Přírodovědecká fakulta Univerzity Palackého
v Olomouci

Společná laboratoř optiky

Návrh a konstrukce lineárně-optických zařízení pro kvantovou komunikaci

diplomová práce

Marek Bula

vedoucí práce:
Mgr. Karel Lemr, Ph.D.

Olomouc duben 2016

Faculty of Science, Palacký University
in Olomouc

Joint Laboratory of Optics

Design and construction of linear-optical devices for quantum communications

master's thesis

Marek Bula

supervisor:
Mgr. Karel Lemr, Ph.D.

Olomouc April 2016

Bibliographic details

Title	Design and construction of linear-optical devices for quantum communications
Nadpis	Návrh a konstrukce lineárně-optických zařízení pro kvantovou komunikaci
Type	master's thesis
Author	Marek Bula
Supervisor	Mgr. Karel Lemr, Ph.D.
University	Palacký University in Olomouc
Study program	N1701 Physics, 1701T029 Optics and Optoelectronics
Department	Joint Laboratory of Optics
Language	English
Year	2016
Pages	75
Available at	`http://portal.upol.cz`

Declaration of originality

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

Olomouc, ..., 2016 ....

Submitted ...., 2016

The author grants permission to Palacký University in Olomouc to store and display this thesis and its electronic version in university library and on official website.

Acknowledgement

I wish to express my sincere gratitude to my supervisor Mgr. Karel Lemr, Ph.D., for patient guidance and to Mgr. Antonín Černoch, Ph.D., and doc. Mgr. Jan Soubusta, Ph.D., for irreplaceable help in the laboratory. My thanks also belong to co-authors of our publications (in alphabetical order) Karol Bartkiewicz, Thomas Jennewein and Evan Meyer-Scott.

I am most thankful to my family and closer friends for empathic listening and decongesting jokes.

Contents

Chapter 1

Introduction

1.1 Motivation and fundamental description

Communication technologies are a natural part of our lifes today. We have more demands on their capabilities every day. For example, Internet was used by 3 366 261 156 people by 30.11.2015 [1] and every day, people post 144.8 $\cdot 10^9$ emails and upload 72 hours of video to Youtube per minute. Humanity with its technologies produce $2.5 \cdot 10^{19}$ bytes every day. The fact that 90% of the world amount of data is created over last 2 years highlights its importance for future [2]. It is thus not surprising that the developing methods for secure and effective transmission of information is one of the most investigated research topic. Many branches of natural sciences focus on research related to communication technologies, e.g. informatics, material research, electronics. Scientists ask questions like how to process, how to encode, how to transfer,... the information in an efficient way. Classical physics based approach is well known and we are using it every day in our computers, mobile phones when we want to know something about weather or how are our friends.

Currently, one of the most promising ways of research relies on quantum physics. The cornerstone of this discipline was founded by Max Planck at turn of the 19. and 20. century. He assumed that the light is emited in little non-continuous quanta, proportional to its frequency [3]. Over the next thirty years, Einstein, Bohr, Schrödinger, Heisenberg, and others participated on the birth of this revolutionary and also controversial theory of quantum mechanics.

Quatum computation is one of the possible application of the quantum theory. Quantum computer had been already defined by D. Deutsch in 1985 [4]. Today, field of quantum information processing (QIP) is still a quickly developing scientific discipline. It promises safer distribution of the cryptographic key [5], faster solving of some informatics algorithms [6], more efficient data storage [7] and more. For instance, a classical computer processes information stored in bits, systems with two logical values denoted 0 and 1. In contrast to that, a quantum bit (qubit) used in QIP benefits from the principle of superposition. Apart from the logical states 0 and 1, a qubit admits any form of

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $|\psi\rangle$ denotes the qubit state and α, β are complex numbers bound by condition $|\alpha|^2 + |\beta|^2 = 1$. In fact, $|\alpha|^2$ represents the probability of observing logical state $|0\rangle$ and similary, $|\beta|^2$ represents the probability of observing logical state $|1\rangle$.

Another interesting property of quantum states lies in nonlocal quantum corellations (also called entanglement) [8]. Effect of the measurement on one particle from the entangled pair instantly causes some changes on the other particle across any distances [9]. It allows us to implement same usefull and non classical protocols, such as quantum teleportation [10].

On the other hand, scientists have to deal with various technical and fundamental limits imposed by quantum–physical laws. For example, upon measurement, the quantum superposition callapses and only one bit is extracted from one qubit. Also, on some platforms, such as the linear optics, some quantum–information protocols can be implemented only probabilistically. It is an obvious issue for their practical use [11].

Some technologies, like quantum cryptography, have already found their application in real life [12]. Laws of nature determine that clasiccal cryptography can not prevent eavesdropping and its safety depends on computational difficulty, i.e. if an attacker captures encryted data, he needs unacceptable amount of time for decoding by classical way. In quantum cryptography, an attacker is revealed, because any disturbance introduces some detectable noise. Attackers can not receive data coded in quantum states, copy it for themself and forward it over the line as like nothing has happened, because unknown quantum states can not be perfectly cloned [13]. The quantum cryptography protocolas are designed to reveal the attacker during exchange of the random key (before the actual secret data is sent). So when an attacker is discovered, the communication is simply cancelled.

As mentioned above, classical cryptography uses difficulty in decoding as an instrument for protection against eavesdropping. It can be based on factorization of large integers, as shown by R. Rivest, A. Shamir a L. Adleman in RAS cryptographic code [14]. It relies on the fact that computing time is growing exponentionaly with size of factorized integers. Thus, enough large integers suffice to provide safety against attackers with a classical computer. However, beware of those, who have a quantum computer! P. W. Shor has found a quantum algorithm for factorization of integers based on the quantum Fourier transform [6]. It spreads an integer into a factor of two prime numbers with time demands growing polynomialy on the size of the original integer. Principle of superposition, the benefit of qubits, allows this algorithm to operate faster then any known classical algorithm [15].

Chapter 2

Methods and Tools

2.1 Field quantization

We need to define some mathematical apparatus to conviniently and sufficiently describe quantum protocols. In this section we present a brief, simplified approach, for a more details, see [16]. First steps in formulation of this concept were achieved by Werner Heisenberg, Max Born and Pascual Jordan, who presented a seminal article in 1925 [17] in which they discuss elementary principles of quantization of electromagnetic field. Over time their ideas matured into a well developed theory known as the canonical quantization. Let us to introduce the principal ideas.

In the above mentioned paper, the authors write about the fundamental law in quantum mechanics. It is the relationship between generalized coordinate x and conjugated generalized momentum p

$$x_i p_j - p_j x_i = \frac{ih}{2\pi}\delta_{ij}, \tag{2.1}$$

where h is the Planck constant and δ is the Kronecker delta. The equation is the so-called “commutation relation” and we write down it as

$$[x, p] = i\hbar\delta_{ij},$$

where $\hbar = \frac{h}{2\pi}$ is the normalised Planck constant. It seems to be harmless and simple formula, but it is really respectable: “The commutation law stores information on the discontinuity, the non-commutativity, the uncertainty, and the complexity of the quantum world.” [18]

Classical mechanics allows us to express energy H (called Hamiltonian) of j independent oscillators as a function of their generalized coordinates

$$H = \sum_j \frac{1}{2} \left(P_j^2 + \omega_j^2 X_j^2 \right),$$

where ω_j is angular frequency of the jth oscillator, and X_j,P_j are rescaled x_j,p_j

$$X_j = \sqrt{\frac{2\hbar}{\omega}}\, x_j,$$
$$P_j = \sqrt{2\hbar\omega}\, p_j.$$

We can imagine, that the electromagnetic field also consists of independent one–dimensional linear harmonic oscilators [19]. This idea allows us to describe the electromagnectic field using the same Hamiltonian as for mechanical oscilators. Simultaneously, for a quantum–mechanical description we replace the Hamiltonian and generalized coordinates by their operator counterparts

$$\hat{H} = \sum_j \frac{1}{2} \left(\hat{P}_j^2 + \omega_j^2 \hat{X}_j^2 \right). \tag{2.2}$$

At this point we can analyse the field Hamiltonian and find its eigenstates (energy levels). For this purpose, a raising and a lowering operators were introduced [20]. The raising (creation) operator is

$$\hat{a}_j^\dagger = \hat{x_j} + i\hat{p_j}$$

and (lowering) anihilation operator

$$\hat{a}_j = \hat{x_j} - i\hat{p_j}.$$

Commutation relation of these operators is

$$[\hat{a}, \hat{a}^\dagger] = 1.$$

If we substitute these operators in (2.2), we obtain an important form of the Hamiltonian operator for one mode of the electromagnetic field

$$\hat{H} = \frac{\omega}{2} \left(\hat{a}\hat{a}^\dagger - \hat{a}^\dagger\hat{a} \right) = \omega \left(\hat{a}^\dagger\hat{a} + \frac{1}{2} \right) = \omega \left(\hat{N} + \frac{1}{2} \right).$$

There is the term $\frac{1}{2}$, that follows from non–zero energy of the vaccum and the number operator $\hat{N}$, which has the same eigenstates as the Hamiltonian operator. These eigenstates form orthogonal basis and are very usefull. They are called Fock states and their ingenvalues represent the number of photons in a certain mode. So, aplication of $\hat{N}$ on the Fock state $|n_j\rangle$ gives the mentioned number of photons n_j

$$\hat{N}|n_j\rangle = n_j|n_j\rangle,$$

where $n = 0, 1, 2, \dots$ [20].

