-15], 2016.

[29] R. L. Jaffe, *Supplementary notes on Dirac notation, quantum states, Massachusetts Institute of Technology: MIT OpenCourseWare*, `http://web.mit.edu/8.05/handouts/jaffe1.pdf`, [Accessed: 2021-05-15], 2007.

[30] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010), ISBN: 978-110700-2173.

[31] E. Schrödinger, "The Present Status of Quantum Mechanics", Naturwissenschaften **23** (1935).

[32] M. Arndt, O. Nairz, J. Vos-Andreae, C. Keller, G. van der Zouw, and A. Zeilinger, "Wave–particle duality of C60 molecules", Nature **401**, 680–682, ISSN: 1476-4687 (1999).

[33] P. Sekatski, N. Sangouard, M. Stobińska, F. Bussières, M. Afzelius, and N. Gisin, "Proposal for exploring macroscopic entanglement with a single photon and coherent states", Phys. Rev. A **86**, 060301 (2012).

[34] R. Riedinger, A. Wallucks, I. Marinković, C. Löschnauer, M. Aspelmeyer, S. Hong, and S. Gröblacher, "Remote quantum entanglement between two micromechanical oscillators", Nature **556**, 473–477, ISSN: 1476-4687 (2018).

[35] C. F. Ockeloen-Korppi, E. Damskägg, J.-M. Pirkkalainen, M. Asjad, A. A. Clerk, F. Massel, M. J. Woolley, and M. A. Sillanpää, "Stabilized entanglement of massive mechanical oscillators", Nature **556**, 478–482, ISSN: 1476-4687 (2018).

[36] G. Altmann, *Web page Pixabay*, `https://pixabay.com/photos/physics-schr%c3%b6dinger-s-cat-3864569/`, [Accessed: 2021-08-03], 2018.

[37] M. L. Cohen, "Essay: Fifty Years of Condensed Matter Physics", Phys. Rev. Lett. **101**, 250001 (2008).

[38] S. Wiesner, "Conjugate Coding", SIGACT News **15**, [Original manuscript written circa 1970.], 78–88, ISSN: 0163-5700 (1983).

[39] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, "Experimental quantum forgery of quantum optical money", npj Quantum Information **3**, 7 (2017).

[40] S. Weinberg, W. S, and T. de campos, *The Quantum Theory of Fields*, Quantum Theory of Fields, Vol. 2: Modern Applications sv. 1 (Cambridge University Press, 1995), ISBN: 9780521550017.

[41] P. W. Atkins, *Atkins' Physical Chemistry*, 7th ed. (Oxford University Press, Oxford, 2002), ISBN: 0-19-879285-9.

[42] A. Barasiński, A. Černoch, and K. Lemr, "Demonstration of Controlled Quantum Teleportation for Discrete Variables on Linear Optical Devices", Phys. Rev. Lett. **122**, 170501 (2019).

[43] N. D. Mermin and D. M. Lee, "Superfluid helium-3", Scientific American **235**, 56–60, 62, 64, 67–68, 70–71, ISSN: 00368733, 19467087 (1976).

[44] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*, edited by E. Grumbling and M. Horowitz (The National Academies Press, Washington, DC, 2019), ISBN: 978-0-309-47969-1.

[45] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement", Rev. Mod. Phys. **81**, 865–942 (2009).

[46] *IBM Quantum.* `https://quantum-computing.ibm.com/`, [Cited: 5.7.2021], 2021.

[47] *Web of Qiskit.* `https://qiskit.org/overview/`, [Cited: 6.7.2021], 2021.

[48] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in Proceedings 35th annual symposium on foundations of computer science (Nov. 1994), pages 124–134.

[49] M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information: 10th Anniversary Edition", in , 10th Anniversary Edition (Cambridge University Press, 2010), pages 6–7, ISBN: 9781107002173.

[50] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, "Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits", Phys. Rev. Lett. **99**, 250504 (2007).

[51] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search", in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96 (1996), pages 212–219, ISBN: 0897917855.

[52] M. Schuld, I. Sinayskiy, and F. Petruccione, "An introduction to quantum machine learning", Contemporary Physics **56**, 172–185 (2015).

[53] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning", Nature **549**, 195–202, ISSN: 1476-4687 (2017).

[54] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Rev. Mod. Phys. **74**, 145–195 (2002).

[55] *MagiQ Demos Quantum Cryptography. In: Web of LightReading.* `https://www.lightreading.com/ethernet-ip/magiq-demos-quantum-cryptography/d/d-id/588776`, [Cited: 6.7.2021], 2003.

[56] M. E. Peck, "Geneva Vote Will Use Quantum Cryptography", IEEE Spectrum, [Cited: 6.7.2021] (2007).

[57] *Toshiba to launch quantum cryptography services this year. In: Web of Nikkei Asia.* `https://asia.nikkei.com/Business/Technology/Toshiba-to-launch-quantum-cryptography-services-this-year`, [Cited: 6.7.2021], 2020.

[58] C. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", in (Dec. 1984), pages 175–179.

[59] D. Bruß, "Optimal Eavesdropping in Quantum Cryptography with Six States", Phys. Rev. Lett. **81**, 3018–3021 (1998).

[60] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. **67**, 661–663 (1991).

[61] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum Secure Direct Communication with Quantum Memory", Phys. Rev. Lett. **118**, 220501 (2017).

[62] L. Ma, X. Tang, and O. Slattery, "Optical quantum memory and its applications in quantum communication systems", Journal of Research (NIST JRES) (2020) `https://doi.org/10.6028/jres.125.002`.

[63] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson, "Realization of a multinode quantum network of remote solid-state qubits", Science **372**, 259–264, ISSN: 0036-8075 (2021).

[64] "Kvantové počítače, sítě, satelity a qubity: Čína odhalila plány na příštích pět let", Computer World (2021).

[65] N. Savage, "Google's Quantum Computer Achieves Chemistry Milestone", Scientific American, https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/, [cited: 5.6.2021] (2020).

[66] K. J. Satzinger et al., "Realizing topologically ordered states on a quantum processor", arXiv e-prints, 2104.01180 (2021).

[67] F. Arute et al., "Quantum supremacy using a programmable superconducting processor", Nature **574**, 505–510, ISSN: 1476-4687 (2019).

[68] C. Neill et al., "A blueprint for demonstrating quantum supremacy with superconducting qubits", Science **360**, 195–199, ISSN: 0036-8075 (2018).

[69] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "Quantum computational advantage using photons", Science **370**, 1460–1463, ISSN: 0036-8075 (2020).

[70] J. Gambetta, "IBM's Roadmap For Scaling Quantum Technology", `https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/`, [Cited: 5.7.2021] (2020).

[71] A. Cho, "IBM promises 1000-qubit quantum computer—a milestone—by 2023", Science (2020).

[72] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications", Phys. Rev. Lett. **115**, 040502 (2015).

[73] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km", Nature Physics **3**, 481–486 (2007).

[74] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1,120 kilometres", Nature **582**, 501–505, ISSN: 1476-4687 (2020).

[75] Y.-A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres", Nature **589**, 214–219, ISSN: 1476-4687 (2021).

[76] *Quantum Overview, In: Web page of ESA.*, `https://www.esa.int/content/view/full/455489`, [cited: 5.7.2021], 2021.

[77] *Future Satellites, In: Web page of EUTELSAT.*, `https://www.eutelsat.com/home/satellites/future-launches.html`, [cited: 5.7.2021], 2021.

[78] M. Bozzio, A. Orieux, L. Trigo Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money", npj Quantum Information **4** (2018).

[79] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete", Phys. Rev. **47**, 777–780 (1935).

[80] E. Schrödinger, "The Present Status of Quantum Mechanics", Naturwissenschaften **23**, 807–812 (1935).

[81] E. Polino, M. Valeri, N. Spagnolo, and F. Sciarrino, "Photonic quantum metrology", AVS Quantum Science **2**, 024703 (2020).

[82] Mandel, Leonard and Emil Wolf, "Chapter 22: Some quantum effects in nonlinear optics", in *Optical coherence and quantum optics* (Cambridge University Press, New York, NY, 1995), pages 1069–1108, ISBN: 0-521-41711-2.

[83] D. N. Klyshko, "Scattering of light in a medium with nonlinear polarizability", Zh. Eksp. Teor. Fiz. **55**, Translated into english in: *Sov. Phys.* JETP **28**, 522 (1969). (1968).

[84] A. Einstein, "The foundation of the general theory of relativity", Annalen der Physik **49**, Translated by: Robert W. Lawson in 1920., 31 (1916).

[85] R. Holmes, "Local realism is dead, long live local realism?", Physics World **30**, 21–25 (2017).

[86] J. S. Bell, "On the Einstein Podolsky Rosen paradox", Physics Physique Fizika **1**, 195–200 (1964).

[87] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories", Phys. Rev. Lett. **23**, 880–884 (1969).

[88] A. Aspect, P. Grangier, and G. Roger, "Experimental Tests of Realistic Local Theories via Bell's Theorem", Phys. Rev. Lett. **47**, 460–463 (1981).

[89] A. Aspect, P. Grangier, and G. Roger, "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities", Phys. Rev. Lett. **49**, 91–94 (1982).

[90] P. R. Tapster, J. G. Rarity, and P. C. M. Owens, "Violation of Bell's Inequality over 4 km of Optical Fiber", Phys. Rev. Lett. **73**, 1923–1926 (1994).

[91] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, "Violation of Bell's Inequality under Strict Einstein Locality Conditions", Phys. Rev. Lett. **81**, 5039–5043 (1998).

[92] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, "Experimental violation of a Bell's inequality with efficient detection", Nature **409**, 791–794, ISSN: 1476-4687 (2001).

[93] P. Shadbolt, T. Vértesi, Y.-C. Liang, C. Branciard, N. Brunner, and J. L. O'Brien, "Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices", Scientific Reports **2**, 470, ISSN: 2045-2322 (2012).

[94] H. S. Poh, S. K. Joshi, A. Cerè, A. Cabello, and C. Kurtsiefer, "Approaching Tsirelson's Bound in a Photon Pair Experiment", Phys. Rev. Lett. **115**, 180408 (2015).

[95] A. Barasiński, A. Černoch, K. Lemr, and J. Soubusta, "Experimental verification of time-order-dependent correlations in three-qubit Greenberger-Horne-Zeilinger-class states", Phys. Rev. A **99**, 042123 (2019).

[96] A. Barasiński, A. Černoch, K. Lemr, and J. Soubusta, "Genuine tripartite nonlocality for random measurements in Greenberger-Horne-Zeilinger-class states and its experimental test", Phys. Rev. A **101**, 052109 (2020).

[97] G. Svetlichny, "Distinguishing three-body from two-body nonseparability by a Bell-type inequality", Phys. Rev. D **35**, 3066–3069 (1987).

[98] R. F. Werner, “Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model”, Phys. Rev. A **40**, 4277–4281 (1989).

[99] J. Perina, *Quantum Statistics of Linear and Nonlinear Optical Phenomena* (Springer Netherlands, 2012), ISBN: 9789400962484.

[100] P. Meystre and M. Sargent, *Elements of Quantum Optics* (Springer Berlin Heidelberg, 1998), ISBN: 9783540642206.

[101] Trávníček, Vojtěch, “Design and construction of devices for quantum information processing”, Disertation theses (Palacky University in Olomouc, Faculty of Science, 2021).

[102] C. K. Hong, Z. Y. Ou, and L. Mandel, “Measurement of subpicosecond time intervals between two photons by interference”, Phys. Rev. Lett. **59**, 2044–2046 (1987).

[103] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, “Linear Optics Controlled-Phase Gate Made Simple”, Phys. Rev. Lett. **95**, 210505 (2005).

[104] K. Lemr and A. Černoch, “Optimal success probability of a tunable linear-optical controlled-phase gate”, Phys. Rev. A **86**, 034304 (2012).

[105] K. Lemr, K. Bartkiewicz, and A. Černoch, “Scheme for a linear-optical controlled-phase gate with programmable phase shift”, Journal of Optics **17**, 125202 (2015).

[106] A. Černoch, J. Soubusta, L. Bartůšková, M. Dušek, and J. Fiurášek, “Experimental implementation of partial symmetrization and anti-symmetrization of two-qubit states”, New Journal of Physics **11**, 023005 (2009).

[107] A. Černoch, J. Soubusta, L. Čelechovská, M. Dušek, and J. Fiurášek, “Experimental demonstration of optimal universal asymmetric quantum cloning of polarization states of single photons by partial symmetrization”, Phys. Rev. A **80**, 062306 (2009).

[108] J. Fiurášek, “Optical implementations of the optimal phase-covariant quantum cloning machine”, Physical Review A **67**, 052314 (2003).

[109] J. Soubusta, L. Bartůšková, A. Černoch, J. Fiurášek, and M. Dušek, “Several experimental realizations of symmetric phase-covariant quantum cloners of single-photon qubits”, Phys. Rev. A **76**, 042318 (2007).

[110] J. Soubusta, L. Bartůšková, A. Černoch, M. Dušek, and J. Fiurášek, “Experimental asymmetric phase-covariant quantum cloning of polarization qubits”, Physical Review A **78** (2008) `10.1103/physreva.78.052323`.

[111] Lemr, Karel, “Experimental quantum information processing with photon pairs”, [cit. 2021-07-17], Disertation theses (Palacky University in Olomouc, Faculty of Science, 2012).

[112] A. MacLeod, H., *Thin-Film Optical Filters*, Series in Optics and Optoelectronics (CRC Press, 2001), ISBN: 9781420033236.

[113] B. Saleh and M. Teich, “Chapter 6: Polarization Optics”, in *Fundamentals of Photonics*, Wiley Series in Pure and Applied Optics (Wiley, 2007), pages 197–242, ISBN: 9780471358329.

[114] D. F. Vanderwerf, *Applied prismatic and reflective optics* (SPIE Press, Bellingham, Washington, 2010), page 310, ISBN: 9780819483324.

[115] G. Agarwal, *Quantum Optics*, Quantum Optics (Cambridge University Press, 2013), ISBN: 9781107006409.

[116] G. Corrielli, A. Crespi, R. Geremia, R. Ramponi, L. Sansoni, A. Santinelli, P. Mataloni, F. Sciarrino, and R. Osellame, "Rotated waveplates in integrated waveguide optics", Nature Communications **5**, 4249, ISSN: 2041-1723 (2014).

[117] Langford, N. K., "Encoding, manipulating and measuring quantum information in optics", [cit. 2021-10-06], Disertation theses (University of Queensland, School of Physical Science, 2007).

[118] C. Gerry, P. Knight, and P. Knight, "Chapter 9: Optical Test of Quantum Mechanics", in *Introductory Quantum Optics* (Cambridge University Press, 2005), pages 213–237, ISBN: 9780521527354.

[119] Soubusta, Jan and Černoch, Antonín, "Chapter 5: Fresnelova rovnice", in *Optické vlastnosti pevných látek* (Univerzita Palackého v Olomouci, Olomouc, 2014), pages 59–73, ISBN: 978-80-244-4111-5.

[120] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New High-Intensity Source of Polarization-Entangled Photon Pairs", Phys. Rev. Lett. **75**, 4337 (1995).

[121] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultra-bright source of polarization-entangled photons", Phys. Rev. A **60**, R773–R776 (1999).

[122] A. Migdall, S. Polyakov, J. Fan, and J. Bienfang, *Single-Photon Generation and Detection: Physics and Applications*, Experimental Methods in the Physical Sciences (Elsevier Science, 2013), ISBN: 9780123876959.