At this moment, we are gonig to show the importance of anihilation and creation operators applied on the Fock states $|n_j\rangle$. The anihilation operator decreases the number of photons by one

$$\hat{a}_j|n_j\rangle = \sqrt{n_j}|\left(n_j - 1\right)\rangle.$$

Symmetrically, the creation operator increases it by one

$$\hat{a}_j^{\dagger}|n_j\rangle = \sqrt{n_j + 1}|\left(n_j + 1\right)\rangle.$$

These two operatos allow us to describe the operation of quantum protocols in this thesis.

2.2 Qubit

As we have mentioned above, qubits are significant ingredient in QIP, but they are only a theoretical model, which needs real physical implementation. In our investigations, we use photons to encode qubits, because the most of elementary experiments can be implemented by quite simple linear-optical elements [21]. Also, light is a very promising platform for modern communications [22].

However, many other physical objects can implement a qubit. For example atomic ensembles [23], quantum dots [24] and Josephson junctions [25] can serve as media for qubits. Only the choice of how to encode the qubit is the main difference between them. For a nucleus we are able to measure its spin up and down. A photon provides us more options like polarization state, number of photons and time of arrival. All these physical platforms fulfill quantum–mechanical laws and are suitable for some QIP tasks, while inconvenient for other. Some allow to design sophisticated quantum processors, while other are suitable for transmission of quantum information [26, 27].

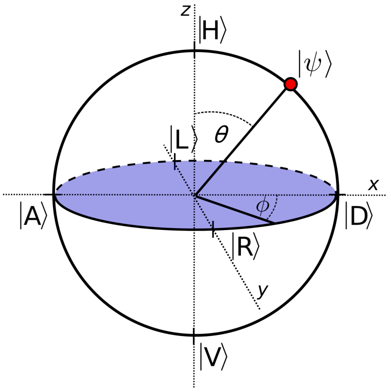


Figure 2.1: The Bloch sphere, where usualy the horizontal polarization state $|H\rangle$, respectively vertical polarization state $|V\rangle$ is encoded as logical state $|0\rangle$, respectively $|1\rangle$.

We have discussed the principle of superposition in Eq. (1.1), where α, β are complex numbers. These complex numbers are composed of two real variables, four degrees of freedom in total. However, one degree is eliminated by normalization and a second is a total phase of the system, which can be factored out. For simplicity, we note a qubit by 2 angles, that geometricaly constitute a sphere called the Bloch sphere:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{2.3}$$

where θ indicates ratio between $|1\rangle$ and $|0\rangle$ using trigonimetrical functions and ϕ is the phase between them, depicted on he Fig.2.1. For any given pair of real numbers θ and ϕ, we can constitute a qubit state and visualized it on the Bloch sphere, that is convinient for encoding into polarization state of a photon. We usually choose horizontal and vertical states as the basis states. The horizontal polarization state $|H\rangle$ usually represents a logical state $|0\rangle$ and the vertical polarization state $|V\rangle$ usually represents a logical state $|1\rangle$. Also other frequently used polarization states belong to this sphere, as diagonal $|D\rangle$ and antidiagonal $|A\rangle$ polarization, left–handed $|L\rangle$ and right–handed $|R\rangle$ circular polarizations. So it is a really suitable concept for the polarization encoding. However, there are cases requiring other degrees of freedom of photons beside polarization. For instance, quantum–optics protocols, that are carried out using optical fibers, routinely use spatial encoding (dual–rail encoding) [28], because commonly avaible fibers do not maintain polarization.

Apart from a single qubit, multi-qubit states are also immportant. Generally, if we work with n qubits, corresponding state has 2^n dimensional basis, it is made of superpositon of 2^n logical states, i.e. for two qubits we get:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{01}|01\rangle + \alpha_{01}|01\rangle.$$

The normalization condition $\sum_{m,n} a_{m,n} = 1$ is still valid and α coefficients have the same meanig as coefficients from Eq. (2.3). Worth mentioning are the Bell states:

$$\begin{aligned}
|\Phi^{+}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
|\Phi^{-}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
|\Psi^{+}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\
|\Psi^{-}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \qquad (2.4)
\end{aligned}$$

These states manifest correlation known as quantum entaglement, which is stronger than any classical correlation. We can see, that state of the second photon will correlate or anti–correlate with the result of probabilistic measurement on the first photon. This effect can be observed in any measurement basis.

2.3 Logical gates

Quantum computers store information in qubit states. Unitary evolutions of these states perform computations in this computer. We have introduced two significant quantum–mechanical capabilities used in a quantum computer: the entanglement and the principle of superposition. Let to describe also quantum interference [11].

We can observe the phenomenon of quantum interference in simple interferometer, for instance in a Mach–Zehnder interferometer (MZI), that is described later in this chapter in subsection “Tools in the laboratory” [29]. There, one photon can interfere with itself owing to indistinguishability of

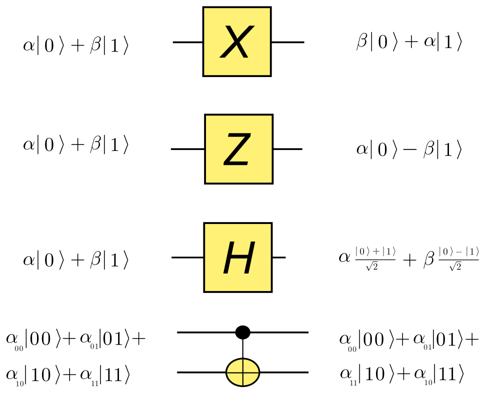

$\alpha|0\rangle + \beta|1\rangle$
X
$\beta|0\rangle + \alpha|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$
Z
$\alpha|0\rangle - \beta|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$
H
$\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
$\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+$
$\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$
$\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+$
$\alpha_{11}|10\rangle+\alpha_{10}|11\rangle$

Figure 2.2: There are several main logical qubit gates. Pauli–X, Pauli–Z and Hadamard (H) are single qubit gates, the last is a C–NOT, which is a two qubit gate.

which path it has traveled. Thus, photon was present in both arms of the interferometer simultaneously. Pay attention, when we try to measure where it was, it will show only in one arm of the interferometer losing the superposition of being in both arms [11].

In the following subsection, we show how a qubit is processed in some qubit gates, that are elementary circuits of a quantum computer. Some quantum logical gates can perform same operations as a classical computer, others operate in a purely quantum way, as we can see below and on the Fig. 2.2

The NOT gate

The quatum NOT gate is an elementary single qubit gate and it has a similiar counterpart of a classical bit. After a qubit passes through this gate, logical basis 1 and 0 are interchanged. It is also called Pauli-X gate and labeled $\hat{X}$[1], see Fig. 2.2. It can be nicely described by a matrix formalism. If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is noted in a vector (the so–called computation basis)

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

[1] Not to be consufed, it is labeled same as position operator

the NOT gate acts in this way

$$\hat{X}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ \alpha\end{pmatrix}.$$

It is obvious, that $\hat{X}$ is defined by a square matrix

$$\hat{X}\equiv\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Pauli-Y, Z gates and Hadamard gates

Let us consider, we have a qubit state visualised on the Bloch sphere as mentioned above. The Pauli-Y gate ($\hat{Y}$) rotates a quantum state around the *y–axis* on the Bloch sphere by 180°. The Pauli-Z gate works in the same way, but around the *z–axis*. The Hadamard gate is one of the most useful gates, it rotates a quantum state about the *x–axis* by 180°and about the *y–axis* by 90°. All of them can be expressed in matrix formalism in computation basis

$$Y\equiv\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, Z\equiv\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ H\equiv\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.$$

These gates work on superpositions of $|0\rangle$ and $|1\rangle$ as well, thus they do not have complete equivalents in a classical computer.

The $\hat{C}_{NOT}$ gate

The controlled NOT ($\hat{C}_{NOT}$) gate has two qubits at the input. First is a control qubit, second is a target qubit. Simply explained, if the control qubit is in logical state $|1\rangle$, than the target qubit will undergo a $\hat{X}$ gate.

$$\hat{C}_{NOT}\equiv\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}.$$

Interestingly, any quantum circuit can be implemented by repetition of a general controlled–unitary gate [30]. Alternatively, a quantum circuit can be built using combination of single qubit gates with $\hat{C}_{NOT}$ gates [31].

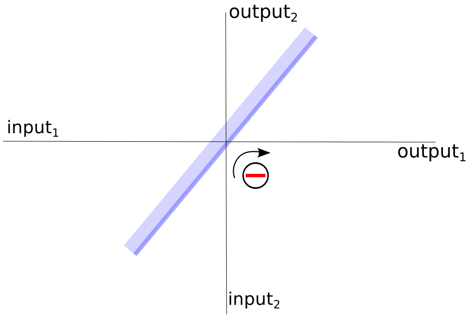


Figure 2.3: Schematic drawing of a beam splitter.

2.4 Tools in the laboratory

On the platform of linear–optics, the above mentioned gates can be implemented using various linear–optics components. In the following subsection, we will discuss these components, which are used in the proposals for realisation of our ideas presented in this thesis.