[123] D. S. Tasca, R. M. Gomes, F. Toscano, P. H. Souto Ribeiro, and S. P. Walborn, "Continuous-variable quantum computation with spatial degrees of freedom of photons", Phys. Rev. A **83**, 052325 (2011).

[124] O. Pfister, "Continuous-variable quantum computing in the quantum optical frequency comb", Journal of Physics B: Atomic, Molecular and Optical Physics **53**, 012001 (2019).

[125] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons", Nature **412**, 313–316, ISSN: 1476-4687 (2001).

[126] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits", New Journal of Physics **8**, 75–75 (2006).

[127] A. Nicolas, L. Veissier, E. Giacobino, D. Maxein, and J. Laurat, "Quantum state tomography of orbital angular momentum photonic qubits via a projection-based technique", New Journal of Physics **17**, 033037 (2015).

[128] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges", Advanced Quantum Technologies **2**, 1900038 (2019).

[129] B. Julsgaard and K. Mølmer, "Fidelity of fock-state-encoded qubits subjected to continuous-variable gaussian processes", Phys. Rev. A **89**, 012333 (2014).

[130] Y. Y. Gao, B. J. Lester, K. S. Chou, L. Frunzio, M. H. Devoret, L. Jiang, S. M. Girvin, and R. J. Schoelkopf, "Entanglement of bosonic modes through

an engineered exchange interaction", Nature **566**, 509–512, ISSN: 1476-4687 (2019).

[131] Y. Pilnyak, P. Zilber, L. Cohen, and H. S. Eisenberg, "Quantum tomography of photon states encoded in polarization and picosecond time bins", Phys. Rev. A **100**, 043826 (2019).

[132] Z. Hradil, J. Řeháček, J. Fiurášek, and M. Ježek, "Maximum-Likelihood Methodsin Quantum Mechanics.", in *(eds) Quantum State Estimation. Lecture Notes in Physics, vol 649*, edited by P. M. and Ř. J. (Springer, Berlin, Heidelberg, Oxford, 2004) Chap. 3, pages 266–290.

[133] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", Nature **299**, 802–803 (1982).

[134] D. Dieks, "Communication by EPR devices", Physics Letters A **92**, 271–272, ISSN: 0375-9601 (1982).

[135] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor, "Quantum money from knots", arXiv e-prints, arXiv:1004.5127 (2010).

[136] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor, "Breaking and making quantum money: toward a new quantum cryptographic protocol", arXiv e-prints, arXiv:0912.3825 (2009).

[137] M. Mosca and D. Stebila, "Quantum Coins", in Error-Correcting Codes, Finite Geometries and Cryptography. Contemporary Mathematics, Vol. 523 (2010), pages 35–47.

[138] R. Amiri and J. M. Arrazola, "Quantum money with nearly optimal error tolerance", Phys. Rev. A **95**, 062334 (2017).

[139] J.-Y. Guan, J. M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J.-W. Pan, "Experimental preparation and verification of quantum money", Phys. Rev. A **97**, 032338 (2018).

[140] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, "Exponential Separation of Quantum and Classical One-way Communication Complexity", in Proceedings of the thirty-sixth annual acm symposium on theory of computing, STOC '04 (2004), pages 128–137, ISBN: 1-58113-852-0.

[141] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, "Experimental Eavesdropping Based on Optimal Quantum Cloning", Phys. Rev. Lett. **110**, 173601 (2013).

[142] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Rev. Mod. Phys. **74**, 145–195 (2002).

[143] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography", Phys. Rev. A **59**, 4238–4248 (1999).

[144] A. Molina, T. Vidick, and J. Watrous, "Optimal Counterfeiting Attacks and Generalizations for Wiesner's Quantum Money", in Theory of quantum computation, communication, and cryptography, edited by K. Iwama, Y. Kawano, and M. Murao (2013), pages 45–64, ISBN: 978-3-642-35656-8.

[145] A. Brodutch, D. Nagaj, O. Sattath, and D. Unruh, "An adaptive attack on Wiesner's quantum money", arXiv e-prints, arXiv:1404.1507 (2014).

[146] D. Gavinsky, "Quantum Money with Classical Verification", in 2012 ieee 27th conference on computational complexity (June 2012), pages 42–52.

[147] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, "Unforgeable noise-tolerant quantum tokens", PNAS **109**, 16079–16082 (2012).

[148] M. Georgiou and I. Kerenidis, "New constructions for Quantum Money", in Leibniz international proceedings in informatics, schloss dagstuhl leibniz-zentrum für informatik (2015), pages 1–19.

[149] J. Wolters, G. Buser, A. Horsley, L. Béguin, A. Jöckel, J.-P. Jahn, R. J. Warburton, and P. Treutlein, "Simple Atomic Quantum Memory Suitable for Semiconductor Quantum Dot Single Photons", Phys. Rev. Lett. **119**, 060502 (2017).

[150] W.-B. Wang, C. Zu, L. He, W.-G. Zhang, and L.-M. Duan, "Memory-built-in quantum cloning in a hybrid solid-state spin register", Scientific Reports, 12203 (2015).

[151] S. Aaronson and P. Christiano, "Quantum Money from Hidden Subspaces", Theory of Computing **9**, 349–401 (2013).

[152] A. Nassiri, *Web page of German Wikipedia: Enigma (Maschine)*, `https://commons.wikimedia.org/w/index.php?curid=47910919`, Museo nazionale della scienza e della tecnologia Leonardo da Vinci, CC BY-SA 4.0, [Accessed: 2021-08-12], 2021.

[153] C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner, "Quantum Cryptography, or Unforgeable Subway Tokens", in Advances in cryptology: proceedings of crypto '82 (1982), pages 267–275.

[154] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol", Phys. Rev. Lett. **84**, 4733–4736 (2000).

[155] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations", Phys. Rev. Lett. **92**, 057901 (2004).

[156] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized Privacy Amplification", IEEE Trans. Inf. Theory **41**, 1915 (1995).

[157] D. Bruß, M. Cinchetti, G. Mauro D'Ariano, and C. Macchiavello, "Phase-covariant quantum cloning", Phys. Rev. A **62**, 012302 (2000).

[158] K. Bartkiewicz, A. Černoch, K. Lemr, J. Soubusta, and M. Stobińska, "Efficient amplification of photonic qubits by optimal quantum cloning", Phys. Rev. A **89**, 062322 (2014).

[159] Chuan-Wei Zhang and Chuan-Feng Li and Guang-Can Guo, "Quantum clone and states estimation for n-state system", Physics Letters A **271**, 31–34, ISSN: 0375-9601 (2000).

[160] A. Chefles and S. M. Barnett, "Strategies and networks for state-dependent quantum cloning", Phys. Rev. A **60**, 136–144 (1999).

[161] R. Rivest, *The MD5 Message-digest Algorithm* (MIT Laboratory for Computer Science, 1992).

[162] M. Bellare, R. Canetti, and H. Krawczyk, *Keying hash functions for message authentication* (Springer-Verlag, 1996), pages 1–15.

[163] J. M. Renes, “Spherical-code key-distribution protocols for qubits”, Phys. Rev. A **70**, 052314 (2004).

[164] M. Schiavon, G. Vallone, and P. Villoresi, “Experimental realization of equiangular three-state quantum key distribution”, Scientific Reports **6** (2016) `10.1038/srep30089`.

[165] G. M. D’Ariano and C. Macchiavello, “Optimal phase-covariant cloning for qubits and qutrits”, Phys. Rev. A **67**, 042306 (2003).

[166] K. Lemr, K. Bartkiewicz, A. Černoch, J. Soubusta, and A. Miranowicz, “Experimental linear-optical implementation of a multifunctional optimal qubit cloner”, Phys. Rev. A **85**, 050307 (2012).

[167] D. Deutsch and R. Jozsa, “Rapid solution of problems by quantum computation”, in Proc. R. Soc. Lond. A, Vol. 439 (1992).

[168] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and J.-W. Pan, “Quantum teleportation with independent sources and prior entanglement distribution over a network”, Nature Photon. **10**, 671 (2016).

[169] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, “Quantum teleportation across a metropolitan fibre network”, Nature Photon. **10**, 676 (2016).

[170] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, “Quantum teleportation and entanglement distribution over 100-kilometre free-space channels”, Nature **488**, 185 (2012).

[171] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, “Quantum teleportation over 143 kilometres using active feed-forward”, Nature **489**, 269 (2012).

[172] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, “Experimental verification of the feasibility of a quantum channel between space and Earth”, New Journal of Physics **10**, 033038 (2008).

[173] J.-G. Ren et al., “Ground-to-satellite quantum teleportation”, Nature **549**, 70 (2017).

[174] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. F. Matthews, M. G. Thompson, and J. L. O’Brien, “Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit”, Nature Photon **6**, 4549 (2012).

[175] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger, “Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link”, Opt. Express **14**, 10050–10059 (2006).

[176] X. Han, H.-L. Yong, P. Xu, K.-X. Yang, S.-L. Li, W.-Y. Wang, H.-J. Xue, F.-Z. Li, J.-G. Ren, C.-Z. Peng, and J.-W. Pan, “Polarization design for ground-to-satellite quantum entanglement distribution”, Opt. Express **28**, 369–378 (2020).

[177] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, "Complete experimental toolbox for alignment-free quantum communication", Nature Communications **3**, 961, ISSN: 2041-1723 (2012).

[178] Y.-P. Li, W. Chen, F.-X. Wang, Z.-Q. Yin, L. Zhang, H. Liu, S. Wang, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Experimental realization of a reference-frame-independent decoy BB84 quantum key distribution based on Sagnac interferometer", Opt. Lett. **44**, 4523–4526 (2019).

[179] R. Tannous, Z. Ye, J. Jin, K. B. Kuntz, N. Lütkenhaus, and T. Jennewein, "Demonstration of a 6 state-4 state reference frame independent channel for quantum key distribution", Applied Physics Letters **115**, 211103 (2019).

[180] C. E. R. Souza, C. V. S. Borges, A. Z. Khoury, J. A. O. Huguenin, L. Aolita, and S. P. Walborn, "Quantum key distribution without a shared reference frame", Phys. Rev. A **77**, 032345 (2008).

[181] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution", Phys. Rev. A **82**, 012304 (2010).

[182] T.-Y. Chen, J. Zhang, J.-C. Boileau, X.-M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J.-W. Pan, "Experimental Quantum Communication without a Shared Reference Frame", Phys. Rev. Lett. **96**, 150504 (2006).

[183] F. Rezazadeh, A. Mani, and V. Karimipour, "Quantum key distribution with no shared reference frame", Quantum Information Processing **19** (2019) `10.1007/s11128-019-2508-y`.

[184] H. Liu, J. Wang, H. Ma, and S. Sun, "Reference-Frame-Independent Quantum Key Distribution Using Fewer States", Phys. Rev. Applied **12**, 034039 (2019).

[185] P.-L. Guo, T. Li, Q. Ai, and F.-G. Deng, "Self-error-rejecting quantum state transmission of entangled photons for faithful quantum communication without calibrated reference frames", EPL (Europhysics Letters) **127**, 60001 (2019).

[186] J. Yoon, T. Pramanik, B.-K. Park, Y.-W. Cho, S.-Y. Lee, S. Kim, S.-W. Han, S. Moon, and Y.-S. Kim, "Experimental comparison of various quantum key distribution protocols under reference frame rotation and fluctuation", Optics Communications **441**, 64–68, ISSN: 0030-4018 (2019).

[187] Y. Xue, L. Shi, J. Wei, L. Yu, H. Yu, J. Tang, and Z. Zhang, "Reference-Frame-Independent Quantum Key Distribution in Uplink and Downlink Free-Space Channel", International Journal of Theoretical Physics **59**, 3299–3309, ISSN: 1572-9575 (2020).

[188] A. Barasiński, I. I. Arkhipov, and J. Svozilík, "Localizable entanglement as a necessary resource of controlled quantum teleportation", Scientific Reports **8**, 15209 (2018).

[189] Z. Wang, C. Zhang, Y.-F. Huang, B.-H. Liu, C.-F. Li, and G.-C. Guo, "Experimental verification of genuine multipartite entanglement without shared reference frames", Science Bulletin **61**, 714–719, ISSN: 2095-9273 (2016).

[190] T. Lawson, A. Pappa, B. Bourdoncle, I. Kerenidis, D. Markham, and E. Diamanti, "Reliable experimental quantification of bipartite entanglement without reference frames", Phys. Rev. A **90**, 042336 (2014).

[191] S.-X. Yang, G. N. Tabia, P.-S. Lin, and Y.-C. Liang, "Device-independent certification of multipartite entanglement using measurements performed in randomly chosen triads", Phys. Rev. A **102**, 022419 (2020).

[192] J. J. Wallman and S. D. Bartlett, "Observers can always generate nonlocal correlations without aligning measurements by covering all their bases", Phys. Rev. A **85**, 024101 (2012).

[193] Y.-C. Liang, N. Harrigan, S. D. Bartlett, and T. Rudolph, "Nonclassical Correlations from Randomly Chosen Local Measurements", Phys. Rev. Lett. **104**, 050401 (2010).

[194] A. Barasiński, A. Černoch, K. Lemr, and J. Soubusta, "Genuine tripartite nonlocality for random measurements in Greenberger-Horne-Zeilinger-class states and its experimental test", Phys. Rev. A **101**, 052109 (2020).

[195] M. C. Tran, B. Dakić, F. Arnault, W. Laskowski, and T. Paterek, "Quantum entanglement from random measurements", Phys. Rev. A **92**, 050301 (2015).

[196] L. Knips, J. Dziewior, W. Kłobus, T. P. W. Laskowski, P. J. Shadbolt, H. Weinfurter, and J. D. A. Meinecke, "Multipartite entanglement analysis from random correlations", npj Quantum Inf **6**, 51 (2020).

[197] W. Laskowski, C. Schwemmer, D. Richart, L. Knips, T. Paterek, and H. Weinfurter, "Optimized state-independent entanglement detection based on a geometrical threshold criterion", Phys. Rev. A **88**, 022327 (2013).

[198] K. Bartkiewicz, G. Chimczak, and K. Lemr, "Direct method for measuring and witnessing quantum entanglement of arbitrary two-qubit states through Hong-Ou-Mandel interference", Phys. Rev. A **95**, 022331 (2017).

[199] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction", Phys. Rev. A **54**, 3824 (1996).

[200] M. Horodecki and P. Horodecki, "Reduction criterion of separability and limits for a class of distillation protocols", Phys. Rev. A **59**, 4206 (1999).

[201] B. M. Terhal and K. G. H. Vollbrecht, "Entanglement of Formation for Isotropic States", Phys. Rev. Lett. **85**, 2625 (2000).

[202] F. Nosrati, A. Castellini, G. Compagno, and R. L. Franco, "Robust entanglement preparation against noise by controlling spatial indistinguishability", npj Quantum Information **6**, 39 (2020).

[203] W. K. Wootters, "Entanglement of Formation of an Arbitrary State of Two Qubits", Phys. Rev. Lett. **80**, 2245–2248 (1998).

[204] A. Uhlmann, "Entropy and Optimal Decompositions of States Relative to a Maximal Commutative Subalgebra", Open Syst. Inf. Dyn. **5**, 209 (1998).

[205] D. T. Pope and G. J. Milburn, "Multipartite entanglement and quantum state exchange", Phys. Rev. A **67**, 052107 (2003).

[206] P. Love, A. van den Brink, A. Smirnov, M. Amin, M. Grajcar, E. Ilichev, A. Izmalkov, and A. Zagoskin, "A Characterization of Global Entanglement", Quant. Inf. Proc. **6**, 187 (2007).

[207] Z.-H. Ma, Z.-H. Chen, J.-L. Chen, C. Spengler, A. Gabriel, and M. Huber, "Measure of genuine multipartite entanglement with computable lower bounds", Phys. Rev. A **83**, 062325 (2011).

[208] Z.-H. Chen, Z.-H. Ma, J.-L. Chen, and S. Severini, "Improved lower bounds on genuine-multipartite-entanglement concurrence", Phys. Rev. A **85**, 062320 (2012).

[209] T. Yu and J. H. Eberly, "Evolution from Entanglement to Decoherence of Bipartite Mixed "X" States", Quantum Inf. Comput. **7**, 459 (2007).

[210] S. M. Hashemi Rafsanjani, M. Huber, C. J. Broadbent, and J. H. Eberly, "Genuinely multipartite concurrence of n-qubit x matrices", Phys. Rev. A **86**, 062303 (2012).

[211] I. Pitowsky and K. Svozil, "Optimal tests of quantum nonlocality", Phys. Rev. A **64**, 014102 (2001).

[212] C. Śliwa, "Symmetries of the Bell correlation inequalities", Phys. Lett. A **317**, 165 (2003).

[213] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio, "Definitions of multipartite nonlocality", Phys. Rev. A **88**, 014102 (2013).

[214] V. Scarani, "The device-independent outlook on quantum physics", Acta Phys. Slovaca **62**, 347 (2012).

[215] F. Verstraete and M. M. Wolf, "Entanglement versus Bell Violations and Their Behavior under Local Filtering Operations", Phys. Rev. Lett. **89**, 170401 (2002).

[216] S. Ghose, N. Sinclair, S. Debnath, P. Rungta, and R. Stock, "Tripartite Entanglement versus Tripartite Nonlocality in Three-Qubit Greenberger-Horne-Zeilinger-Class States", Phys. Rev. Lett. **102**, 250404 (2009).

[217] A. Barasiński, "Restriction on the local realism violation in three-qubit states and its relation with tripartite entanglement", Scientific Reports **8**, 12305 (2018).

[218] H.-X. Lu, J.-Q. Zhao, X.-Q. Wang, and L.-Z. Cao, "Experimental demonstration of tripartite entanglement versus tripartite nonlocality in three-qubit Greenberger-Horne-Zeilinger–class states", Phys. Rev. A **84**, 012111 (2011).

[219] J. J. Wallman, Y.-C. Liang, and S. D. Bartlett, "Generating nonclassical correlations without fully aligning measurements", Phys. Rev. A **83**, 022110 (2011).

[220] V. Lipinska, F. Curchod, A. Máttar, and A. Acín, "Towards an equivalence between maximal entanglement and maximal quantum nonlocality", New J. Phys. **20**, 063043 (2018).

[221] A. Barasiński, A. Černoch, W. Laskowski, K. Lemr, T. Vértesi, and J. Soubusta, "Experimentally friendly approach towards nonlocal correlations in multisetting N-partite Bell scenarios", Quantum **5**, 430, ISSN: 2521-327X (2021).

[222] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, "Measurement of qubits", Phys. Rev. A **64**, 052312 (2001).

[223] J. P. Torres, K. Banaszek, and I. Walmsley, "Engineering Nonlinear Optic Sources of Photonic Entanglement", Progress in Optics **56**, 227 (2011).

[224] F. Bussières, C. Clausen, A. Tiranov, B. Korzh, V. B. Verma, S. W. Nam, F. Marsili, A. Ferrier, P. Goldner, H. Herrmann, C. Silberhorn, W. Sohler, M. Afzelius, and N. Gisin, "Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory", Nature Photon. **8**, 775 (2014).

[225] L. Masanes, "Tight Bell inequality for d-outcome measurements correlations", Quantum Inf. Comput. **3**, 345 (2003).

[226] D. Collins and N. Gisin, “A relevant two qubit Bell inequality inequivalent to the CHSH inequality”, J. Phys. A **37**, 1775 (2004).

[227] C. Eltschka and J. Siewert, “Entanglement of Three-Qubit Greenberger-Horne-Zeilinger–Symmetric States”, Phys. Rev. Lett. **108**, 020502 (2012).

[228] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory* (Springer-Verlag Berlin Heidelberg, 1983).

[229] J. Batle and M. Casas, “Nonlocality and entanglement in qubit systems”, J. Phys. A: Math. Theor. **44**, 445304 (2011).

[230] K. H. Kagalwala, G. D. Giuseppe, A. F. Abouraddy, and B. E. Saleh, “Bell's measure in classical optical coherence”, Nat. Phot. **7**, - see example C, 72 (2013).

[231] W. J. Munro, D. F. V. James, A. G. White, and P. G. Kwiat, “Maximizing the entanglement of two mixed qubits”, Phys. Rev. A **64**, 030302 (2001).

[232] T.-C. Wei, K. Nemoto, P. M. Goldbart, P. G. Kwiat, W. J. Munro, and F. Verstraete, “Maximal entanglement versus entropy for mixed quantum states”, Phys. Rev. A **67**, 022110 (2003).

[233] W. Dür and J. I. Cirac, “Classification of multiqubit mixed states: separability and distillability properties”, Phys. Rev. A **61**, 042314 (2000).

[234] A. Barasiński and J. Svozilík, “Controlled teleportation of qubit states: relation between teleportation faithfulness, controller's authority, and tripartite entanglement”, Phys. Rev. A **99**, 012306 (2019).

[235] O. Cohen and T. A. Brun, “Distillation of Greenberger-Horne-Zeilinger States by Selective Information Manipulation”, Phys. Rev. Lett. **84**, 5908 (2000).

[236] W. Dür, G. Vidal, and J. I. Cirac, “Three qubits can be entangled in two inequivalent ways”, Phys. Rev. A **62**, 062314 (2000).

[237] H. A. Carteret and A. Sudbery, “Local symmetry properties of pure three-qubit states”, J. Phys. A **33**, 4981 (2000).

[238] E. Halenková, A. Černoch, K. Lemr, J. Soubusta, and S. Drusová, “Experimental implementation of the multifunctional compact two-photon state analyzer”, Appl. Opt. **51**, 474–478 (2012).

[239] E. Schrödinger, “Discussion of Probability Relations between Separated Systems”, Math. Proc. Camb. Phil. Soc. **31**, 555–563 (1935).

[240] E. Schrödinger, “Probability relations between separated systems”, Math. Proc. Camb. Phil. Soc. **32**, 446–452 (1936).

[241] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, “Bell nonlocality”, Rev. Mod. Phys. **86**, 419–478 (2014).

[242] D. Cavalcanti and P. Skrzypczyk, “Quantum steering: a review with focus on semidefinite programming”, Rep. Prog. Phys. **80**, 024001 (2017).

[243] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, “Quantum steering”, Rev. Mod. Phys. **92** (2020).

[244] H. M. Wiseman, S. J. Jones, and A. C. Doherty, “Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox”, Phys. Rev. Lett. **98**, 140402 (2007).

[245] Y.-Y. Zhao, H.-Y. Ku, S.-L. Chen, H.-B. Chen, F. Nori, G.-Y. Xiang, C.-F. Li, G.-C. Guo, and Y.-N. Chen, "Experimental demonstration of measurement-device-independent measure of quantum steering", npj Quantum Inf. **6**, 77 (2020).

[246] H.-Y. Ku, S.-L. Chen, N. Lambert, Y.-N. Chen, and F. Nori, "Hierarchy in temporal quantum correlations", Phys. Rev. A **98**, 022104 (2018).

[247] J. F. Fitzsimons, J. A. Jones, and V. Vedral, "Quantum correlations which imply causation", Sc. Rep. **5**, 18281 (2015).

[248] T. Fritz, "Quantum correlations in the temporal Clauser-Horne-Shimony-Holt (CHSH) scenario", New J. Phys. **12**, 083055 (2010).

[249] Y.-N. Chen, C.-M. Li, N. Lambert, S.-L. Chen, Y. Ota, G.-Y. Chen, and F. Nori, "Temporal steering inequality", Phys. Rev. A **89**, 032112 (2014).

[250] K. Bartkiewicz, A. Černoch, K. Lemr, A. Miranowicz, and F. Nori, "Temporal steering and security of quantum key distribution with mutually unbiased bases against individual attacks", Phys. Rev. A **93**, 062345 (2016).

[251] R. T. Thew and W. J. Munro, "Mixed state entanglement: Manipulating polarization entangled photons", Phys. Rev. A **64**, 022320 (2001).

[252] C. Zhang, "Preparation of polarization-entangled mixed states of two photons", Phys. Rev. A **69**, 014304 (2004).

[253] T.-C. Wei, J. B. Altepeter, D. Branning, P. M. Goldbart, D. F. V. James, E. Jeffrey, P. G. Kwiat, S. Mukhopadhyay, and N. A. Peters, "Synthesizing arbitrary two-photon polarization mixed states", Phys. Rev. A **71**, 032329 (2005).

[254] G. Lima, F. Torres-Ruiz, L. Neves, A. Delgado, C. Saavedra, and S. Pádua, "Generating mixtures of spatial qubits", Opt. Commun. **281**, 5058–5062, ISSN: 0030-4018 (2008).

[255] A. Ling, P. Y. Han, A. Lamas-Linares, and C. Kurtsiefer, "Preparation of Bell states with controlled white noise", Laser Phys. **16**, 1140–1144, ISSN: 1555-6611 (2006).

[256] T.-J. Liu, C.-Y. Wang, J. Li, and Q. Wang, "Experimental preparation of an arbitrary tunable Werner state", EPL (Europhys. Lett.) **119**, 14002 (2017).

[257] G. Puentes, D. Voigt, A. Aiello, and J. P. Woerdman, "Tunable spatial decoherers for polarization-entangled photons", Opt. Lett. **31**, 2057–2059 (2006).

[258] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, "Exploring Hilbert space: Accurate characterization of quantum information", Phys. Rev. A **65**, 012301 (2001).

[259] Y.-S. Zhang, Y.-F. Huang, C.-F. Li, and G.-C. Guo, "Experimental preparation of the werner state via spontaneous parametric down-conversion", Phys. Rev. A **66**, 062315 (2002).

[260] C. Cinelli, G. Di Nepi, F. De Martini, M. Barbieri, and P. Mataloni, "Parametric source of two-photon states with a tunable degree of entanglement and mixing: Experimental preparation of Werner states and maximally entangled mixed states", Phys. Rev. A **70**, 022321 (2004).

[261] M. Caminati, F. De Martini, R. Perris, F. Sciarrino, and V. Secondi, "Nonseparable Werner states in spontaneous parametric down-conversion", Phys. Rev. A **73**, 032312 (2006).

[262] G. Puentes, A. Aiello, D. Voigt, and J. P. Woerdman, “Entangled mixed-state generation by twin-photon scattering”, Phys. Rev. A **75**, 032319 (2007).

[263] A. Aiello, G. Puentes, D. Voigt, and J. P. Woerdman, “Maximally entangled mixed-state generation via local operations”, Phys. Rev. A **75**, 062118 (2007).

[264] G. Brida, M. Genovese, M. V. Chekhova, and L. A. Krivitsky, “Tailoring polarization entanglement in anisotropy-compensated spontaneous parametric down-conversion”, Phys. Rev. A **77**, 015805 (2008).

[265] N. A. Peters, J. B. Altepeter, D. Branning, E. R. Jeffrey, T.-C. Wei, and P. G. Kwiat, “Maximally Entangled Mixed States: Creation and Concentration”, Phys. Rev. Lett. **92**, 133601 (2004).

[266] M. Barbieri, F. De Martini, G. Di Nepi, and P. Mataloni, “Generation and Characterization of Werner States and Maximally Entangled Mixed States by a Universal Source of Entanglement”, Phys. Rev. Lett. **92**, 177901 (2004).

[267] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, “Experimental Verification of Decoherence-Free Subspaces”, Science **290**, 498–501, ISSN: 0036-8075 (2000).

[268] W. J. Munro, D. F. V. James, A. G. White, and P. G. Kwiat, “Maximizing the entanglement of two mixed qubits”, Phys. Rev. A **64**, 030302 (2001).

[269] Y.-C. Jeong, J.-C. Lee, and Y.-H. Kim, “Experimental implementation of a fully controllable depolarizing quantum operation”, Phys. Rev. A **87**, 014301 (2013).

[270] K. Lemr, K. Bartkiewicz, and A. Černoch, “Experimental measurement of collective nonlinear entanglement witness for two qubits”, Phys. Rev. A **94**, 052334 (2016).

[271] M. Gavenda, A. Černoch, J. Soubusta, M. Dušek, and R. Filip, “Knowledge excess duality and violation of Bell inequalities: theory and experiment”, Mod. Phys. Lett. B **19**, 195–210 (2005).

[272] A. Aspect, J. Dalibard, and G. Roger, “Experimental Test of Bell’s Inequalities Using Time-Varying Analyzers”, Phys. Rev. Lett. **49**, 1804 (1982).

[273] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, “Detection-Loophole-Free Test of Quantum Nonlocality, and Applications”, Phys. Rev. Lett. **111**, 130406 (2013).

[274] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons”, Phys. Rev. Lett. **115**, 250401 (2015).

[275] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres”, Nature (London) **526**, 682 (2015).

[276] E. Shchukin and W. Vogel, “Inseparability Criteria for Continuous Bipartite Quantum States”, Phys, Rev. Lett. **95**, 230502 (2005).

[277] A. Miranowicz and M. Piani, “Comment on “Inseparability Criteria for Continuous Bipartite Quantum States””, Phys, Rev. Lett. **97**, 058901 (2006).

[278] A. Miranowicz, M. Piani, P. Horodecki, and R. Horodecki, “Inseparability criteria based on matrices of moments”, Phys. Rev. A **80**, 052303 (2009).

[279] I. Kogias, P. Skrzypczyk, D. Cavalcanti, A. Acín, and G. Adesso, “Hierarchy of Steering Criteria Based on Moments for All Bipartite Quantum Systems”, Phys. Rev. Lett. **115**, 210401 (2015).

[280] M. Navascués, S. Pironio, and A. Acín, “Bounding the Set of Quantum Correlations”, Phys. Rev. Lett. **98**, 010401 (2007).

[281] T. Richter and W. Vogel, “Nonclassicality of Quantum States: A Hierarchy of Observable Conditions”, Phys. Rev. Lett. **89**, 283601 (2002).

[282] W. Vogel, “Nonclassical Correlation Properties of Radiation Fields”, Phys. Rev. Lett. **100**, 013605 (2008).

[283] A. Miranowicz, M. Bartkowiak, X. Wang, Y.-x. Liu, and F. Nori, “Testing nonclassicality in multimode fields: A unified derivation of classical inequalities”, Phys. Rev. A **82**, 013824 (2010).

[284] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, “Volume of the set of separable states”, Phys. Rev. A **58**, 883–892 (1998).

[285] M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed states: necessary and sufficient conditions”, Phys. Lett. A **223**, 1–8 (1996).

[286] K. Audenaert, M. B. Plenio, and J. Eisert, “Entanglement Cost under Positive-Partial-Transpose-Preserving Operations”, Phys. Rev. Lett. **90**, 027901 (2003).