2.4.1 Beam splitter

Beam splitter (BS) represents operation of most of a linear–optics devices. It is realized either by a semitransparent glass plate or a fiber coupler. It transforms two inputs into a two outputs according to an equation for annihilation operators

$$\begin{pmatrix} \hat{a}_{out1} \\ \hat{a}_{out2} \end{pmatrix} = \begin{pmatrix} \sqrt{T} & -\sqrt{R} \\ \sqrt{R} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_{in1} \\ \hat{a}_{in2} \end{pmatrix}, \tag{2.5}$$

where T and R represent intensity transmissivity and reflectivity of the beam splitter. We introduce term “splitting ratio”, that is ratio between $T : R$. Sign minus in the tranformation matrix represents the phase flip of the signal in one of BS outputs, that is illustrated on Fig. 2.3. We expect validity of energy conservation law, thus $T + R = 1$ for an ideal BS. It brings to mind a quite similar equation of a trigonometric functions cosine and sine $\cos^2\vartheta + \sin^2\vartheta = 1$. This offers a substitution $T = \cos^2\vartheta$, $R = \sin^2\vartheta$ that allows us to use only one parameter ϑ for description of the BS.

When two indistinguishable photons impinge on separate input ports of a BS with splitting ratio $50 : 50$, then we can not observe photons in both outputs in any case. This phenomenon is called bunching and it is a cornerstone of linear–optical QIP [32].

2.4.2 Polarization dependent beam splitter

If different splitting for different polarizations is required, we use a polarization dependent beam splitter. It differs from the ordinary BS by independent splitting ratios for two orthogonal polarizations. We expect a four different modes both at output and input, thus Eq. (2.5) extends to

$$\begin{pmatrix} \hat{a}_{H,out1} \\ \hat{a}_{V,out1} \\ \hat{a}_{H,out2} \\ \hat{a}_{V,out2} \end{pmatrix} = \begin{pmatrix} \sqrt{T_H} & 0 & -\sqrt{R_H} & 0 \\ 0 & \sqrt{T_V} & 0 & -\sqrt{R_V} \\ \sqrt{R_H} & 0 & \sqrt{T_H} & 0 \\ 0 & \sqrt{R_V} & 0 & \sqrt{T_V} \end{pmatrix} \begin{pmatrix} \hat{a}_{H,in1} \\ \hat{a}_{V,in1} \\ \hat{a}_{H,in2} \\ \hat{a}_{V,in2} \end{pmatrix}, \tag{2.6}$$

where H is horizontal polarization and V is vertical polarization.

2.4.3 Wave plates

Wave plates are linear–optical components with two orthogonal axis, “fast and slow”, introducing phase shift between orthogonal polarizations by introducing temporal delay. The half–wave plate shifts one polarization against the other by half of the wavelength. It is described by tranformation of annihilation operators

$$\begin{pmatrix} \hat{a}_{H,out} \\ \hat{a}_{V,out} \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \begin{pmatrix} \hat{a}_{H,in} \\ \hat{a}_{V,in} \end{pmatrix} \tag{2.7}$$

with lower indexes H, V denoting horizontal and vertical polarizations. The parameter α represents angle between the horizontal direction and the fast optical axis of the half–wave plate.

Likewise, a quater–wave plate introduces shift between orthogonal polarizations by a quater of wavelength, described by slightly differented transformation

$$\begin{pmatrix} \hat{a}_{H,out} \\ \hat{a}_{V,out} \end{pmatrix} = e^{\frac{i\pi}{4}} \begin{pmatrix} \cos^2\alpha + i\sin^2\alpha & (1-i)\sin\alpha\cos\alpha \\ (1-i)\sin\alpha\cos\alpha & \sin^2\alpha + i\cos^2\alpha \end{pmatrix} \begin{pmatrix} \hat{a}_{H,in} \\ \hat{a}_{V,in} \end{pmatrix}. \qquad (2.8)$$

An arbitrary polarization can be transformed to another arbitrary polarization by three rotatable wave plates, two quater–wave plates and one half–wave plate [33].

2.4.4 Neutral density filter

In the experimental reality, we may need to scale down intensity of a beam in a certain part of an experimental setup. It could be realized by a neutral density filter that acts on an annihilation operator

$$\hat{a}_{out} = \sqrt{T}\hat{a}_{in},$$

where T is transmisivity that depends on the absorption by the filter. Note that this non–unitary transformation is the effective segment of a unitary transformation involving mixing of the signal mode with a vacuum ancillary mode on a beam splitter.

2.4.5 Single photon detectors

The photon–number–resolving detector with enough good efficiency is a quite complicated device and not necessary for our purposes. The binary photon detector is sufficient instead. It gives a detection event that can described by two POVMs

$$\hat{\Pi}_{NOCLICK} = \sum_{n=0}^{\infty}(1-\eta)^n|n\rangle\langle n|,$$

$$\hat{\Pi}_{CLICK} = \hat{1\!\!1} - \hat{\Pi}_{NOCLICK},$$

where η is the detector quantum efficiency and n represents Fock state number. These detectors has quantum efficiency about 60% and they are based on APD (avalanche photo-diodes) detectors.

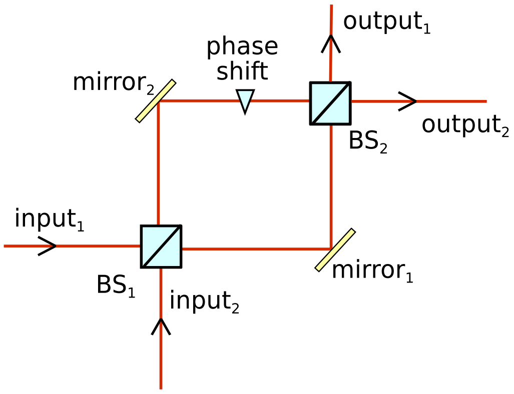


Figure 2.4: Mach–Zehnder interferometer consists of two beam splitters BS_1 and BS_2 and of two mirrors.

2.4.6 The Mach–Zehnder interferometer

Heart of each proposal in this thesis is the Mach–Zehnder interferometer (MZI), so called "two path interferometr" invented by L. Zehnder and L. Mach in 1891 [34]. It is a versatile device used also in commercial sector, for example in spectroscopy, in measuring of surface quality or in aerodynamics [29].

It consists of two inputs, two beam spliters, two mirrors or another reflective components and two outputs. The primary advantage of MZI are two spatially separated arms, where in one of them phase shift is inserted (see Fig. 2.4). It allows to choose between destructive and constructive interference at one of the outputs by using this phase shift. Quality of interference is usualy expresed in term of visibility V, unitless quantity denoted

$$V = \frac{I_{MAX} - I_{MIN}}{I_{MAX} + I_{MIN}},$$

where I_{MAX} is maximum measured intensity and I_{MIN} is minimum measured intensity, both are measured at one output as function of the phase shift. Visibility takes values between 0, that denotes no interference, and 1, that denotes full interference [33].

Chapter 3

Linear–optical qubit amplifier

3.1 Introduction

In classical communications data needs to be transfered over long distances. However, transmision is bound by losses occuring in the communications channel. This fundamental issue is circumvented by amplifiers, devices that take input signal, increase its amplitude and resend it with the encoded information preserved. This is possible with classical signal because principles of electronics allow to generate exactly same signal as received.

It seems that transferring data by optical networks is a realy promising way. Optical transmission channels are bound by losses as well [22], which leads to the necessity of having an optical amplifier. Classical communication focuses on amplifying a strong signal, that means not single photons [22]. Whereas in quantum information we need to amplify single photons.

For instance, test of Bell inequalities across long distances includes detection of entangled pairs of photons. When one photon of such photon pair is absorbed by transmission channel, entangled pair will not be detected, measurement will fail. The suitable amplifier seems to be a really helpful device for solving this task [35].

It would be nice if we could amplify a quantum system, photon state in "measure and resend" manner, e.g. take information carrier and exactly copy it with preserving its quantum state. Unfortunately, quantum mechanics prohibits exact cloning of quantum state [13] and we have to pay for cloning by adding noise. Classical amplification increases number of carriers, so increases signal intensity. It can be realized also in quantum manner, but necessarily with increased noise [36, 37].

Quantum principles give another point of view on amplification that circumvents adding noise. It can be realised by suppression of vacuum in the desired state. This manner of amplification is quite similar to "filtering", thus without adding noise. The concept of amplification without adding noise was proposed by T. C. Ralph and A. P. Lund in 2008 [38]. Soon, experimental realisation appeared [39–41]. It seems it is an ideal amplifier, nevertheless it operates only probabilistically. This disadvantage is often circumvented by post–selection on coincidence counts that give us information "it worked right". Such device is the so–called "heralded noiseless photon amplifier".

However, quantum information is coded into qubits. Thus, we require amplification to preserve the qubit state encoded into a photon. Let us consider a superposition of vacuum and qubit state $|\psi\rangle$

$$\alpha|0\rangle + \beta|\psi\rangle,$$

where $|\alpha|^2$ is probability of vacuum presence and $|\beta|^2$ is probability of presence of the state $|\psi\rangle$, both bound by normalization condition $|\alpha|^2 + |\beta|^2 = 1$. We introduce amplification on the state $|\psi\rangle$ described by gain G

$$\frac{1}{N}\left(\alpha|0\rangle + G\beta|\psi\rangle\right),$$

with $N = \sqrt{\alpha^2 + G^2\beta^2}$ as the normalisation condition and G as a real number always larger than 1. It is obvious that probability of presence of the state $|\psi\rangle$ is larger than before amplification. Such device was proposed by N. Gisin *et al.* [42] and experimentaly realised by C. Kocsis [43].

Heralded qubit amplifiers are primary important for secure transfer of key in quantum cryptography, specifically in the case of device–independent quantum key distribution (DIQKD) [44, 45]. This type of amplifier closes the detection loophole that DIQKD is suffering from.