[287] S. Ishizaka, “Binegativity and geometry of entangled states in two qubits”, Phys. Rev. A **69**, 020301 (2004).

[288] C. Eltschka and J. Siewert, “Negativity as an Estimator of Entanglement Dimension”, Phys. Rev. Lett. **111**, 100503 (2013).

[289] W. K. Wootters, “Entanglement of Formation of an Arbitrary State of Two Qubits”, Phys. Rev. Lett. **80**, 2245–2248 (1998).

[290] J. K. Asbóth, J. Calsamiglia, and H. Ritsch, “Computable Measure of Nonclassicality for Light”, Phys. Rev. Lett. **94**, 173602 (2005).

[291] A. Miranowicz, K. Bartkiewicz, A. Pathak, J. Peřina Jr., Y. Chen, and F. Nori, “Statistical mixtures of states can be more quantum than their superpositions: Comparison of nonclassicality measures for single-qubit states”, Phys. Rev. A **91**, 042309 (2015).

[292] A. Miranowicz, K. Bartkiewicz, N. Lambert, Y. Chen, and F. Nori, “Increasing relative nonclassicality quantified by standard entanglement potentials by dissipation and unbalanced beam splitting”, Phys. Rev. A **92**, 062314 (2015).

[293] K. Bartkiewicz, P. Horodecki, K. Lemr, A. Miranowicz, and K. Życzkowski, “Method for universal detection of two-photon polarization entanglement”, Phys. Rev. A **91**, 032315 (2015).

[294] R. Augusiak, M. Demianowicz, and P. Horodecki, “Universal observable detecting all two-qubit entanglement and determinant-based separability tests”, Phys. Rev. A **77**, 030301 (2008).

[295] P. Skrzypczyk, M. Navascués, and D. Cavalcanti, “Quantifying Einstein-Podolsky-Rosen Steering”, Phys. Rev. Lett. **112**, 180404 (2014).

[296] M. Piani and J. Watrous, “Necessary and Sufficient Quantum Information Characterization of Einstein-Podolsky-Rosen Steering”, Phys. Rev. Lett. **114**, 060404 (2015).

[297] H.-Y. Ku, S.-L. Chen, C. Budroni, A. Miranowicz, Y.-N. Chen, and F. Nori, “Einstein-Podolsky-Rosen steering: Its geometric quantification and witness”, Phys. Rev. A **97**, 022338 (2018).

[298] S.-L. Chen, N. Lambert, C.-M. Li, A. Miranowicz, Y.-N. Chen, and F. Nori, “Quantifying Non-Markovianity with Temporal Steering”, Phys. Rev. Lett. **116**, 020503 (2016).

[299] H.-Y. Ku, S.-L. Chen, H.-B. Chen, N. Lambert, Y.-N. Chen, and F. Nori, “Temporal steering in four dimensions with applications to coupled qubits and magnetoreception”, Phys. Rev. A **94**, 062126 (2016).

[300] S.-L. Chen, N. Lambert, C.-M. Li, G.-Y. Chen, Y.-N. Chen, A. Miranowicz, and F. Nori, “Spatio-Temporal Steering for Testing Nonclassical Correlations in Quantum Networks”, Sc. Rep. **7**, 3728 (2017).

[301] F. Hirsch, M. T. Quintino, T. Vértesi, M. F. Pusey, and N. Brunner, “Algorithmic Construction of Local Hidden Variable Models for Entangled Quantum States”, Phys. Rev. Lett. **117**, 190402 (2016).

[302] M. Fillettaz, F. Hirsch, S. Designolle, and N. Brunner, “Algorithmic construction of local models for entangled quantum states: Optimization for two-qubit states”, Phys. Rev. A **98**, 022115 (2018).

[303] R. Horodecki, P. Horodecki, and M. Horodecki, “Violating Bell inequality by mixed states: necessary and sufficient condition”, Phys. Lett. A **200**, 340–344 (1995).

[304] R. Horodecki, “Two-spin-1/2 mixtures and Bell’s inequalities”, Phys. Lett. A **210**, 223–226 (1996).

[305] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, “Quantum nonlocality without entanglement”, Phys. Rev. A **59**, 1070 (1999).

[306] S. Popescu, “Bell’s inequalities versus teleportation: What is nonlocality?”, Phys. Rev. Lett. **72**, 797–799 (1994).

[307] A. Miranowicz, “Violation of Bell inequality and entanglement of decaying Werner states”, Phys. Lett. A **327**, 272–283 (2004).

[308] K. Bartkiewicz, K. Lemr, A. Černoch, and A. Miranowicz, “Bell nonlocality and fully entangled fraction measured in an entanglement-swapping device without quantum state tomography”, Phys. Rev. A **95**, 030102 (2017).

[309] A. C. Elitzur, S. Popescu, and D. Rohrlich, “Quantum nonlocality for each pair in an ensemble”, Phys. Lett. A **162**, 25–28 (1992).

[310] J. Barrett, A. Kent, and S. Pironio, “Maximally Nonlocal and Monogamous Quantum Correlations”, Phys. Rev. Lett. **97**, 170409 (2006).

[311] L. Aolita, R. Gallego, A. Acín, A. Chiuri, G. Vallone, P. Mataloni, and A. Cabello, “Fully nonlocal quantum correlations”, Phys. Rev. A **85**, 032107 (2012).

[312] S. Ghosh, G. Kar, A. Sen(De), and U. Sen, “Mixedness in the Bell violation versus entanglement of formation”, Phys. Rev. A **64**, 044301 (2001).

[313] T.-C. Wei, K. Nemoto, P. M. Goldbart, P. G. Kwiat, W. J. Munro, and F. Verstraete, “Maximal entanglement versus entropy for mixed quantum states”, Phys. Rev. A **67**, 022110 (2003).

[314] K. Banaszek, G. M. D’Ariano, M. G. A. Paris, and M. F. Sacchi, “Maximum-likelihood estimation of the density matrix”, Phys. Rev. A **61**, 010304 (1999).

[315] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, “Measurement of qubits”, Phys. Rev. A **64**, 052312 (2001).

[316] C. Sanderson and R. Curtin, “Armadillo: a template-based C++ library for linear algebra”, J. Open Source Software **1**, 26 (2016).

[317] C. Sanderson and R. Curtin, “A User-Friendly Hybrid Sparse Matrix Class in C++”, in *Mathematical Software – ICMS 2018*, Vol. 10931, Lecture Notes in Computer Science (Springer Int. Pub., 2018), pages 422–430.

[318] P. Girdhar and E. G. Cavalcanti, “All two-qubit states that are steerable via Clauser-Horne-Shimony-Holt-type correlations are Bell nonlocal”, Phys. Rev. A **94**, 032317 (2016).

[319] E. G. Cavalcanti, C. J. Foster, M. Fuwa, and H. M. Wiseman, “Analog of the Clauser-Horne-Shimony-Holt inequality for steering”, J. Opt. Soc. Am. B **32**, A74 (2015).

[320] A. C. S. Costa and R. M. Angelo, “Quantification of Einstein-Podolski-Rosen steering for two-qubit states”, Phys. Rev. A **93**, 020103 (2016).

[321] Č. Brukner, “Quantum causality”, Nat. Phys. **10**, 259 (2014).

[322] R. Horodecki, P. Horodecki, and M. Horodecki, “Violating bell inequality by mixed spin-12 states: necessary and sufficient condition”, Physics Letters A **200**, 340–344, ISSN: 0375-9601 (1995).

[323] K. Bartkiewicz, J. Beran, K. Lemr, M. Norek, and A. Miranowicz, “Quantifying entanglement of a two-qubit system via measurable and invariant moments of its partially transposed density matrix”, Phys. Rev. A **91**, 022323 (2015).

[324] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, “Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox”, Phys. Rev. A **80**, 032112 (2009).

[325] M. Grant and S. Boyd, *CVX: Matlab software for disciplined convex programming,* http://cvxr.com/cvx, 2012.

[326] D. Cavalcanti, L. Guerini, R. Rabelo, and P. Skrzypczyk, “General Method for Constructing Local Hidden Variable Models for Entangled Quantum States”, Phys. Rev. Lett. **117**, 190401 (2016).

[327] E. V. Shchukin and W. Vogel, “Nonclassical moments and their measurement”, Phys. Rev. A **72**, 043808 (2005).

[328] M. Hillery and M. S. Zubairy, “Entanglement Conditions for Two-Mode States”, Phys. Rev. Lett. **96**, 050503 (2006).

[329] R. M. Gomes, A. Salles, F. Toscano, P. H. S. Ribeiro, and S. P. Walborn, “Quantum entanglement beyond Gaussian criteria”, PNAS **106**, 21517 (2009).

[330] A. Wünsche, "Tomographic reconstruction of the density operator from its normally ordered moments", Phys. Rev. A **54**, 5291 (1996).

Appendix A Supplementary Material of Chapter 2

A.1 Strategies for assigning information to measurements performed on cloned pairs

During the transaction, a pair of states is taken from the card, which the hacker clones and from which we receive two pairs of copied qubits. To carefully consider the actual attack it is necessary to present all the situations in which the states are distorted. Using the knowledge of the protocol and assuming high fidelity of cloning, we can consider three strategies applied for analysing the results of measurements made on cloned pairs. For each measurement result, we assume the most likely situation.

A.1.1 Strategy a

We assume that both pairs of qubits are cloned perfectly. The measurements result in the same outcome for clones of the first qubit from a given pair and different outcome for clones of the second qubit from the pair. This is a strategy that allows to reject the largest number of possible options and gives the most information about the cloned state.
Example:

- The hacker measures two pairs ($|VA\rangle$, $|VA\rangle$) in the same basis, i.e., Q_{zz}.
- The result is: ($|VH\rangle$, $|VV\rangle$) or ($|VV\rangle$, $|VH\rangle$).
- The last bit of the hacker's information is assigned at random: ($01r$).

A.1.2 Strategy b

We assume that both qubits are cloned ideally, but the measurement results on each pair of clones are the same. This is a strategy allows us to reject half of the possible options, from which we are still able to obtain some information about the cloned state.
Example:

- The hacker measures two pairs ($|VA\rangle$, $|VA\rangle$) in the same basis, i.e., Q_{zz}.
- The result is: ($|VH\rangle$, $|VH\rangle$) or ($|VV\rangle$, $|VV\rangle$).
- The second or the third bit of the hacker's information is information is random: ($01r$ or $1r0$) = (010,011) or (100, 110), or ($01r$ or $1r1$) = (010, 011) or (101, 111). This results in four random options.

A.1.3 Strategy c

We assume that one of the clones is orthogonal to the cloned state. This is a strategy that does not allow the elimination of any possibility. We do not get any information about the cloned state.
Example:

- The hacker measures two pairs ($|HA\rangle$, $|VA\rangle$) in the same basis Q_{zz}.
- The result is: ($|HH\rangle$, $|VV\rangle$) or ($|HV\rangle$, $|VH\rangle$).
- All bits of the hacker's information are random, i.e., 8 options are equally probable: (000, 001, 010, 100, 110, 101, 011, 111).

A.1.4 Additional variants

There is also an option that two or more clones end up in the orthogonal state resulting in errors in the hacker's information. The probability of such situations is, however, for optimal phase-covariant cloner no larger than $(F-1)^2 = 0.0213$. In Tab. 4 we give the probability of a successful attack on a single pair when both qubits from a pair are cloned (variant 1) for strategies a_1 and b_1. The probability of a successful attack (assigning the correct information to a pair of qubits) for a single pair for measurement in any basis, when both qubits in the pair are cloned for strategy c (i.e., strategy c$_1$) is constant and equals to $\frac{1}{8}(F-1)F$. In Tab. 4 we also present the probabilities for the case where only one qubit from the pair has been cloned (variant 2, strategies a_2 and b_2). The probability of a successful attack on a single pair for measurement in any basis for strategy c when only one qubit from a pair is cloned (i.e., variant 2, strategy c_2) is constant and equals to $\frac{1}{16}(F-F^2+\frac{1}{4})$. Note that very similar analysis is valid for measurements Q_{xx}.

The table has been created using the following procedure. We assume that if the bank sends a bit sequence, let it be 000 (in general it is X – 8 possible sequences). Next, the cloning is performed. With probability P^2 it succeeds twice, with probability $2(1-P)P$ it succeeds once with only one of two qubits in the sequence, and with probability $(1-P)^2$ it fails and the attacker learns nothing. At this point we have already 4 cases to consider for 8 inputs. To simplify our explanations, let us analyse a case where $X = 000 \longrightarrow |HD\rangle$ (the same procedure is applied for all 8 inputs).

- **Variant 0:** With probability $(1-P)^2$ neither of the clones is created, thus, as in the case of erasure channel we get the following direct product of two probabilistic spaces:

  $\{[|HD\rangle, 1/4], [|HA\rangle, 1/4], [|VD\rangle, 1/4], [|VA\rangle, 1/4]\} \times$
  $\{[|HD\rangle, 1/4], [|HA\rangle, 1/4], [|VD\rangle, 1/4], [|VA\rangle, 1/4]\}.$

- **Variant 1:** For two clones the outcome of optimal cloning appearing with probability P^2 is a direct product of two probabilistic spaces, i.e., with probability P^2 both clones are created and F is fidelity of cloning:

  $\{[|HD\rangle, F^2], [|HA\rangle, F(1-F)], [|VD\rangle, F(1-F)], [|VA\rangle, (1-F)^2]\} \times$
  $\{[|HD\rangle, F^2], [|HA\rangle, F(1-F)], [|VD\rangle, F(1-F)], [|VA\rangle, (1-F)^2]\}.$

- **Variant 2:** With probability $(1-P)P$ the first qubit is cloned resulting in the following direct product of two probabilistic spaces:

$\{[|HD\rangle, \frac{F}{2}], [|HA\rangle, \frac{F}{2}], [|VD\rangle, \frac{1-F}{2}], [|VA\rangle, \frac{1-F}{2}]\} \times$
$\{[|HD\rangle, \frac{F}{2}], [|HA\rangle, \frac{F}{2}], [|VD\rangle, \frac{1-F}{2}], [|VA\rangle, \frac{1-F}{2}]\}$

- **Variant 2:** With probability $(1-P)P$ the second qubit is cloned resulting in the following direct product of two probabilistic spaces:
  $\{[|HD\rangle, \frac{F}{2}], [|HA\rangle, \frac{1-F}{2}], [|VD\rangle, \frac{F}{2}], [|VA\rangle, \frac{1-F}{2}]\} \times$
  $\{[|HD\rangle, \frac{F}{2}], [|HA\rangle, \frac{1-F}{2}], [|VD\rangle, \frac{F}{2}], [|VA\rangle, \frac{1-F}{2}]\}$.

To complete the stochastic trees we need to explain the decision process of the attacker as outlined above to guess three bits Y according to strategies a,b, and c. Let us choose query Q_{xx}. The attacker can measure (with some probability given by the above-listed probabilistic spaces):

- DD, $DD \longrightarrow$ set $Y = 000$ or $Y = 001$ or $Y = 101$ or $Y = 110$ with equal probability.
- DD, $DA \longrightarrow$ set $Y = 000$ or $Y = 001$ with equal probability.
- DD, $AD \longrightarrow$ set $Y = 100$ or $Y = 101$ with equal probability.
- DD, $AA \longrightarrow$ impossible, set any Y with equal probability OR do nothing.
- DA, $DD \longrightarrow$ set $Y = 000$ or $Y = 001$ with equal probability.
- DA, $DA \longrightarrow$ set $Y = 001$ or $Y = 011$ or $Y = 100$ or $Y = 101$ with equal probability
- DA, $AD \longrightarrow$ impossible, set any Y with equal probability OR do nothing.
- DA, $AA \longrightarrow$ set $Y = 001$ or $Y = 011$ with equal probability.
- AD, $DD \longrightarrow$ set $Y = 000$ or $Y = 010$ with equal probability.
- AD,$DA \longrightarrow$ impossible, set any Y with equal probability OR do nothing.
- AD, $AD \longrightarrow$ set $Y = 110$ or $Y = 111$ or $Y = 000$ or $Y = 010$ with equal probability.
- AD, $AA \longrightarrow$ set $Y = 110$ or $Y = 111$ with equal probability.
- AA, $DD \longrightarrow$ impossible, set any Y with equal probability OR do nothing.
- AA, $DA \longrightarrow$ set $Y = 001$ or $Y = 011$ with equal probability.
- AA, $AD \longrightarrow$ set $Y = 110$ or $Y = 111$ with equal probability.
- AA, $AA \longrightarrow$ set $Y = 001$ or $Y = 011$ or $Y = 110$ or $Y = 111$ with equal probability.

If the query is Q_{zz}, the logic is the same. Finally, by tracking the relevant branches of stochastic tree, we create probability tables. Having explained all the steps, a complete stochastic tree for a given query would have the following structure: 8 input states $X \longrightarrow$ 4 cloning failure/success events $\longrightarrow$ 16 qubit pairs $\longrightarrow$ 16 measurement outcomes $\longrightarrow$ 8 states Y. The complete analysis of the tree would correspond to tracking 8 nodes $\longrightarrow$ 32 nodes $\longrightarrow$ 512 nodes $\longrightarrow$ 8192 nodes $\longrightarrow$ 65536 nodes. Note that the attacker

Table 4: Joint probability distribution describing encoded bits and hacker's knowledge Y gained from an attack on a single pair of qubits encoding 3-bit sequence X for query Q_{zz} or after swapping two last bits of X and Y for query Q_{xx}. When cloning both qubits in the pair and deal with strategy a (i.e., strategy a_1), we have $p_1 = \frac{1}{4}F^2$, $p_2 = \frac{1}{4}(1-F)^2$, and $p_3 = \frac{1}{4}F(1-F)$. In the same regime, for strategy b (i.e., strategy b_1), we have $p_1 = \frac{1}{8}F^2$, $p_2 = \frac{1}{8}(1-F)^2$, and $p_3 = \frac{1}{8}F^2 - \frac{1}{8}F + \frac{1}{16}$. If successful cloning was achieved only with one qubit from a pair, we assume that the second qubit of the pair is associated with two completely mixed clones of the fidelity of $1/2$. In this second regime we have for strategy a (i.e., strategy a_2) $p_1 = \frac{1}{8}F^2 + \frac{1}{32}$, $p_2 = \frac{1}{8}F^2 - \frac{1}{4}F + \frac{5}{32}$, and $p_3 = -\frac{1}{8}F^2 + \frac{1}{8}F + \frac{1}{32}$. Under the same assumption on cloning in case of strategy b we have $p_1 = \frac{1}{16}F^2 + \frac{1}{64}$, $p_2 = \frac{1}{16}F^2 - \frac{1}{16}F + \frac{5}{64}$, and $p_3 = \frac{1}{16}F^2 - \frac{1}{16}F + \frac{3}{64}$.

	000	001	010	011	100	101	110	111
000	p_1	p_1	p_2	p_2	p_3	p_3	p_3	p_3
001	p_1	p_1	p_2	p_2	p_3	p_3	p_3	p_3
010	p_2	p_2	p_1	p_1	p_3	p_3	p_3	p_3
011	p_2	p_2	p_1	p_1	p_3	p_3	p_3	p_3
100	p_3	p_3	p_3	p_3	p_1	p_1	p_2	p_2
101	p_3	p_3	p_3	p_3	p_1	p_1	p_2	p_2
110	p_3	p_3	p_3	p_3	p_2	p_2	p_1	p_1
111	p_3	p_3	p_3	p_3	p_2	p_2	p_1	p_1

knows when the cloning succeeds/fails and what is measured. Thus, also for each cloning failure/success event and each query a separate probability table is created. Finally, three different probability tables are created depending on the decision strategy (the attacker differentiates between the strategies).

The hacker, collecting the results of measurements, is able to learn the algorithm of encoding pairs of qubits. However, in order to make it possible the cloning fidelity must be optimized. Cloning operation unavoidably involves causing errors in the measurement results used for verification. If the level of incorrect results exceeds the specified limit the transaction will be rejected. In order to minimize the error rate it is, therefore, necessary to implement an attack strategy that takes into account all measurement circumstances.

A.2 Attack-verification scenarios

There are 3 attack–verification scenarios that we consider in our work:

- **Scenario (i):** Providing the bank with results each time cloning takes place. If cloning fails, sending random values.

- **Scenario (ii):** Providing the bank with results only when the measurement is recorded by the terminal. In case of unsuccessful cloning, the loss of the qubit is reported.

- **Scenario (iii):** Measurement of qubits in the specified database after the card is removed from terminal, without cloning operation. Random results are sent to the bank.

Note that in the main text these cases are referred to as strategies. However, here it is more suitable to call them scenarios.

From direct calculations based on the probabilities leading to verification error, we can derive an expression concerning the frequency of errors in the verification of a pair of qubits ϵ. This is the probability of reporting an error to the bank. Note that it depends only on what happens to a qubit measured in a compatible basis. For each strategy, the error rate is described by the respective equation [see Eq. (2) and (3) in the main text], i.e.:

$$\begin{aligned}\epsilon_{\text{(i)}} &= P(1-F)+(1-P)/2,\\ \epsilon_{\text{(ii)}} &= (1-F),\\ \epsilon_{\text{(iii)}} &= \frac{1}{2}.\end{aligned}$$

The parameter $\epsilon_{\text{(i)}}$ takes into account two situations. In the first case, one or both cubits are lost during cloning and therefore random results are reported to the bank (50% chance of getting an error). In the second case, even if the cloning is successful, imperfect fidelity may cause the measurement to give an incorrect result. The error rate in scenario (ii) depends only on the imperfect fidelity of the cloning.

A.3 Mutual information

In order to quantify the correlation between the attacker and the information encoded as a pair of qubits, we enter the value of mutual information I. This value determines how many bits of information an attacker can get after cloning one pair of qubits and depends on the strategy used, cloning the probability of success P and fidelity F. Mutual information is calculated as

$$I = I_{X,Y} = I_{Y,X} = \sum_{X,Y=000}^{111} p_{X,Y} \log_2 \frac{p_{X,Y}}{p_X p_Y},$$

where $p_X = \sum_{Y=000}^{111} p_{X,Y}$, $p_Y = \sum_{X=000}^{111} p_{X,Y}$, and X, Y = 000, 001, 010, 100, 110, 101, 011, 111. When considering scenario (i) to calculate mutual information we need to utilise probabilities from Tabs. 1–4 and possibility uniform probability distribution (the cloned pair is lost) referred to as strategy 0. The mutual information for security analysis of scenarios (i) and (ii), respectively, reads

$$\begin{aligned}I_{\text{sec(i)}} &= P^2(I_{a_1}+I_{b_1}+I_{c_1})\\ &\quad +2P(1-P)(I_{a_2}+I_{b_2}+I_{c_2})+(1-P)^2 I_0\end{aligned}$$

and

$$I_{\text{sec(ii)}} = I_{a_1}+I_{b_1}+I_{c_1},$$

where $I_0 = 0$ and the subscripts denote the strategy. These values are query independent. For scenario (iii) the information learned by the hacker is $I_{\text{sec(iii)}} = \frac{1}{2}$. Note that for this strategy while the attacker can eliminate some of 8 encodings (values of Y), these eliminated encodings depend on the order of basis. The attacker can assume/guess that the order of encoding bases for the received pair of qubits is XZ or ZX. The order must be random because there is no way of gaining this information (thus maximum

Table 5: Joint probability distribution describing encoded bits and hacker's knowledge Y gained from an attack on a single pair of qubits encoding 3-bit sequence X for query Q_{xx} (i.e., XX–basis measurement) for scenario (iii), where the attacker assumes at random encoding XZ or ZX.

	000	001	010	011	100	101	110	111
000	$\frac{1}{32}$	0	$\frac{1}{32}$	0	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
001	0	$\frac{1}{32}$	0	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
010	$\frac{1}{32}$	0	$\frac{1}{32}$	0	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
011	0	$\frac{1}{32}$	0	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
100	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{32}$	0	$\frac{1}{32}$	0
101	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	0	$\frac{1}{32}$	0	$\frac{1}{32}$
110	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{32}$	0	$\frac{1}{32}$	0
111	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	0	$\frac{1}{32}$	0	$\frac{1}{32}$

Table 6: Joint probability distribution describing encoded bits and hacker's knowledge Y gained from an attack on a single pair of qubits encoding 3-bit sequence Z for query Q_{zz} (i.e., ZZ–basis measurement) for scenario (iii), where the attacker assumes at random encoding XZ or ZX.

	000	001	010	011	100	101	110	111
000	$\frac{1}{32}$	$\frac{1}{32}$	0	0	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
001	$\frac{1}{32}$	$\frac{1}{32}$	0	0	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
010	0	0	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
011	0	0	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$
100	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{32}$	$\frac{1}{32}$	0	0
101	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{32}$	$\frac{1}{32}$	0	0
110	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	0	0	$\frac{1}{32}$	$\frac{1}{32}$
111	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	0	0	$\frac{1}{32}$	$\frac{1}{32}$

information to gain is here $I_{\max} = 2$ instead of $I_{\max} = 3$ when the order is known). Then, under this assumption, with probability 1/2 the attacker, depending on the measurement outcomes (query Q_{xx} or Q_{zz} - honest but curious attacker), can exclude some encodings. The attacker can guess the order of bases correctly only in half of the cases. Only if successful, half of 4 encodings can be eliminated. This makes $I_{\mathrm{sec(iii)}} = \frac{1}{4}I_{\max} = \frac{1}{2}$. This is confirmed by direct calculations based on Tab. 5 or Tab. 6.

Note that Figs. 2 and 3 presented in the main text are depict functions $I_{\mathrm{sec}(n)}[\epsilon(n)]$ for $n =$ i,ii,iii. In case of Fig. 3 depicting conditional mutual information, $I_{\mathrm{sec(i)}}$ is calculated assuming $P = 1$, because in this case the hacker infers the information only if both qubits are cloned.

Appendix B Supplementary Material of Chapter 3

B.1 Analytical Derivation of Eq. (3.9)

The CHSH inequality for general two-qubit state ρ can be written as [322]

$$|\mathbf{a}_0 \cdot R^\rho \cdot (\mathbf{b}_0 + \mathbf{b}_1) + \mathbf{a}_1 \cdot R^\rho \cdot (\mathbf{b}_0 - \mathbf{b}_1)\,| \leq 2, \tag{B1}$$

where $\mathbf{a}_0$, $\mathbf{a}_1$, $\mathbf{b}_0$, $\mathbf{b}_1$ are unitary vectors in $\mathbb{R}^3$ and R^ρ denotes the 3×3 correlation matrix with elements $R^\rho_{ij} = \mathrm{Tr}[\rho\,(\sigma_i \otimes \sigma_j)]$ given in terms of the three Pauli matrices. For the special case, when ρ stands for the Werner state (in the form proposed in Ref. [98]), the correlation matrix $R = -v\mathbb{1}_3$, where v is the visibility.

Next we introduce a pair of unitary vectors $\mathbf{c}_0$ and $\mathbf{c}_1$ by $\mathbf{b}_0 + \mathbf{b}_1 = \mathbf{c}_0\sqrt{2(1+x)}$, $\mathbf{b}_0 - \mathbf{b}_1 = \mathbf{c}_1\sqrt{2(1-x)}$, where $x = \mathbf{b}_0 \cdot \mathbf{b}_1$. Substituting all these quantities into Eq. (B1), one has

$$|\mathbf{a}_0 \cdot \mathbf{c}_0\sqrt{1+x} + \mathbf{a}_1 \cdot \mathbf{c}_1\sqrt{1-x}| \leq \frac{\sqrt{2}}{v}. \tag{B2}$$

To prove Eq. (3.9) we shall find how often inequality (B2) is violated when unit vectors $\mathbf{a}_0$, $\mathbf{a}_1$, $\mathbf{c}_0$, $\mathbf{c}_1$ and the variable x are chosen independently, randomly, and isotropically. Following arguments presented in Ref. [193], to solve the above problem, it is sufficient to sample x and dot products $\mathbf{a}_0 \cdot \mathbf{c}_0$ and $\mathbf{a}_1 \cdot \mathbf{c}_1$ uniformly from the interval $[-1, 1]$ as the actual direction of individual vectors is irrelevant (hereafter, we use $\alpha = \mathbf{a}_0 \cdot \mathbf{c}_0$ and $\beta = \mathbf{a}_1 \cdot \mathbf{c}_1$).

From a geometrical point of view, this solution denotes the fraction of the cube's volume containing points (α, β, x) violating the inequality (B2). For a particular fixed x, the regime of the cube containing points violating Eq. (B2) are given by

$$\begin{aligned} \beta &> \frac{\sqrt{2} - \alpha v\sqrt{1+x}}{v\sqrt{1-x}}, \\ \beta &< -\frac{\sqrt{2} + \alpha v\sqrt{1+x}}{v\sqrt{1-x}}. \end{aligned} \tag{B3}$$

Therefore, with some straightforward calculation, one can find that the fraction of Alice and Bob's measurement directions that would violate the CHSH inequality and, hence, the nonlocal fraction is given by

$$p_{\mathrm{V}} = 4\int_{x_-}^{x_+} \frac{\left(\sqrt{2} - v(\sqrt{1-x} + \sqrt{1+x})\right)^2}{V_{\mathrm{cube}}\; v^2\sqrt{1-x^2}}\,dx, \tag{B4}$$

where $V_{\mathrm{cube}} = 2^3$ stand for the cube's volume, the integration is performed for $x_\pm = \pm\sqrt{\frac{2v^2-1}{v^4}}$ and the result is multiplied by 4 to take into account any possible relabelling of measurement settings and/or outcomes. This is because, for any given measurement directions, at most one of the CHSH inequalities can be violated. The value of $x_\pm$ is caused by the fact that for fixed v and $x > x_+$ ($x < x_-$), there are no pairs (α, β) (both in the interval $[-1, 1]$) which satisfy constraints (B2). After appropriate integration in Eq. (B3), we obtain Eq. (3.9). Note that for $v = 1$ the nonlocal fraction $p_V = 2(\pi - 3)$, which is in line with [193].