We have proposed the heralded qubit amplifier that outperforms the other published heralded qubit amplifiers [42, 46, 47]. Success probability of our amplifier does not go to the zero in contrast to Gisin *et al.* [42] in the case when gain goes to infinity.

Our proposed device has tuneable gain. In the case of the infinite gain it works similary as scheme proposed by Curty and Moroder [47] that can work

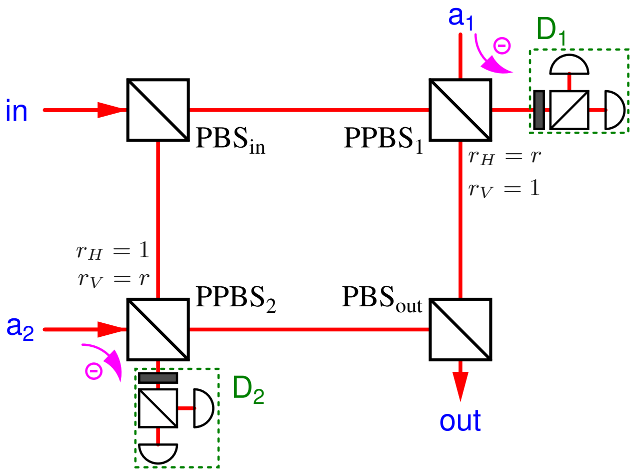


Figure 3.1: Scheme for entanglement-based linear-optical qubit amplifier as described in the text. D_1 and D_2 are standard polarization analysis detection blocks (for reference see [49]).

only in this regime. We outperforms Pitkanen *et al.* proposal [46], because they require photon–number–resolving detectors and our device needs only binary detectors in the infinite gain regime.

Moreover, we also investigated more general purpose of our scheme, which can be used for a weak measurement and presence detection of a photon.

3.2 Principle of operation of our qubit amplifier

Text adopted from: Evan Meyer–Scott, Marek Bula, Karol Bartkiewicz, Antonín Černoch, Jan Soubusta, Thomas Jennewein, and Karel Lemr. Entanglement–based linear–optical qubit amplifier. Phys. Rev. A, 88:012327, Jul 2013. [48].

The amplifier (depicted in Fig. 3.1) consists of four polarizing beam splitters. Two of them (PBS_{in} and PBS_{out}) form a Mach-Zehnder interferometer between signal input port "in" and output port "out". These polarizing beam splitters totally transmit horizontally polarized light while totally reflect light with vertical polarization. The other two are partially-polarizing beam splitters, denoted as PPBS_1 and PPBS_2, and placed in their respective arms of the interferometer. PPBS_1 reflects vertically polarized light, while having reflectivity r for horizontal polarization. In terms of creation operators this transformation reads

$$\begin{array}{rcl}\hat{a}^\dagger_{\rm in,H} & \rightarrow & r\hat{a}^\dagger_{\rm out,H} + \sqrt{1-r^2}\hat{a}^\dagger_{\rm D1,H},\\ \hat{a}^\dagger_{\rm a1,H} & \rightarrow & -r\hat{a}^\dagger_{\rm D1,H} + \sqrt{1-r^2}\hat{a}^\dagger_{\rm out,H},\\ \hat{a}^\dagger_{\rm a1,V} & \rightarrow & -\hat{a}^\dagger_{\rm D1,V},\end{array}$$

where labelling of spatial modes has been adopted from Fig. 3.1 and H, V denote horizontal and vertical polarizations. Similarly the PPBS$_2$ reflects completely the horizontal polarization and with reflectivity r it reflects vertically polarized photons. The parameter r is to be tuned as explained below. Successful operation of the amplifier is heralded by two-photon coincidence detection on detection blocks D$_1$ and D$_2$.

To demonstrate the principle of operation, let us assume the input signal to be a coherent superposition of vacuum and a polarization-encoded single photon qubit

$$|\psi_{\rm in}\rangle = \alpha|0\rangle + \beta_H|H\rangle + \beta_V|V\rangle,$$

where $|0\rangle$ denotes vacuum, $|H\rangle$, $|V\rangle$ denote horizontal and vertical polarization states respectively and the coefficients meet the normalization condition $|\alpha|^2 + |\beta_H|^2 + |\beta_V|^2 = 1$. The amplifier makes also use of a pair of ancillary photons impinging on ports a_1 and a_2 of PPBS$_1$ and PPBS$_2$ respectively. These ancillary photons are initially in a maximally entangled Bell state of the form

$$|\Phi^+_{a_1a_2}\rangle = \frac{1}{\sqrt{2}}(|H_{a_1}H_{a_2}\rangle + |V_{a_1}V_{a_2}\rangle),$$

where the indices denote the ancillary photons' spatial modes.

The total state entering the amplifier composed of the signal and ancillary photons reads

$$\begin{array}{rcl}|\psi_T\rangle & = & |\psi_{\rm in}\rangle \otimes |\Phi^+_{a_1a_2}\rangle\\ & = & \frac{1}{\sqrt{2}}\left[\alpha|0_{\rm in}H_{a1}H_{a2}\rangle + \alpha|0_{\rm in}V_{a1}V_{a2}\rangle\right.\\ & + & \beta_H|H_{\rm in}H_{a1}H_{a2}\rangle + \beta_H|H_{\rm in}V_{a1}V_{a2}\rangle\\ & + & \left.\beta_V|V_{\rm in}H_{a1}H_{a2}\rangle + \beta_V|V_{\rm in}V_{a1}V_{a2}\rangle\right].\end{array}$$

Now we inspect evolution of all the individual terms present in previous equation. Since the successful operation of the amplifier is conditioned by a two-photon coincidence detection by D_1 & D_2 we post-select only such cases:

$$\begin{aligned}
|0_{\mathrm{in}}H_{a1}H_{a2}\rangle &\rightarrow r|0_{\mathrm{out}}H_{D1}H_{D2}\rangle\\
|0_{\mathrm{in}}V_{a1}V_{a2}\rangle &\rightarrow r|0_{\mathrm{out}}V_{D1}V_{D2}\rangle\\
|H_{\mathrm{in}}H_{a1}H_{a2}\rangle &\rightarrow (2r^2-1)|H_{\mathrm{out}}H_{D1}H_{D2}\rangle\\
|H_{\mathrm{in}}V_{a1}V_{a2}\rangle &\rightarrow r^2|H_{\mathrm{out}}V_{D1}V_{D2}\rangle\\
|V_{\mathrm{in}}H_{a1}H_{a2}\rangle &\rightarrow r^2|V_{\mathrm{out}}H_{D1}H_{D2}\rangle\\
|V_{\mathrm{in}}V_{a1}V_{a2}\rangle &\rightarrow (2r^2-1)|V_{\mathrm{out}}V_{D1}V_{D2}\rangle.
\end{aligned}$$

Note that for $r = 0$, it is impossible to have more than one photon in the output mode, even for multiple photons in the input mode. Subsequently we perform polarization-sensitive detection on D_1 and D_2 in the basis of diagonal $|D\rangle \propto (|H\rangle + |V\rangle)$ and anti-diagonal $|A\rangle \propto (|H\rangle - |V\rangle)$ linear polarization. This way we erase the information about the ancillary state and project the signal at the output port to

$$|\psi_{\mathrm{out}}\rangle \propto \alpha r|0\rangle + \frac{3r^2-1}{2}\left(\beta_H|H\rangle + \beta_V|V\rangle\right),$$

where we have incorporated the fact that only if both the detected polarizations on D_1 and D_2 are identical (DD or AA coincidences) the device heralds a successful amplification and thus only one half of the measurement outcomes contributes to success probability.

At this point, we define the amplification gain G as a fraction between signal and vacuum probabilities

$$G = \frac{(3r^2-1)^2}{4r^2} \tag{3.1}$$

and calculate the corresponding success probability

$$P = r^2\left[|\alpha|^2 + G\left(|\beta_H|^2 + |\beta_V|^2\right)\right]. \tag{3.2}$$

Note that while the gain itself is input state independent, the success probability depends on both the gain and the input state parameters. This reflects the intuitive fact that it is for instance impossible to amplify a qubit that is actually not present in the input state ($\beta_H = \beta_V = 0$).

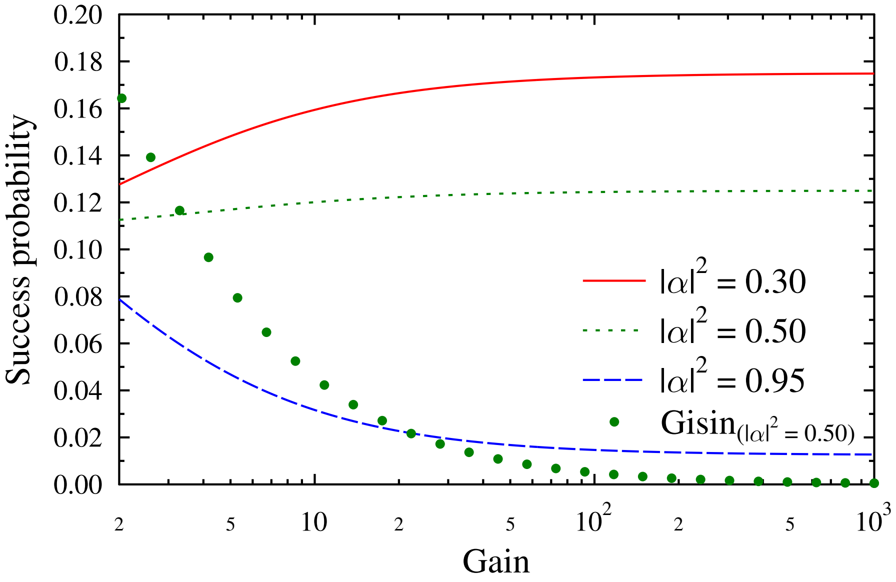


Figure 3.2: Success probability is depicted as a function of gain for three different input states parametrized by $|\alpha|^2$. For comparison, the success probability of Gisin *et al.* scheme [42] is presented (in this case $|\alpha|^2 = 0.5$). Note that the success probability of our amplifier converges asymptotically to a non-zero value for any state with $|\alpha|^2 \neq 1$.

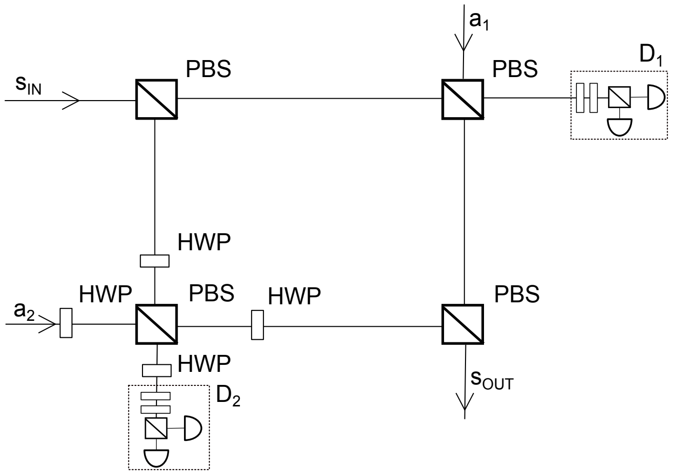


Figure 3.3: Scheme for linear-optical quantum non-demolition measurement of single photon; PBS–polarization beam splitter, HWP–half wave plate (all rotated by 45 deg. with respect to horizontal polarization direction), s–signal photon mode, a$_1$, a$_2$–ancillary photon modes

3.3 Linear-optical scheme for non-demolition detection of single photon presence

Text adopted from Marek Bula, Karol Bartkiewicz, Antonín Černoch, and Karel Lemr. Entanglement–assisted scheme for nondemolition detection of the presence of a single photon. Phys. Rev. A, 87:033826, Mar 2013. [50]

In this section, we show how to use our amplifier for quantum non-demolition detection of a single photon presence [21]. By measuring the state of ancillary photons, the presence of a photon in signal mode is revealed with success probability of 1/2 without any disturbance to its state. We also show how to tune the setup to perform quantum non-demolition measurement of the signal photon state and we provide trade-off between the extracted information and the signal state disturbance.

3.3.1 Principle of operation

The hereby proposed scheme for linear-optical quantum non-demolition measurement is depicted in Fig. 3.3. It consists of four polarizing beam splitters (PBS) transmitting horizontally polarized light and reflecting vertically polarized light, four half wave plates (HWP) set to perform horizontal-vertical polarization swap (H ↔V) and two detectors D_1 and D_2. Apart from the signal photon entering the device by input port s_{IN} there are also two ancillary photons entering by input ports a_1 and a_2. Successful non-demolition detection of the signal photon is obtained when two-photon coincidence detection on the detectors D_1 and D_2 is observed. As derived below, this occurs with probability of 1/2 when signal photon is present and with zero rate if there is no signal photon.

Let us assume the signal photon entering the scheme in an arbitrary polarization state

$$|\psi_s\rangle = \alpha|H\rangle + \beta|V\rangle, \tag{3.3}$$

where H and V denote horizontal and vertical polarization states respectively and the coefficients follow normalization condition $|\alpha|^2 + |\beta|^2 = 1$. The ancillary photons are initially in a maximally entangled Bell state

$$|\psi_{a_1a_2}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle). \tag{3.4}$$

One can therefore formulate the total three-photon state entering the aparatus

$$\begin{aligned} |\psi_T\rangle &= \frac{1}{\sqrt{2}}(\alpha|HHH\rangle + \alpha|HVV\rangle + \\ &\quad +\beta|VHH\rangle + \beta|VVV\rangle), \end{aligned} \tag{3.5}$$

where the order of photons is: signal, first ancillary, second ancillary.

In order to understand the transformation of the total three-photon state, we need to study the transformation of its respective components. As one can easily verify the state $|HHH\rangle$ goes through the scheme unchanged and leads to two photons impinging the detectors D_1 and D_2 while one photon with horizontal polarization leaves the scheme by the signal output port s_{OUT}. Similarly the state $|VVV\rangle$ always passes through the device unmodified leading as well to two-photon coincidence on the detectors and vertically polarized photon leaving the device.

On the other hand, one can observe that in the two remaining cases ($|HVV\rangle$ and $|VHH\rangle$) the states never lead to two-photon coincidence on the detectors D_1 and D_2. In these cases only one of the detectors registers detection event. These cases are excluded from the output state by coincidence post-selection. Since the probability of such outcome is 1/2, the overall success probability of the scheme is the remaining 1/2.

Taking into account the transformation of the input state and the post-selection on detection coincidences, the total state at the output before detection reads

$$|\psi_{\mathrm{OUT}}\rangle = \frac{1}{\sqrt{2}}(\alpha|HHH\rangle + \beta|VVV\rangle), \tag{3.6}$$

where renormalization has been carried out having the success probability of 1/2 in mind. We now perform a projection polarization measurement in the output ancillary ports using diagonal $|D\rangle$ and antidiagonal $|A\rangle$ linear polarization basis. Using this basis, one can rewrite the total output state as

$$\begin{aligned}|\psi_{\mathrm{T}}\rangle = \frac{1}{2\sqrt{2}}[\alpha|H\rangle(|DD\rangle + |AA\rangle + \\ +|DA\rangle + |AD\rangle) + \beta|V\rangle(|DD\rangle + |AA\rangle - \\ -|DA\rangle - |AD\rangle].\end{aligned} \tag{3.7}$$

If $|DD\rangle$ or $|AA\rangle$ coincidence is detected on the ancillary photons the signal photon (in the signal output mode) is projected directly into its initial state (3.3). If $|AD\rangle$ or $|DA\rangle$ coincidences are observed the signal photon is projected into the state

$$|\psi_s\rangle = \alpha|H\rangle - \beta|V\rangle, \tag{3.8}$$

which can be easily reverted to the initial state (3.3) just by inserting a half-wave plate with optical axis coinciding with vertical polarization direction to the signal output port and thus implementing the transformation $V \to -V$ on the signal photon. Note that the particular choice of the measurement basis leads to restoration of the signal state to its exact initial form, while giving no information about its polarization state. Only the presence of the signal photon is witnessed.

To complete the derivation of the principle of operation, let us consider the case when there is no signal photon. Such total state reads

$$|\psi_{\mathrm{T}}\rangle = \frac{1}{\sqrt{2}}\left(|0HH\rangle + |0VV\rangle\right), \tag{3.9}$$

where 0 denotes the absence of signal photon. It is easy to observe, that nor $|0HH\rangle$ nor $|0VV\rangle$ can lead to a coincidence on detectors D_1 and D_2. Therefore observing such coincidence can only happen when the signal photon is present.

3.3.2 Weak measurement

We can be more demanding and apart from the detection of signal photon presence, we can modify the scheme in order to acquire some information also about its polarization state. For instance we can get complete information about the polarization of the signal photon state by simple projection measurement on the first ancillary photon. Eq. (3.6) indicates that there is a perfect correlation between the signal and the ancillary photons. Unfortunately, the signal state is completely disturbed by such measurement.

On the other hand, we can tune the correlation between the signal and ancillary states simply by rotation of the ancillary photons measurement basis. Let us denote the basis rotation angle by ϕ and express the transformation of the basis explicitly

$$\left(\begin{array}{c} |H\rangle \\ |V\rangle \end{array}\right) \rightarrow \left(\begin{array}{cc} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{array}\right) \cdot \left(\begin{array}{c} |H\rangle \\ |V\rangle \end{array}\right).$$

One can substitute the new basis to the original Eq. (3.6) obtaining

$$\begin{aligned} |\psi_\mathrm{T}\rangle &= \alpha[\cos(\phi)^2|HHH\rangle + \cos(x)\sin(x)|HHV\rangle \\ &+ \cos(\phi)\sin(\phi)|HVH\rangle + \sin(\phi)^2|HVV\rangle] \\ &+ \beta[\cos(\phi)^2|VVV\rangle + \cos(\phi)\sin(\phi)|VHV\rangle \\ &+ \cos(\phi)\sin(\phi)|VVH\rangle + \sin(\phi)^2|VHH\rangle]. \end{aligned} \tag{3.10}$$

Hence we can extract the signal photon polarization state information in a tunable manner at the expense of some degree of signal state disturbance. To quantitize the amount of extracted information, we can use the mutual information I defined as

$$I = \sum_{i,j} P_{i,j} \cdot \log_2 \frac{P_{i,j}}{P_i P_j},$$

where P_i is marginal probability of the signal photon having given polarization, P_j is marginal probability of the first ancillary photon having given polarization and $P_{i,j}$ is the joint probability of the both photons having given polarizations. It is evident that I depends on the signal state parameters α and β and the angle of rotation ϕ. One can calculate the explicit formula for the mutual information

$$\begin{aligned} I = |\alpha|^2 \cos\phi^2 \log_2 \frac{\cos\phi^2}{|\alpha|^2\cos\phi^2 + |\beta|^2 \sin\phi^2} \\ +|\alpha|^2 \sin\phi^2 \log_2 \frac{\sin\phi^2}{|\alpha|^2\sin\phi^2 + |\beta|^2 \cos\phi^2} \\ +|\beta|^2 \cos\phi^2 \log_2 \frac{\cos\phi^2}{|\beta|^2\cos\phi^2 + |\alpha|^2 \sin\phi^2} \\ +|\beta|^2 \sin\phi^2 \log_2 \frac{\sin\phi^2}{|\beta|^2\sin\phi^2 + |\alpha|^2 \cos\phi^2} \end{aligned} \tag{3.11}$$