B.2 Nonlocal Fraction Based on the Distribution of the Strength of Violation

Let us take a three-qubit state ρ and a finite set of measurement settings $\{\hat{M}_i\}$, where $i = 1, \ldots, m$. To verify whether the genuine nonlocal correlations are generated for the state ρ and given measurement setting $\hat{M}_i$, one should test 185 Bell inequalities [213] of the form $\tilde{\mathcal{I}}_j(\rho|M_i) \leq C_j^{\mathrm{LHV}}$, where $j = 1, \ldots, 185$. To this end, it is expedient to consider $C_j^{\mathrm{LHV}} = 1$ and $\mathcal{I}_j(\rho|M_i) = \tilde{\mathcal{I}}_j(\rho|M_i)/C_{\mathrm{LHV}}$. Based on such a test, a maximal strength of violation for $\hat{M}_i$ is determined as $\mathcal{I}_i^{\max}(\rho) = \max_j\{\mathcal{I}_j(\rho|M_i)\}$, where the maximum is taken over 185 Bell inequalities. Dividing the number of $\mathcal{I}_i^{\max}(\rho)$, satisfying the constraints $\mathcal{I}_i^{\max}(\rho) > 1$, by the number of measurement settings m, the nonlocal fraction is estimated

$$p_{\mathrm{V}}(\rho) = \lim_{m\to\infty} \frac{n\Big(\{\mathcal{I}_i^{\max}(\rho), \mathcal{I}_i^{\max}(\rho) > 1\}\Big)}{m}. \tag{B5}$$

Next, let us consider a state $\sigma(v) = v\rho + (1 - v)/8 \cdot \mathbb{1}_8$, i.e., a statistical mixture of the state ρ and white noise. Then, one can easily prove that $\mathcal{I}_j(\sigma|M_i) = v\ \mathcal{I}_j(\rho|M_i)$ and, hence, the maximal strength of violation $\mathcal{I}_i^{\max}(\sigma) = v\ \mathcal{I}_i^{\max}(\rho)$. Consequently, by analogy to Eq. (B5), the nonlocal fraction of state σ can be written

$$p_{\mathrm{V}}(\sigma) = \lim_{m\to\infty} \frac{n\Big(\{\mathcal{I}_i^{\max}(\rho), \mathcal{I}_i^{\max}(\rho) > \mathcal{I}_{\min} = 1/v\}\Big)}{m}. \tag{B6}$$

In other words, if one knows the distribution of the strength of violation $\{\mathcal{I}_i^{\max}(\rho)\}$, then the nonlocal fraction of any state $\sigma(v)$ can be estimated by suitable shiftiness of the classical threshold denoted by $\mathcal{I}_{\min}$. As a result, one can find a relationship between $p_{\mathrm{V}}(\sigma)$ and the visibility v (c.f. Fig. 3.3(a)).

In particular, if we assume that $\rho = \rho_3(\theta, v_0)$, then the state $\sigma(v) = v \cdot v_0 \left|\theta\right\rangle_3 \left\langle\theta\right| + + \frac{1-v\cdot v_0}{8}\mathbb{1}_8$ and the relationship between $p_{\mathrm{V}}(\sigma)$ and v is described by Eq. (3.15) with unknown values v_0 and angle θ. Therefore, Eq. (3.15) can be rewritten as

$$v = \frac{1}{v_0}\left(v_3^{\mathrm{cr}}(\theta) + g_1(\theta)\ p_{\mathrm{V}}^{1/6} + g_2(\theta)\ p_{\mathrm{V}}^{1/2} + g_3(\theta)\ p_{\mathrm{V}}\right). \tag{B7}$$

By fitting the distribution $p_{\mathrm{V}}(\sigma)$ versus v described previously with Eq. (B7) one obtains an approximation of both parameters v_0 and θ.

Appendix C: Supplementary Material of Chapter 4

C.1 Universal Detection of Quantum Correlations Without Full Quantum State Tomography

In this work we determined quantum correlations from experimentally generated and reconstructed states using a full QST. Here we address the question of universal detection of quantum correlations *without* full QST.

(a) *Universal detection of an entanglement measure without QST.*— The first experimental universal detection of standard two-qubit entanglement without full QST has been proposed in Ref. [293] (see also [323]) based on the universal witness of Ref. [294]. This method has been later improved in Ref. [198] to show theoretically a direct experimental method for determining the negativity of a general two-qubit state based on eleven measurements performed on multiple copies of the state using Hong-Ou-Mandel interference. To our knowledge, none of these methods of universal entanglement detection without a full state tomography has been demonstrated experimentally yet because of the complexity of such setups and low probability of required multiple coincidences. Note that an experimental detection, without a complete tomography, of the fully entangled fraction of Bennett *et al.* [199] has been demonstrated by us in Ref. [308]. Unfortunately, the fully entangled fraction is *not* a universal entanglement witness in general, so it usually only gives a sufficient (but not necessary) condition of entanglement.

(b) *Universal detection of a steering measure without QST.*— To our knowledge, such methods have been implemented or even proposed neither for the steering robustness nor the steerable weight. The calculations of these popular steering measures for general states are based on numerical optimization (using semidefinite programs). Thus, in general, these measures up to now can only be determined experimentally for tomographically reconstructed states or processes, as it has been done in dozens of experimental works (see reviews [242, 243] and references therein). Of course, there are many experiments demonstrating quantum steering via nonuniversal witnesses (to reveal a hierarchy of criteria), i.e., by observing the violations of steering inequalities [242, 243]. We note that measures of steering (e.g., that proposed for a 2MS and a 3MS in Ref. [320]) which are based on the maximal violation of well-established steering inequalities can be measured without a complete QST. For example, the optimal violation of the Cavalcanti-Jones-Wiseman-Reid inequality [324] can in principle be experimentally demonstrated with polarized photons without scanning all the angles of polarisers. This can be done, as we anticipate, in systems similar to those demonstrating the Horodecki measure of Bell nonlocality [308].

(c) *Universal detection of a nonlocality measure without QST.*—The Horodecki measure [303, 304]) of Bell-CHSH nonlocality of two-qubit states can indeed be measured without a full QST, but, to our knowledge, it has been first determined experimentally only recently in our experiment [308] without scanning the angles of the polarisers to obtain an optimal value of the angles maximizing the violation of the Bell-CHSH inequality for an unknown two-qubit state. To demonstrate the power of this method, we have implemented an entanglement-swapping device. To our knowledge, no other experimental universal detections of a nonlocality measure (without scanning the polarization angles or without *a priori* information about a given generated state) have been reported yet.

C.2 Steerable Weight in a Three-Measurement Scenario

Here we consider two-qubit EPR steering in a 3MS, when Alice performs the measurements of the three Pauli operators: $X = |+\rangle\langle+| - |-\rangle\langle-|$, $Y = |R\rangle\langle R| - |L\rangle\langle L|$, $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, of qubits encoded in the polarization states of photons, as in our experiment. Thus, these measurements are just the projections onto the Pauli-operator eigenstates $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, $|R\rangle = (|0\rangle + i\,|1\rangle)/\sqrt{2}$, $|L\rangle = (|0\rangle - i\,|1\rangle)/\sqrt{2}$, $|0\rangle$, and $|1\rangle$, which correspond to the diagonal, anti-diagonal, right-circular, left-circular, horizontal, and vertical polarization states, respectively. These measurements of Alice generate unnormalized states $\sigma_{a|x}$ of Bob for $x = X, Y, Z$ assuming measured eigenvalues $a = \pm 1$. By denoting $f(|m\rangle) = \mathrm{Tr}_A[(|m\rangle\langle m| \otimes I)\rho]$, the six possible unnormalized Bob states $\sigma_{a|x}$ read as:

$$\begin{aligned} \sigma_{+1|X} &= f(|+\rangle), \quad \sigma_{-1|X} = f(|-\rangle), \\ \sigma_{+1|Y} &= f(|R\rangle), \quad \sigma_{-1|Y} = f(|L\rangle), \\ \sigma_{+1|Z} &= f(|0\rangle), \quad \sigma_{-1|Z} = f(|1\rangle). \end{aligned} \tag{C1}$$

Alice, after performing her measurements, holds a classical random variable $\lambda \equiv [x, y, z] = [\langle x|X|x\rangle, \langle y|Y|y\rangle, \langle z|Z|z\rangle]$, where hereafter $x, y, z = \pm 1$. Thus, the variable λ can take the values $\lambda_1 = [-1, -1, -1]$, $\lambda_2 = [-1, -1, 1]$, ..., and $\lambda_8 = [1, 1, 1]$. The unsteerable assemblage $\sigma^{\mathrm{US}}_{a|x}$, can now be expressed as: $\sigma^{\mathrm{US}}_{\pm 1|X} = \sum_{y,z} \sigma_{\pm 1,y,z}$, $\sigma^{\mathrm{US}}_{\pm 1|Y} = \sum_{x,z} \sigma_{x,\pm 1,z}$, and $\sigma^{\mathrm{US}}_{\pm 1|Z} = \sum_{x,y} \sigma_{x,y,\pm 1}$, where $\sigma_\lambda \equiv \sigma_{xyz}$ are the states held by Bob.

The steerable weight S_3 in our 3MS can be given by the solution of the following SDP (semidefinite program):

$$S_3 = 1 - \max \mathrm{Tr} \sum_{x,y} \sigma_{xyz}, \tag{C2}$$

such that $\sigma_{xyz} \geq 0$ and

$$\begin{aligned} \sigma_{\pm 1|X} &- \sum_{y,z} \sigma_{\pm 1,y,z} \geq 0, \\ \sigma_{\pm 1|Y} &- \sum_{x,z} \sigma_{x,\pm 1,z} \geq 0, \\ \sigma_{\pm 1|Z} &- \sum_{x,y} \sigma_{x,y,\pm 1} \geq 0. \end{aligned} \tag{C3}$$

C.3 Steerable Weight in Two-Measurement Scenarios

The above approach can be simplified when analysing EPR steering in 2MSs, i.e., when Alice is performing the measurements of only two Pauli operators (XY, XZ, and YZ). Thus, one can consider the following three measures:

(i) The steerable weight S_2^{XY} for the measurements of X and Y. In this case the corresponding unsteerable assemblage $\sigma^{\text{US}}_{a|x}$ can be expressed as $\sigma^{\text{US}}_{\pm1|X} = \sum_y \sigma_{\pm1,y}$ and $\sigma^{\text{US}}_{\pm1|Y} = \sum_x \sigma_{x,\pm1}$, where $\sigma_\lambda \equiv \sigma_{xy}$ are the states held by Bob. Then the corresponding steerable weight S_2^{XY} can be calculated as the solution of the following SDP:

$$S_2^{XY} = 1 - \max \operatorname{Tr} \sum_{x,y} \sigma_{xy}, \tag{C4}$$

under the constraints: $\sigma_{xy} \geq 0$ and

$$\sigma_{\pm1|X} - \sum_y \sigma_{\pm1,y} \geq 0, \quad \sigma_{\pm1|Y} - \sum_x \sigma_{x,\pm1} \geq 0. \tag{C5}$$

(ii) The steerable weight S_2^{XZ}, based on Alice's measurements of the Pauli operators X and Z, is given by:

$$S_2^{XZ} = 1 - \max \operatorname{Tr} \sum_{x,z} \sigma_{xz} \tag{C6}$$

such that $\sigma_{xz} \geq 0$ and

$$\sigma_{\pm1|X} - \sum_z \sigma_{\pm1,z} \geq 0, \quad \sigma_{\pm1|Z} - \sum_x \sigma_{x,\pm1} \geq 0. \tag{C7}$$

(iii) The steerable weight S_2^{YZ} corresponding to measuring the Pauli operators Y and Z can be calculated as

$$S_2^{YZ} = 1 - \max \operatorname{Tr} \sum_{y,z} \sigma_{y,z}, \tag{C8}$$

under the conditions $\sigma_{yz} \geq 0$, and

$$\sigma_{\pm1|Y} - \sum_z \sigma_{\pm1,z} \geq 0, \quad \sigma_{\pm1|Z} - \sum_y \sigma_{y,\pm1} \geq 0. \tag{C9}$$

The optimized 2MS steerable weight (S_2) can be given as the maximum value of the steerable weights for specific measurement choices, i.e.,

$$S_2 = \max(S_2^{XY}, S_2^{XZ}, S_2^{YZ}). \tag{C10}$$

This definition of S_2 can directly be applied to symmetric states, including the Werner states and GWSs. However, for non-symmetric states (including some of our experimental density matrices), the optimal projectors can be found numerically by maximizing the steerable weight over unitary transformations for any two Pauli operators. In our experiments and theoretical analysis, we apply only single Pauli operators (rather than their linear combinations) and then optimize them over their unitary transformations. Thus, we obtained the steerable weights, which were optimized over von Neumann's projection-valued measures (PVMs), instead of the most general case of POVMs. Note that the required optimization over POVMs is more demanding both experimentally and theoretically and it is not applied in this work. We find that, on the scale of

Figs. 4.4(c) and 4.5(c), no differences can be seen for S_2 if it is calculated by the optimized projectors and by applying directly Eq. (C10) for any of the measured states.

Note that, in this approach to determine S_2, we are limiting the number of the types of measurements on Alice's side, but a full QST is always assumed on Bob's side corresponding to measuring all the Pauli operators. Thus, the steerable weight S_3 corresponds to a 3-3 measurement scenario, i.e., three types of measurements on Alice's and Bob sides (assuming that the efficiency of detectors is known). While the steerable weight S_2^{ij} (for the specific choice of two Pauli operators) corresponds to a 2-3 scenario, i.e., based on two types of measurements on Alice's side and three on Bob's side.

All these steerable weights in the two- and three-measurement scenarios can be efficiently calculated numerically as solutions of the described semidefinite programs using standard numerical packages for convex optimization. Our numerical programs are based on the software for disciplined convex programming of Ref. [325]. The steerable weights in our work were calculated using experimental density matrices, which were reconstructed using a full quantum tomography.

C.4 Steerability in Multi-Measurement Scenarios

A related question arises about the steerability using a larger number n of the types of measurements on Alice's side, and especially in the limit of an infinite number of measurements. The algorithms of Refs. [301, 302, 326] for constructing LHS models can be applied to arbitrary entangled states and thus can be used for finding numerically a sufficient condition of unsteerability (i.e., a lower bound on steerability) based on a given number of projective measurements. Note that for the GWSs, such a lower bound on steerability was determined up to $n = 136$ measurements in Ref. [302]. For convenience, we consider here a steering lower bound $p_S^{\text{low}}(n)$, which can be numerically determined by the protocols of Refs. [301, 302] for a given number n of measurements. We also consider a steering upper bound $p_S^{\text{up}}(n)$, being a sufficient condition for steerability, based on an SDP technique of Ref. [242] (see also [302]) assuming specifically 13 measurements on the Bloch sphere.

The algorithm of Refs. [301, 302] has already been applied to the steerability of the Bell-diagonal states (including the Werner states) and GWSs (there referred to as partially entangled states with white noise). Sufficient conditions of unsteerability, corresponding to $n = 6$, 16, 46, and 136 types of measurements, were found for four levels of the algorithm [302]. These results can enable calculating $p_S^{\text{low}}(n)$. Note that each type of measurement is characterized by a Bloch vector, and all such vectors form a polyhedron on the Bloch sphere.

It is quite challenging to numerically calculate the lower bound $p_S^{\text{low}}(n)$ of steerability in multi-measurement scenarios, even for the next layer of the protocol of Filletaz *et al.* [302] (corresponding to the number of measurements greater than 136) because of the problem which is closely related to the "curse of dimensionality". Indeed, the number of deterministic strategies to be checked numerically grows exponentially with the number of measurements. The results should also be optimized for the orientation of the polyhedra; otherwise the results differ significantly, as explicitly shown in Ref. [301].