Inevitably we have to pay for obtained information by partial disturbance of the signal state. Amount of a disturbance can be described using fidelity

$$F = \langle\psi_s|\hat{\rho}_{\mathrm{OUT}}|\psi_s\rangle, \tag{3.12}$$

where $\hat{\rho}_{\mathrm{OUT}}$ denotes the generally mixed state of the signal photon at the output obtained from (3.10) by tracing over the ancillary photons. Similarly to the mutual information, we can explicitly find the formula for fidelity as a function of α, β and ϕ

$$F = |\alpha|^4 + |\beta|^4 + |\alpha|^2|\beta|^2 \cos\phi^2 \sin\phi^2. \tag{3.13}$$

The Eqs. (3.11) and (3.13) manifest the the trade-off between the obtained information and the output state disturbance parametrized by the angle ϕ. The plot in Fig. 3.4 visualizes this trade-off for several different values of α and β.

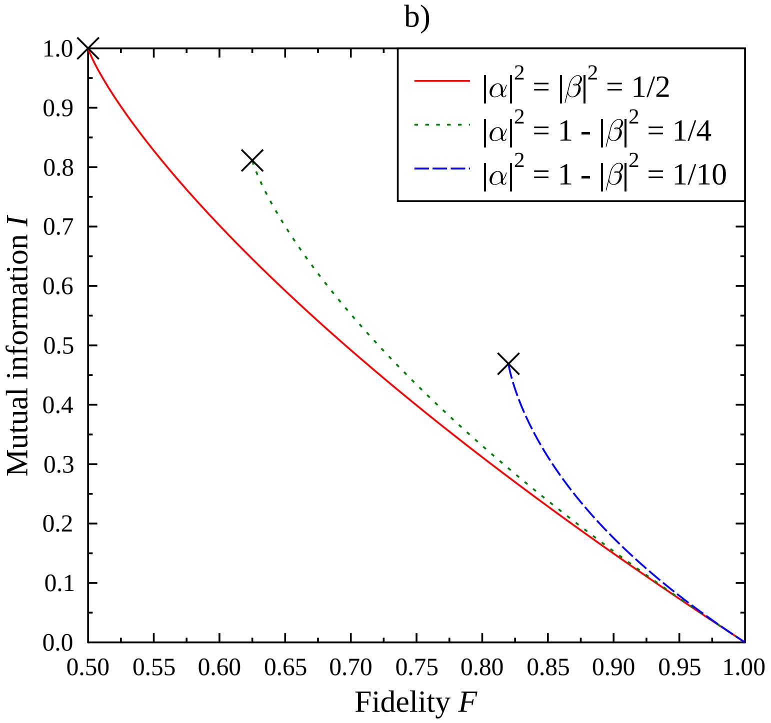


Figure 3.4: Mutual information vs. output state fidelity trade-off shown for three different input states parameters α and β.

Chapter 4

Experimental test of interference visibility with spectrally resolved modes

In this chapter, we focus on realization of an experiment, which challenges conclusions of the experiment by Danan *et al.* from three years ago [51], that demonstred counterintuitive behavior of photons. Our investigation is based on a theoretical paper published by scientists from the Joint Laboratory of Optics of Palacký University [52] addressing the experiment in Ref. [51].

Danan *et al.* [51] tried to measure paths of photons in an interferometer without destroing the interference pattern at the output. Such experiments are usualy called "which–way" or "welcher–weg" experiments.

The which–way experiment arises from thoughts about the wave–particle duality at the beging of the 19th century. Since 1807 we have known about this special behaviour of the light owing to the double–slit experiment executed by Tomas Jung [53]. However when Heisenberg derived the uncertainty principle, a question had arised: can we exactly determine the path of a photon in the double–slit experiment and simultaneously preserve the interference pattern? Over time, several physicists made significant mathematical and experimental proves that it is imposible [54–57]. Simply put, we can say, that better knowing the path leads always to more blurred interference pattern. However, the debate about "welcher–weg" experiments is stil alive and lot of investigators are searching how to test elementary principles of quantum mechanics. For instance, S. Afshar carried out the special kind of double–slit experiment with results, which are seemingly not in agreement with principle of complementarity [58]. But his conclusions are controversial and strongly criticised [59].

In 2013 Danan *et al.* have performed another “welcher–weg” experiment using weak measurement to investigate path of photons [51]. Their experimental setup consists of two composite Mach–Zehnder interferomets (MZI), depicted in Fig. 4.1. This arrangement have several specialities, mainly that each mirror vibrates in vertical direction with frequencies, that are comprime interegers. Deviations of mirrors are small enough to preserve interference conditions. The same intensities of light on the mirrors are provided by unbalanced beam spliters (BS) of the outer interferometer, the inner MZI uses balanced BS. The setup is terminated by a quad–cell photodetector, which measures difference of the currents generated from upper and lower parts. Detected signal is processed by the harmonic analysis in Matlab.

In the paper, they describe three measurement regimes with different adjustments (Fig.4.1). First they tested correct working of their setup (Fig.4.1–a). We can see that power spectrum contains several frequency peeks corresponding to frequencies of mirrors.

They obtained two suprising results in the second measurement (Fig.4.1–b), where the phase in the inner MZI is set for destructive interference to occur at output towars mirror F, e.g. light goes out from the setup. Nevertheless, harmonic analysis shows not only frequency C in the output signal, as we usualy assume, but there are A, B frequencies present as well. There are however no frequencies E, F. They ascribe this phenomenon to the photon interacting with mirrors A, B despite it supposedly traveled in lower arm of the outer MZI.

Third measurement (Fig.4.1–c) should prove mentioned adjustment of destructive intefrence on the output BS of the inner MZI. Light in lower arm of the outer MZI is blocked and frequency peak of mirror C is not obtained, of course. But we can not observe any of the frequencies (not even A or B)!

Some criticism arised together with questions of the results and conclusions of the Danan *et al.* experiment [51]. Physicists from our Joint Laboratory of Optics revised Danan’s *et al.* experimental procces and conclusions and discovered alternative explanaition of their results [52].

Frequencie A, B are distinguishable, respectively we can recognize that

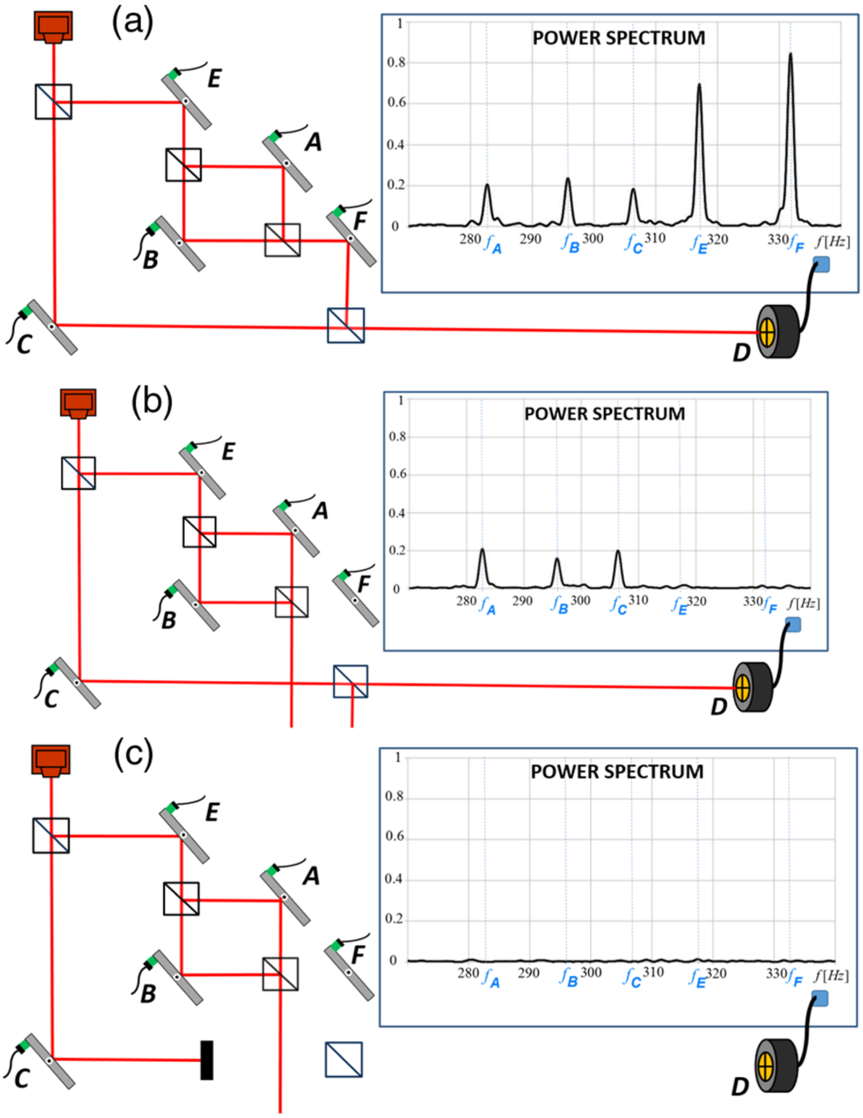


Figure 4.1: Experimental setup and results of the Danan *et al.* experiment. Direct copy from Ref. [51] is shown here.

photon interacted with one of these mirrors, thus gives us information about which path it traveled and no interference takes place. The lack of destructive interference makes half of the photons from the inner interferometer lead towards the mirror F. Instead of this, knowing frequencies E, F can not reveal the photon's path, these photons are allowed to interfere and do not travel towards the detector. Second measurement (Fig.4.1–b) does not really demonstrate surprising behavior.