The ranges of the allowed values of the mixing (p) and superposition (q) parameters in $\rho_{\text{GW}}(p,q)$, for which the GWSs are steerable, increase with the number of measurements n. Thus, finding numerically a solution to these steering problems could in principle enable us to analyse a more refined hierarchy of the classes of steerability as a function of the number of measurements such that a given state is steerable using a given number of measurements, but unsteerable using a smaller number of measurements. But an experimental demonstration of such a refined hierarchy is quite challenging, as explained below.

Clearly, a direct experimental demonstration that a given state is indeed unsteerable based on 136 types of measurements is extremely demanding using linear optics. However, even theoretical demonstration of such a refined hierarchy of the classes of multi-measurement steerability for tomographically reconstructed experimental states is quite challenging. These problems include the following:

First problem.—We recall that our experimental GWSs, $\rho^E_{\rm GW}(p,q)$, have a high Bures fidelity F compared to the theoretical optimal GWSs, $\rho_{\rm GW}(p_{\rm opt}, q_{\rm opt})$ which on average are equal to 0.97. Nevertheless, $\rho^E_{\rm GW}(p,q)$ and $\rho_{\rm GW}(p_{\rm opt}, q_{\rm opt})$ can still have very different steering properties such that one of the states is steerable and the other is unsteerable in the same n-measurement scenario, especially for $n > 3$.

Note that all the examples of multi-measurement steerability, based on the protocols of Refs. [301, 302, 326], were numerically tested only for highly-symmetric states (including the Werner states and GWSs). Unfortunately, our experimental states $\rho^E_{\rm GW}$ have usually a broken symmetry compared to that of the theoretical GWSs, $\rho_{\rm GW}$. So the calculation of the steerability of $\rho^E_{\rm GW}$ in the 2MS and 3MS is sometimes much more time-consuming and less precise. This is even the case for calculating the steerable weight and steering robustness using standard packages in the 2MS. For example, the calculations of these two steering measures for $\rho_{\rm GW}$ take at most a few seconds on a standard PC, while those for the generated $\rho^E_{\rm GW}$ require sometimes dozens of minutes assuming the same precision in both cases. These numerical problems grow very fast with the increasing number n of measurements.

Second problem.—Our experimental tuning of the parameters p and q for the GWSs is not fine enough, as explained in greater detail in Sec. 4.4.1. Note that the ranges of parameters p and q of the GWSs are very small such that a given GWS is steerable with $(n+1)$ measurements and unsteerable with n measurements for $n > 3$. Our experimental tuning of p and q was good enough to directly generate states in the regime #3 corresponding to $S_3 > 0$ and $S_2 = 0$. However, we were not able to *directly* generate experimentally GWSs belonging to different regimes of steerability for a larger number n. Note that even our experimental GWS in the regime #4, corresponding to $S_2 > 0$ and $B = 0$, was not generated directly. Indeed, we have obtained it in a hybrid way, i.e., by numerically mixing experimental states belonging to other regimes, as explained in Sec. 4.6.1.

Third problem.—It is numerically very challenging to check whether a given $\rho^E_{\rm GW}$ is n-measurement steerable and $(n-1)$-measurement unsteerable, which is crucial in experimentally demonstrating such a refined hierarchy of the steerability classes for multi-measurement scenarios. Specifically, if we numerically obtain $S_n(\rho^E_{\rm GW}) \sim 10^{-12}$, which is the precision of our numerical calculation of the steering measures, it is quite biased to decide whether this state $\rho^E_{\rm GW}$ is indeed steerable or not. With the increasing number n of measurements, the numerically estimated $S_n(\rho^E_{\rm GW})$ become less and less precise. So the question arises how to correctly classify the steerability of a given experimental state in the hierarchy of classes of steerability in various multi-measurement scenarios.

Fourth problem.—The border between the steerable and unsteerable theoretical GWSs is not precisely determined in the limit of an infinite number n of measurements on Alice's side. Indeed, the border corresponds to the region #7 in Fig. 4.8(a) spanned by the curves $p_S^{\rm low}$ and $p_S^{\rm up}$. Estimating $p_S^{\rm low}$ for our experimental imperfect GWSs, $\rho^E_{\rm GW}$, is even more demanding because $\rho^E_{\rm GW}$ usually exhibits a broken symmetry compared to that of the ideal GWSs $\rho_{\rm GW}$.

Thus, for these numerical and experimental reasons, we have decided to analyse in detail the steerability of our experimental states for the two simplest types of measurement scenarios only. We believe that this is good enough to show the hierarchy of some classes of correlations (including steerability in 2MS and 3MS) for experimental states.

C.5 Hierarchy of Entanglement Criteria

C.5.1 Hierarchy of the Shchukin-Vogel Entanglement Criteria

Here we briefly recall the Shchukin-Vogel entanglement criteria for the universal detection of distillable entanglement via the matrices of moments of the annihilation and creation operators [276]. This approach, in principle, does not require a full QST, so it is an alternative to the approach applied in our experiment using QST. We indicate some advantages and drawbacks of this approach for detecting two-qubit entanglement.

The Shchukin-Vogel criteria are based on the Hermitian matrices of moments for a given two-mode state ρ, which are defined as follows

$$\mathcal{M}_N^{\rm org} = \begin{bmatrix} M_{11} & M_{12} & ... & M_{1N} \\ M_{21} & M_{22} & ... & M_{2N} \\ ... & ... & ... & ... \\ M_{N1} & M_{N2} & ... & M_{NN} \end{bmatrix}, \tag{C11}$$

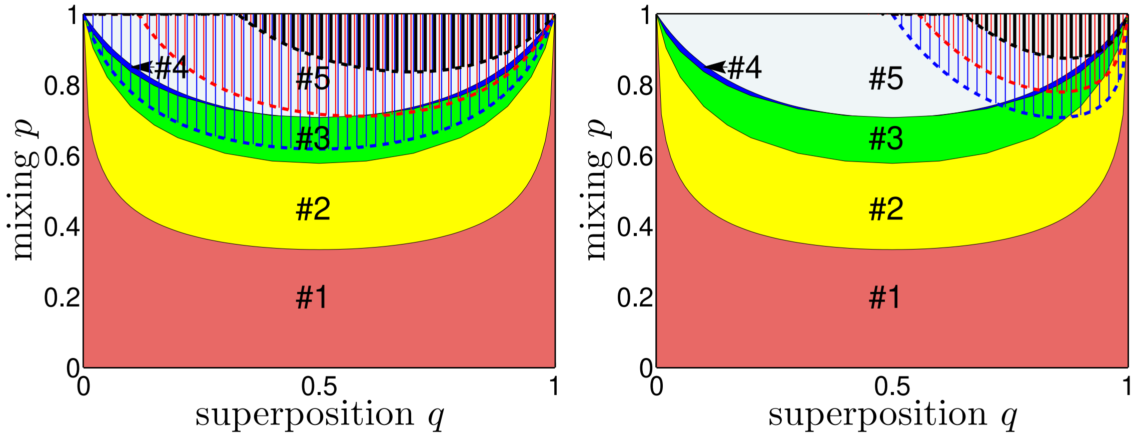
where $M_{ij} = \langle (a^{\dagger i_2} a^{i_1} b^{\dagger i_4} b^{i_3})(a^{\dagger j_1} a^{j_2} b^{\dagger j_3} b^{j_4})\rangle$ are the moments of the annihilation (a, b) and creation ($a^\dagger$, $b^\dagger$) operators of two modes of arbitrary dimension. Here i and j label multi-indices, e.g., (i_1, i_2, i_3, i_4). These moments can be detected experimentally (at least for not too high powers) using, e.g., the setup based on homodyne detection as described by Shchukin and Vogel [327]. A partially transposed matrix of moments can be obtained from $\mathcal{M}_N^{\rm org}$ as follows:

$$\begin{aligned} M_{ij}^\Gamma &= \langle (a^{\dagger i_2} a^{i_1} a^{\dagger j_1} a^{j_2})(b^{\dagger i_4} b^{i_3} b^{\dagger j_3} b^{j_4})\rangle^\Gamma \\ &= \langle (a^{\dagger i_2} a^{i_1} a^{\dagger j_1} a^{j_2})(b^{\dagger i_4} b^{i_3} b^{\dagger j_3} b^{j_4})^\dagger\rangle \\ &= \langle (a^{\dagger i_2} a^{i_1} a^{\dagger j_1} a^{j_2})(b^{\dagger j_4} b^{j_3} b^{\dagger i_3} b^{i_4})\rangle, \end{aligned} \tag{C12}$$

where the superscript Γ denotes partial transposition applied here for the second mode. This relation between $\mathcal{M}_N^{\rm org}$ and $\mathcal{M}_N^\Gamma$ is a key observation of Ref. [276]. Let $\mathcal{M}_{N,(r_1,r_2,\cdots,r_n)}$ denotes the $n\times n$ submatrix of $\mathcal{M}_N$ having $\mathcal{M}_{r_i,r_j}$ elements. The Shchukin-Vogel criteria are based on the following Sylvester's theorem [277]: $\mathcal{M}_N$ is *positive semidefinite* if and only if its all *principal minors* are nonnegative, i.e., $\det\{\mathcal{M}\}_{N,(r_1,r_2,\cdots,r_n)} \geq 0$. Thus, the Shchukin-Vogel criteria correspond to the positive partial transposition Peres-Horodecki criterion, but formulated in terms of the matrix moments as follows [276, 277]:

$$\begin{aligned} \rho \text{ is PPT} \quad &\Leftrightarrow \quad \forall N, \forall\{r_k\}: \quad \det\{\mathcal{M}\}^\Gamma_{N,(r_1,r_2,\cdots,r_n)} \geq 0, \\ \rho \text{ is NPT} \quad &\Leftrightarrow \quad \exists N, \exists\{r_k\}: \quad \det\{\mathcal{M}\}^\Gamma_{N,(r_1,r_2,\cdots,r_n)} < 0, \end{aligned} \tag{C13}$$

where $1 \leq r_1 < r_2 < \cdots < r_n \leq N$, $n = 1, 2, \cdots, N$, and PPT (NPT) stands for positive (nonpositive) under partial transposition. Many popular entanglement criteria can be derived from the Shchukin-Vogel criteria [276, 283], including the Hillery-Zubairy inequalities, which are below recalled and applied to the GWSs.



(a)

(b)

Figure 9: Hierarchy of criteria versus the CC hierarchy for the GWSs. Specifically, the criterion hierarchy is based on different nonuniversal witnesses for a given class of quantum correlation, while the CC hierarchy reveals different types of correlations determined by their measures or universal witnesses. This is shown here by the example of nonuniversal entanglement witnesses using the (a) first and (b) second HZ witnesses. The colour regions reveal the CC hierarchy, as in Fig. 4.6(a), while the areas filled with parallel lines show the criterion hierarchy. The latter areas determine the allowed values of the mixing parameter p and the superposition parameter q for the locally rotated GWSs, $\rho_\phi(p,q)$, for which entanglement can be revealed by the corresponding HZ witnesses: (a) $\bar{H}_1(\rho_\phi)$ for $\phi=\pi$ (area filled with blue lines), $\phi=0.8\pi$ (red-line area), and $\phi=0.7\pi$ (black-line area); and (b) $\bar{H}_2(\rho_\phi)$ for $\phi=$0 (blue-line-filled area), $\phi=0.2$ (red-line area), and $\phi=$0.3 (black-line-filled area). For $\phi=\pi/2$ neither of the HZ witnesses can detect the entanglement of the GWSs. The dashed curves are obtained from the analytical formulas in Eqs. (C22), (C25), (C28), and (C29).

C.5.2 Hierarchy of the Hillery-Zubairy Entanglement Criteria

The Hillery-Zubairy (HZ) entanglement criteria for nonuniversal detection of two-mode entanglement read as [328]:

$$H_1(\rho) \equiv \langle n_1 n_2\rangle - |\langle ab^\dagger\rangle|^2 < 0, \tag{C14}$$
$$H_1(\rho) \equiv \langle n_1\rangle\langle n_2\rangle - |\langle ab\rangle|^2 < 0, \tag{C15}$$

where $n_1 = a^\dagger a$ and $n_2 = b^\dagger b$. Thus, if $H_1(\rho) < 0$ or $H_2(\rho) < 0$ then ρ is entangled. The criteria are simple and useful witnesses of entanglement and have already been experimentally tested in a number of setups (see, e.g., [329]). These two criteria can be derived from the Shchukin-Vogel criteria by calculating

$$H_n(\rho) = \det\{\mathcal{M}\}_n^\Gamma \tag{C16}$$

for

$$\mathcal{M}_1^{\text{org}} = \begin{bmatrix} 1 & \langle ab\rangle \\ \langle a^\dagger b^\dagger\rangle & \langle n_1 n_2\rangle \end{bmatrix}, \mathcal{M}_1^\Gamma = \begin{bmatrix} 1 & \langle ab^\dagger\rangle \\ \langle a^\dagger b\rangle & \langle n_1 n_2\rangle \end{bmatrix} \tag{C17}$$

and

$$\mathcal{M}_2^{\text{org}} = \begin{bmatrix} \langle n_1\rangle & \langle a^\dagger b\rangle \\ \langle ab^\dagger\rangle & \langle n_2\rangle \end{bmatrix}, \mathcal{M}_2^\Gamma = \begin{bmatrix} \langle n_1\rangle & \langle a^\dagger b^\dagger\rangle \\ \langle ab\rangle & \langle n_2\rangle \end{bmatrix}, \tag{C18}$$

respectively. To analyse the HZ criteria on the same footing as the discussed measures of quantum correlations, one can redefine H_n to be the following HZ witnesses,

$$\bar{H}_n \;=\; \max\{0, -H_n\}\,. \tag{C19}$$

Let us now analyse in detail the hierarchy and effectiveness of these criteria in detecting the entanglement of the GWSs compared to the true measures of entanglement and other correlations.