Someone may say, that A and B should be present in the third measurement (Fig.4.1–c) as well like in the second measurement (Fig.4.1–b). Indeed, thay are, assuming that the detector is able to observe them. We claim, that there are interference fringes parallel with axis of symmetry of the detector. Owing to measuring of the difference between upper and lower part, the signal was discarded.

This part of the thesis reimplements the Danan *et al.* measurement in a different configuration and direct frequency mode measurement. The results predicted in Ref. [52] disagree with Danan *et al.* [51] conclusion only in configuration (c), Fig.4.1–c. It is thus necessary to build only the inner MZI to test this configuration since the outer MZI has the other arm blocked.

4.1 Experimental setup and adjustment

We have built an experimental setup in the form of a MZI, depicted in Fig.4.2.

It consists of two polarization independent beam splitters $\mathrm{BS}_{1,2}$ and two pentagonal prisms (pentaprism) serving as mirrors. The light beam was produced by a modelocked femtosecond laser Coherent Mira with central wavelength of 826 nm, 10 nm bandwidth and typical mean power of 1W. Light is coupled into the interferometer by BS_1. Motorized translation stage (MT) is attached to lower pentaprism to balance lengths of both of the arms. The piezo translation stage is attached to the upper pentaprism to change the relative phase of the light in the two arms. For purposes of this experiment, we have used two identical filters $\mathrm{F}_{1,2}$ with transmission bandwidth of 3 nm centered at 826 nm. F_2 was mounted on a rotation stage allowing to shift its spectral transmission window. The last component of the interferometer, BS_2, provides indistinguishable coupling of the light from both the arms. Because of technological imperfections BS_1 and BS_2 are not 50:50 balanced splitters.

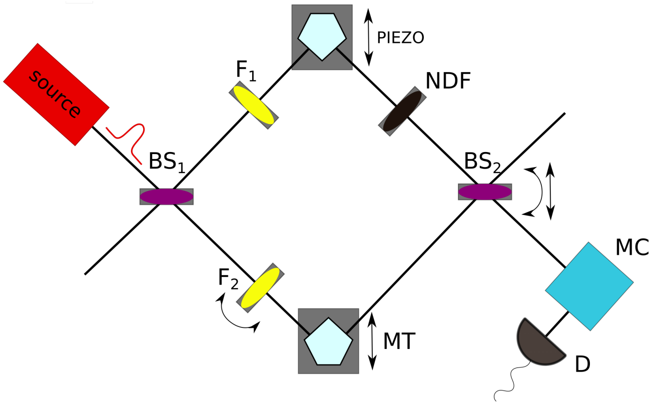


Figure 4.2: Experimental setup of the “which–way” experiment as described in the text. Individual components are labaled as follows: laser SOURCE producing a light beam, $BS_{1,2}$ are beam spliters, $F_{1,2}$ are narrowband filters, $P_{1,2}$ are pentaprisms, MT is motorized translation, PIEZO is piezo–driven translation, MC is monochromator and D is detector.

Also overall transmission of F_2 depends on its rotation. Neutral density filter (NDF) was therefore inserted into one of the arms to componsate for it. The monochromator Jobin Yvon Triax (MC) is located in one of the interferometer output ports and provides us the capability to discriminate detected light depending on its frequency. The output signal was coupled to single–mode fibre to maximize spatial indistingushability and then detected using a Thorlabs Power meter PM 210 (D). For the adjustments of the setup, both filters $F_{1,2}$ were rotated perpendicular to the light beam and MC was removed. First, we ensured precise coupling of the beam to the setup. We checked, that polarization remains unchanged being transmitted or reflected on beam splitters. The remaing part of adjustments consists of several independent steps, which have to be repeated several times during process of measurement. Balanced output intensities from both of the arms are substantial and we achieve that by using NDF. Then lenghts of the arms were equalised using MT. Accurate setting of MT position has been adjusted by finding maxima of the autocorrelation function. We were able to reach visibility of the interefometer about 98%. Temporal stability of the interferometer is much higher then typical measurement time, which is about 30 sec.

4.2 Measurement and results

The purpose of this measurement is to observe various levels of distinguishability between the light traveling in the two arms of the interferometer. In order to do that, filter F_2 was rotated to various positions, so to shift the central wavelength. Then we have observed the spectrally dependent interference between the arms at the output. The rotation causes shift of the lenght of the optical path as well, which has to be again balanced by MT. We have performed nine sets of measurements for different rotations of F_2. Each measurement set consists of scanning the light spectrum by MC in the range from 815 to 835 nm with resolution of 0.2 nm. First, we measured intensity spectrum from each arm separately, thus without the interference. We use this data for theoretical prediction, see below. Next, for each wavelength we measured the visibility of interference as a measure of distinguishability between the arms. This was achieved by scaning of the piezo–driven translation as discussed in Sec. 2.4.6. When the light beams have equal intensities at a given wavelength, the visibility is maximized. It can be calculated as function of the mutual phase shift between the arms for interference contrast.

$$V(\lambda) = \frac{I_{\max}(\lambda) - I_{\min}(\lambda)}{I_{\max}(\lambda) + I_{\min}(\lambda)} \tag{4.1}$$

The error of the intensity measurement was estimated from typical measurement errors of detector D. These have been found by determinating the standard deviation for the various mean values of the light intensity.

The example of one measurement set is depicted in the Fig.4.3. Based on this measurement, we selected three wavelengths from the measured spectrum corresponding to the maximum and two minima of visibility. These wavelengths were labeled E for maximum of the visibility and A, B for the two minima. The labeling of wavelengths/frequencies is adopted from the experiment executed by Danan *et. al.* [51]. Both arms have same intensity on E, thus indistinguishable and we observe maximum visibility. On the other hand, frequencies A, B are as much distinguishable as possible for the given rotation of F_2. Normalized intensities at these wavelengths are summarised in Tab.4.1 and visualised in Fig.4.4.

Black bars depict intensity maxima, whereby grey bars depict intensity minima. Input intensity corrected for technological losses was used for inten-

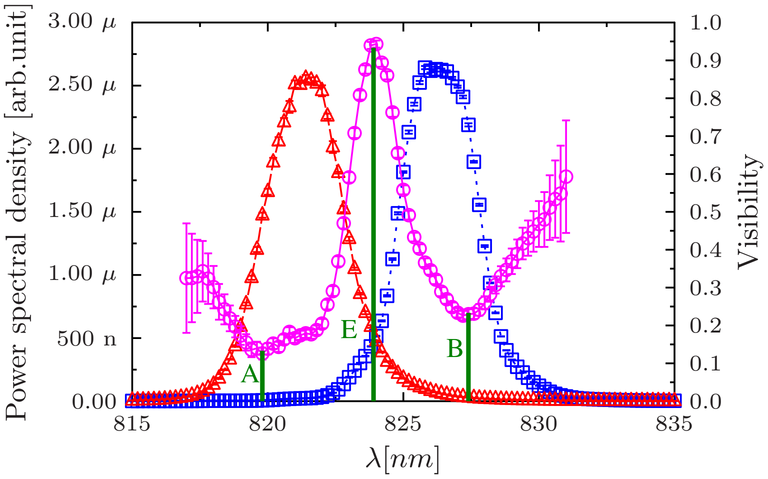


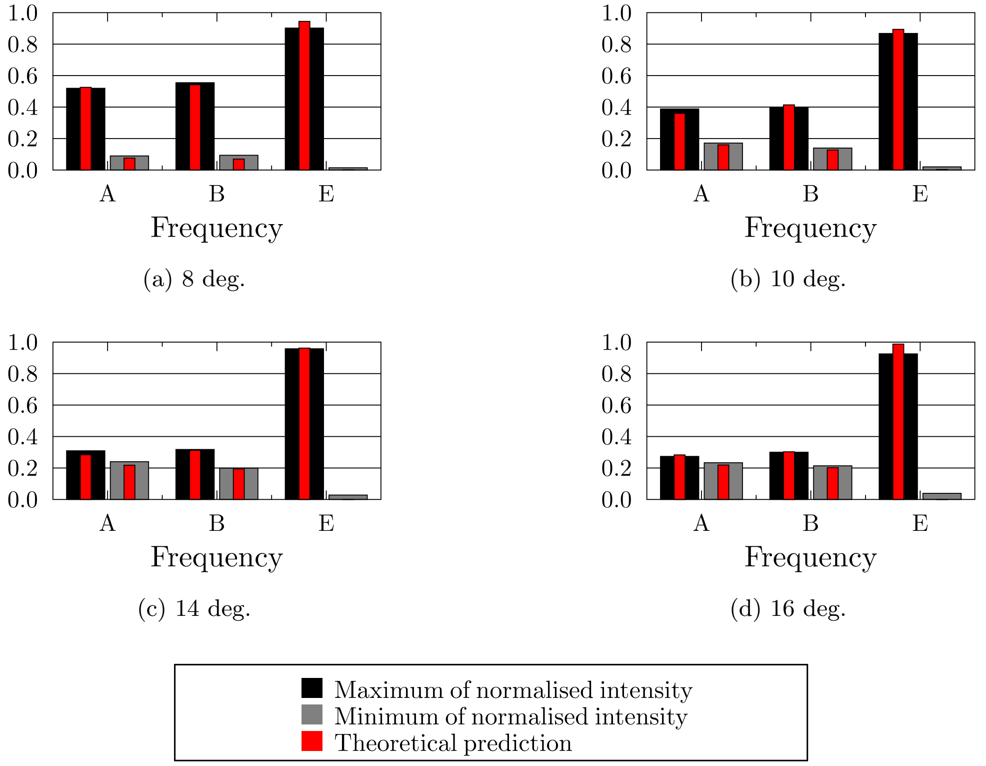
Figure 4.3: Example of measured data for F_2 rotated by 14 degrees. Triangles and squares represent pure spectral density for lower and upper arms. Circles visualize obtaneid visibility. Vertical lines labeled A,E,B are selected wavelengths corresponding to maximum and minima of the visibility.