We find the following HZ witnesses for the original GWSs:

$$\begin{aligned}\bar{H}_1(\rho_{\rm GW}) &= \max\left\{0, -\tfrac{1}{4}[1+p(3-4q)]\right\}=0, &\text{(C20)}\\ \bar{H}_2(\rho_{\rm GW}) &= \max\left\{0, p^2q\bar{q}-\tfrac{1}{4}(1+p-2pq)^2\right\}, &\text{(C21)}\end{aligned}$$

where $\bar{q}=1-q$. It can be seen that $\bar{H}_1(\rho_{\rm GW})$ is useless in detecting the entanglement of the GWSs; however, $\bar{H}_2(\rho_{\rm GW})$ can be nonzero. Thus, it detects entanglement for the GWSs corresponding to the blue-line-filled area in Fig. 9(a). The threshold (border) curve, as a function of the superposition parameter q in $\rho_{\rm GW}(p,q)$, corresponds to the smallest allowed values of the mixing parameter p, for which the entanglement of the GWSs can be detected. This threshold is shown by the blue dashed curve in this figure, and is given by

$$p_{H_2}(q) \;=\; 1/[2(q+\sqrt{q\bar{q}})-1], \tag{C22}$$

for $q\in[\frac{1}{2}, 1]$. Let us now apply the Pauli operator σ_1 (the NOT gate) to the second qubit in the GWS, which results in the state $\rho_X=(I\otimes\sigma_1)\rho_{\rm GW}(I\otimes\sigma_1)$. Note that any local unitary operation does not change entanglement measures, but of course it can change entanglement witnesses, which is the case for the HZ criteria. Indeed, this local transformation results in the following HZ witnesses:

$$\begin{aligned}\bar{H}_1(\rho_X) &= \max\left\{0, p^2q\bar{q}-\tfrac{1}{4}\bar{p}\right\}, &\text{(C23)}\\ \bar{H}_2(\rho_X) &= \max\left\{0, -\tfrac{1}{4}(1-p^2)-p^2q\bar{q}\right\}=0, &\text{(C24)}\end{aligned}$$

where $\bar{p}=1-p$. It is seen that the sensitivities of the HZ witnesses are exchanged for ρ_X compared to $\rho_{\rm GW}$. The second criterion cannot detect entanglement, while the first reveals entanglement of some GWSs corresponding to those shown in the blue-line-filled area in Fig. 9(b). Analogously to Eq. (C22), the threshold curve for the first HZ witness for $\rho_X(p,q)$ is given by

$$p_{H_1X}(q) \;=\; 2/[1+\sqrt{1+16q\bar{q}}], \tag{C25}$$

for $q\in[0, 1]$. Now let us apply an arbitrary rotation along the y-axis of the second qubit in the GWSs. Thus, we transform $\rho_{\rm GW}$ into $\rho_\phi=[I\otimes R_Y(\phi)]\rho_{\rm GW}[I\otimes R_Y^\dagger(\phi)]$, where the rotation is described by $R_Y(\phi)=[c, -s;\ s, c]$, with $c=\cos(\phi/2)$ and $s=\sin(\phi/2)$. The HZ witnesses for the locally rotated GWSs read:

$$\begin{aligned}\bar{H}_1(\rho_\phi) &= \max\left\{0, -\tfrac{1}{4}\big[c^2[1+p(3-4q)]\right.\\ &\qquad\left.+s^2(\bar{p}-4s^2p^2q\bar{q})\big]\right\}, &\text{(C26)}\\ \bar{H}_2(\rho_\phi) &= \max\left\{0, c^4p^2q\bar{q}-\tfrac{1}{4}f_+(c^2f_++s^2f_-)\right\}, &\text{(C27)}\end{aligned}$$

where $f_\pm=1\pm p(1-2q)$. The threshold curves for the HZ witnesses applied to $\rho_\phi(p,q)$ are given by

$$\begin{aligned}p_{H_1}(q, \phi) &= \left(f_1+\sqrt{f_1^2+2f_2}\right)f_2^{-1}, &\text{(C28)}\\ p_{H_2}(q, \phi) &= 2/[\sqrt{f}+2(1+C_1)q-C_1-1], &\text{(C29)}\end{aligned}$$

which are physically meaningful only in the regions of q for a given ϕ such that $p_{H_n}(q,\phi) \in [0,\ 1]$ $(n = 1,\ 2)$. Here $f = (1 - C_1)^2(1 - 2q)^2 + 2(4C_1 + C_2 + 3)q\bar{q}$, with $C_n = \cos(n\phi)$, $f_1 = c^2(3 - 4q) - s^2$, and $f_2 = 8q\bar{q}s^4$. As seen in Fig. 9, the lowest value of q for which the entanglement of the GWSs can be detected via the HZ witness $\bar{H}_1(\rho_\phi)$ $[\bar{H}_2(\rho_\phi)]$ is 0 $(\frac{1}{2})$ for $\phi = \pi$ $(\phi = 0)$. For both HZ witnesses, the largest allowed value of q is equal to 1.

Figure 9 shows a comparison of the two approaches to analyse a hierarchy of quantum correlations, i.e., the criterion hierarchy, which is based on the HZ witnesses, and the CC hierarchy, which is based on the discussed quantum correlation measures. Any good measure of entanglement results in the same CC hierarchy for the GWSs, while the criterion hierarchy depends on the applied nonuniversal witnesses and can reveal only a subset of the entangled GWSs, which correspond to the regimes #2–#5. This figure explains our motivation of experimentally demonstrating in detail only the CC hierarchy instead of the hierarchy based on the HZ witnesses, or using other either sufficient or necessary conditions of quantum correlations. Unfortunately, by contrast to such a hierarchy of criteria, it is experimentally challenging to reveal such a CC hierarchy for the GWSs *without* QST.

C.5.3 Quantum State Tomography via Moments of Annihilation and Creation Operators

Here we give an example showing that some very limited additional measurements on a given state can supplement a partial state reconstruction into a full QST.

We recall that a general single-mode density matrix ρ of a bosonic field can be reconstructed from the following moments of the annihilation and creation operators via the formula [330]:

$$\langle m_1|\rho|m_2\rangle = \sum_{j=0}^{\infty} \frac{1}{j!\sqrt{m_1!m_2!}} \langle (a^\dagger)^{m_2+j} a^{m_1+j} \rangle. \tag{C30}$$

Note that this formula can be divergent for some states of the radiation field including thermal field with the mean photon number $\langle n \rangle \geq 1$. However, for finite-dimensional states, the above sum becomes finite. In particular, a two-mode version of Eq. (C30) leads to the following moment-based representation:

$$\begin{bmatrix} f & \langle b^\dagger\rangle - \langle n_1 b^\dagger\rangle & \langle a^\dagger\rangle - \langle a^\dagger n_2\rangle & \langle a^\dagger b^\dagger\rangle \\ \langle b\rangle - \langle n_1 b\rangle & \langle n_2\rangle - \langle n_1 n_2\rangle & \langle a^\dagger b\rangle & \langle a^\dagger n_2\rangle \\ \langle a\rangle - \langle a n_2\rangle & \langle a b^\dagger\rangle & \langle n_1\rangle - \langle n_1 n_2\rangle & \langle n_1 b^\dagger\rangle \\ \langle ab\rangle & \langle a n_2\rangle & \langle n_1 b\rangle & \langle n_1 n_2\rangle \end{bmatrix} \tag{C31}$$

of a general two-qubit state ρ, where $f = 1 - \langle n_1\rangle - \langle n_2\rangle + \langle n_1 n_2\rangle$, and the annihilation operator $a = a_1$ (and analogously $b = a_2$) is simply $a = \sigma_- = [0,\ 1;\ 0,\ 0]$, i.e., the qubit lowering operator. Thus, an arbitrary two-qubit state can be completely reconstructed by measuring only the following moments: $\langle n_i\rangle$, $\langle n_1 n_2\rangle$, $\langle a_i\rangle$, $\langle n_i a_{2-i}\rangle$, $\langle a_1 a_2\rangle$, and $\langle a_1 a_2^\dagger\rangle$ for $i = 1, 2$.

Note that experimental implementations of the HZ witnesses require measuring $\langle n_i\rangle$, $\langle n_1 n_2\rangle$, $\langle a_1 a_2\rangle$, and $\langle a_1 a_2^\dagger\rangle$. Thus, by measuring additionally only the following moments $\langle a_i\rangle$ and $\langle n_i a_{2-i}\rangle$, one can collect all the information required for a complete QST, with which one can thus calculate any properties of an experimentally-reconstructed two-qubit state.

Appendix D
Co-Authors' Statements

Přírodovědecká
fakulta

Confirmation of Contribution

As the supervisor of Kateřina Jiráková and the co-author of her articles:

[1] Kateřina Jiráková, Karol Bartkiewicz, Antonín Černoch, and Karel Lemr, "Experimentally attacking quantum money schemes based on quantum retrieval games", Sci. Rep. **9**, 16318 (2019). `https://doi.org/10.1038/s41598-019-51953-9`

[2] Kateřina Jiráková, Artur Barasiński, Antonín Černoch, Karel Lemr, and Jan Soubusta, "Measuring Concurrence in Qubit Werner States Without an Aligned Reference Frame", Phys. Rev. Applied **16**, 054042, (2021). `https://doi.org/10.1103/PhysRevApplied.16.054042`

[3] Kateřina Jiráková, Antonín Černoch, Karel Lemr, Karol Bartkiewicz, and Adam Miranowicz, "Experimental hierarchy and optimal robustness of quantum correlations of two-qubit states with controllable white noise", Phys. Rev. A **104**, 062436, (2021). `https://link.aps.org/doi/10.1103/PhysRevA.104.062436`

I, Karel Lemr, hereby confirm that Mgr. Kateřina Jiráková contributed significantly to the scientific research presented in the above-listed publication. Her contributions included construction of the experimental setup, data analysis, creation of plots and writing the manuscript.

Olomouc, 7. ledna 2021

....
doc. Mgr. Karel Lemr, Ph.D.
Společná laboratoř optiky

Přírodovědecká
fakulta

Confirmation of Contribution

As the tutor of Kateřina Jiráková and the co-author of her articles:

[1] Kateřina Jiráková, Karol Bartkiewicz, Antonín Černoch, and Karel Lemr, "Experimentally attacking quantum money schemes based on quantum retrieval games", Sci. Rep. **9**, 16318 (2019). `https://doi.org/10.1038/s41598-019-51953-9`

[2] Kateřina Jiráková, Artur Barasiński, Antonín Černoch, Karel Lemr, and Jan Soubusta, "Measuring Concurrence in Qubit Werner States Without an Aligned Reference Frame", Phys. Rev. Applied **16**, 054042, (2021). `https://doi.org/10.1103/PhysRevApplied.16.054042`

[3] Kateřina Jiráková, Antonín Černoch, Karel Lemr, Karol Bartkiewicz, and Adam Miranowicz, "Experimental hierarchy and optimal robustness of quantum correlations of two-qubit states with controllable white noise", Phys. Rev. A **104**, 062436, (2021). `https://link.aps.org/doi/10.1103/PhysRevA.104.062436`

I, Antonín Černoch, hereby confirm that Mgr. Kateřina Jiráková contributed significantly to the scientific research presented in the above-listed publication. Her contributions included construction of the experimental setup, data analysis, creation of plots and writing the manuscript.

Olomouc, 7. ledna 2021 ....

Mgr. Antonín Černoch, Ph.D.
Společná laboratoř optiky

Confirmation of Contribution

As the co-author of Kateřina Jiráková's article:

[1] Kateřina Jiráková, Artur Barasiński, Antonín Černoch, Karel Lemr, and Jan Soubusta, "Measuring Concurrence in Qubit Werner States Without an Aligned Reference Frame", Phys. Rev. Applied **16**, 054042, (2021). `https://doi.org/10.1103/PhysRevApplied.16.054042`

I, Jan Soubusta, hereby confirm that Mgr. Kateřina Jiráková contributed significantly to the scientific research presented in the above-listed publication. Her contributions included construction of the experimental setup, data analysis, creation of plots and writing the manuscript.

Olomouc, 14th December 2021 ....

doc. Mgr. Jan Soubusta, Ph.D.
Joint Laboratory of Optics, UPOL

Confirmation of Contribution

As the co-author of Kateřina Jiráková's article:

[1] Kateřina Jiráková, Antonín Černoch, Karel Lemr, Karol Bartkiewicz, and Adam Miranowicz, "Experimental hierarchy and optimal robustness of quantum correlations of two-qubit states with controllable white noise", Phys. Rev. A **104**, 062436, (2021). `https://link.aps.org/doi/10.1103/PhysRevA.104.062436`

I, Adam Miranowicz, hereby confirm that Mgr. Kateřina Jiráková contributed significantly to the scientific research presented in the above-listed publication. Her contributions included construction of the experimental setup, data analysis, creation of plots and writing the manuscript.

Poznań, 22th December 2021

A. Miranowicz

....

prof. dr hab. Adam Miranowicz
Faculty of Physics
Adam Mickiewicz University

Confirmation of Contribution

As the co-author of Kateřina Jiráková's article:

[1] Kateřina Jiráková, Karol Bartkiewicz, Antonín Černoch, and Karel Lemr, "Experimentally attacking quantum money schemes based on quantum retrieval games", Sci. Rep. **9**, 16318 (2019). `https://doi.org/10.1038/s41598-019-51953-9`

[2] Kateřina Jiráková, Antonín Černoch, Karel Lemr, Karol Bartkiewicz, and Adam Miranowicz, "Experimental hierarchy and optimal robustness of quantum correlations of two-qubit states with controllable white noise", Phys. Rev. A **104**, 062436, (2021). `https://link.aps.org/doi/10.1103/PhysRevA.104.062436`

I, Karol Bartkiewicz, hereby confirm that Mgr. Kateřina Jiráková contributed significantly to the scientific research presented in the above-listed publication. Her contributions included construction of the experimental setup, data analysis, creation of plots and writing the manuscript.

Poznań, 22th December 2021

Karol Bartkiewicz ....

Dr hab. Karol Bartkiewicz, prof. UAM
Faculty of Physics
Adam Mickiewicz University

Appendix E Contents of Enclosed CD-ROM

- folder data_Concurence_WS:
  - folder Maps:
    - Mapa4_GHZ03_35deg.dat
    - Mapa4_GHZ03_45deg.dat
    - Mapa4_SEP03_2_000.dat
    - Mapa4_SEP03_3_001.dat
    - Mapa4_SEP03_4_010.dat
    - Mapa4_SEP03_5_011.dat
    - Mapa4_SEP03_6_100.dat
    - Mapa4_SEP03_7_101.dat
    - Mapa4_SEP03_8_110.dat
    - Mapa4_SEP03_9_111.dat
    - README_map.txt
  - folder Tomography:
    - README_Tom.txt
    - tom200114a_GHZ45deg.dat
    - tom200114a_GHZ45deg.mat
    - tom200221a_GHZ35deg.dat
    - tom200221a_GHZ35deg.mat
- folder data_hierarchy_QCorrelations:
  - folder GWS_densityMat_data:
    - GWS_densityMat_p_0_15.mat
    - GWS_densityMat_p_0_4.mat
    - GWS_densityMat_p_0_6.mat
    - GWS_densityMat_p_0_8.mat
    - GWS_densityMat_p_0_9.mat
    - GWS_densityMat_p_1_b1.mat
    - GWS_densityMat_p_1.mat
  - folder GWS_RAW_data:
    - GSW_RAW_p_0_6.dat
    - GWS_RAW_p_0_15.dat

    - GWS_RAW_p_0_4.dat
    - GWS_RAW_p_0_8.dat
    - GWS_RAW_p_0_9.dat
    - GWS_RAW_p_1_b1.dat
    - GWS_RAW_p_1.dat
    - README.txt
  - folder WS_densityMat_data:
    - WS_densityMat_p_0_15.mat
    - WS_densityMat_p_0_333.mat
    - WS_densityMat_p_0_5.mat
    - WS_densityMat_p_0_577.mat
    - WS_densityMat_p_0_6.mat
    - WS_densityMat_p_0_65.mat
    - WS_densityMat_p_0_707.mat
    - WS_densityMat_p_0_73.mat
    - WS_densityMat_p_0_8.mat
    - WS_densityMat_p_0_9.mat
    - WS_densityMat_p_1.mat
  - folder WS_RAW_data:
    - README.txt
    - WS_RAW_p_0_15.dat
    - WS_RAW_p_0_333.dat
    - WS_RAW_p_0_5.dat
    - WS_RAW_p_0_577.dat
    - WS_RAW_p_0_6.dat
    - WS_RAW_p_0_65.dat
    - WS_RAW_p_0_707.dat
    - WS_RAW_p_0_73.dat
    - WS_RAW_p_0_8.dat
    - WS_RAW_p_0_9.dat
    - WS_RAW_p_1.dat

- folder data_Quantum_Money:
  - clones171121aDx.dat
  - clones171121bDo.dat
  - clones171121cAx.dat
  - clones171121dAo.dat
  - clones171121eRx.dat
  - clones171121fRo.dat
  - clones171121gLo.dat
  - clones171121hLx.dat
  - dip171010d.dat

- jirakovaK_doctoral_thesis.pdf