sity normalisation. Inner red bars depict theoretical prediction showing a good agreement with measurement data. Assuming perfect indistinguishability in all degrees of freedom apart from the intensity spectra overlap, maximum and minimum intensity are predicted to be

$$I_{\text{max}} = \left(\sqrt{I_1} + \sqrt{I_2}\right)^2$$

$$I_{\text{min}} = \left(\sqrt{I_1} - \sqrt{I_2,}\right)^2 \tag{4.2}$$

where I_1 and I_2 denote intensity observed from individual arms at a given frequency mode. These predicted values are used for comparison with directly obtained experimental data. Theoretical model is derived from measured I_1 and I_2, because finding of analytic description of the shape of the filter is very complicated, moreover when the filter F_2 changes its shape by rotation from the perspective of beam.



(a) 8 deg.

(b) 10 deg.

(c) 14 deg.

(d) 16 deg.

Figure 4.4: Processed maesurement data for four rotations of F_2: 8, 10, 14 and 16 degrees. Black bars represent normalised maxima of spectral power density for the wavelengts A, B, E, grey bars, in a similar way, represent spectral power density minima. Theoretical predictions are shown using the inner red bars.

4.3 Conclusion

Experimental data confirm theoretical prediction from [52]. Possible differences and errors are negligible and caused by experimental imperfections.

Visibility for wavelengths A, B is higher for smaller angles, as it is a consequence of higher spectral overlap of A, B. In case that overlap is small, interference fringes almost vanish. On the other hand, visibility of wavelength E is stable for each angle since it does not provide any "which–path" information.

We therefore conclude that frequency peaks A and B insensitive to phase adjustment in the inner MZI when their corresponding modes are completely indistinguishable. In contrast to the Danan *et al.* method, our detection method is able to register these peaks even when the experimental setup keeps the conditions of the Danan *et al.* experimental setting in Fig.4.1–c.

This fact back–ups the conclusion drawn in [52] that the measurement methods of Danan *et al.* ignores axially symmetric signal.

Table 4.1: The table contains measuered data and their theoretical predictions for various rotations of the filter F_2. All intensities are normalised, thus unitless.

		Frequency mode A		**Frequency mode B**		**Frequency mode E**	
F_2 rotation		I_{max}	I_{min}	I_{max}	I_{min}	I_{max}	I_{min}
8 deg.	experiment	0.519 ± 0.005	0.089 ± 0.002	0.555 ± 0.007	0.094 ± 0.003	0.902 ± 0.006	0.014 ± 0.001
	theory	0.525	0.076	0.542	0.067	0.945	0.001
10 deg.	experiment	0.388 ± 0.006	0.171 ± 0.004	0.398 ± 0.005	0.140 ± 0.003	0.868 ± 0.006	0.020 ± 0.001
	theory	0.360	0.160	0.414	0.127	0.894	0.003
12 deg.	experiment	0.296 ± 0.004	0.191 ± 0.003	0.410 ± 0.005	0.204 ± 0.003	1.058 ± 0.011	0.040 ± 0.002
	theory	0.310	0.196	0.349	0.167	0.919	0.002
14 deg.	experiment	0.309 ± 0.007	0.240 ± 0.006	0.318 ± 0.005	0.199 ± 0.003	0.958 ± 0.020	0.028 ± 0.005
	theory	0.284	0.218	0.312	0.195	0.962	0.0004
16 deg.	experiment	0.274 ± 0.005	0.234 ± 0.005	0.300 ± 0.006	0.214 ± 0.005	0.925 ± 0.030	0.039 ± 0.010
	theory	0.274	0.219	0.303	0.202	0.987	0.00004

Chapter 5

Conslusions

Today, modern society requires progress in comunication technologies. Quantum computation promises faster transmission and proccesing of data, more efficiency storage or unconditionally secure communications. These ideas are confirmed by several experiments with exciting results, like quantum teleportation or realization of quantum logical gates. We consider that research in quantum computation is a reasonable topic for intensive scientific investigation.

In our proposals and experiments, we use linear–optical components like beam splitters, wave plates, neutral density filters. The platform of linear optics is relatively low cost and accessible laboratory equipment. Moreover, it seems to be a prominent platform, which could be used in practical implementations of quantum protocols.

In the third chapter of this thesis, we introduce our proposal for the heralded qubit amplifier, that can be used to increase safety of quantum key distribution in quantum cryptography [48]. It outpermforms the other published heralded qubit amplifiers [42,46,47]. Success probability of our amplifier does not go to the zero in contrast to Gisin *et al.* [42] for infinite gain. Our proposed device has also tunable gain and in the case of the infinite gain it works similarly as the scheme proposed by Curty and Moroder [47], which however works only in this regime. We overcome Pitkanen *et al.* proposal [46], because they require photon–number–resolving detectors and our device needs only standard binary detectors at least in infinite gain regime.

Moreover, we investigated more generaly this device, which can be used for weak measurement and presence detection of a photon [50].

In the fourth chapter, we introduce experimental part of this thesis. We executed a quite known “welcher–weg” experiment that tried to contribute to the discusion about counterintuitive results of the experiment executed by Danan *et al* [51]. We want to experimentaly show that Danan *et al.* [51] used a non–suitable detection method.

Bibliography

[1] Internet World Stats. http://www.internetworldstats.com/stats.htm). Accessed:2016-04-10.

[2] Data on big data. http://marciaconner.com/blog/data-on-big-data). Accessed:2016-04-10.

[3] ter Dirk Haar. On an Improvement of Wien's Equation for the Spectrum translated by Dirk ter Haar. http://www.ffn.ub.es/luisnavarro/nuevo_maletin/Planck%20%281900%29,%20Improvement%20of%20Wien's.pdf. Accessed: 2016-27-3.

[4] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, 1985.

[5] Peter W. Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[6] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[7] Julsgaard Brian, Sherson Jacob, Cirac J. Ignacio, Fiurasek Jaromir, and Polzik Eugene S. Experimental demonstration of quantum memory for light. *Nature*, 432(7016):482–486, nov 2004. 10.1038/nature03064.

[8] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[9] Ma Xiao-Song, Herbst Thomas, Scheidl Thomas, Wang Daqing, Kropatschek Sebastian, Naylor William, Wittmann Bernhard, Mech Alexandra, Kofler Johannes, Anisimova Elena, Makarov Vadim, Jennewein Thomas, Ursin Rupert, and Zeilinger Anton. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269–273, sep 2012.

[10] Bouwmeester Dik, Pan Jian-Wei, Mattle Klaus, Eibl Manfred, Weinfurter Harald, and Zeilinger Anton. Experimental quantum teleportation. *Nature*, 390(6660):575–579, dec 1997.

[11] M. Dušek. *Koncepční otázky kvantové teorie.* Univerzita Palackého, 2002.

[12] Commercial use of QKD by ID Quantique. `http://www.idquantique.com/quantum-safe-crypto/`. Accessed: 2016-27-3.

[13] Wootters W. K. and Zurek W. H. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, oct 1982.

[14] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[15] T. Opatrný and L. Richterek. *Vybrané partie současné fyziky.* Univerzita Palackého v Olomouci, 2005.

[16] Weinberg Steven. *The quantum theory of fields.* University of Texas at Austin, 1995.

[17] M. Born and P. Jordan. Zur Quantenmechanik (On Quantum Mechanics). *Zeitschrift für Physik*, 34(1):858–888, December 1925.

[18] William A. Fedak and Jeffrey J. Prentis. The 1925 Born and Jordan paper “On quantum mechanics”. *American Journal of Physics*, 77(2):128–139, 2009.

[19] Karel Lemr. *Experimental quantum information processing with photon pairs.* PhD thesis, Faculty of Science, Palacký University in Olomouc, 2012.

[20] Sakurai J. J. *Modern Quantum Mechanics (Revised Edition).* Addison Wesley, September 1993.

[21] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79:135–174, Jan 2007.

[22] Govind P. Agrawal. *Fibre-optic communication systems.* WILEY- 623 INTERSCIENCE A JOHN WILEY & SONS, INC., PUBLICATION, third edition, 2002.

[23] Klemens Hammerer, Anders S. Sørensen, and Eugene S. Polzik. Quantum interface between light and atomic ensembles.

[24] Trauzettel Bjorn, Bulaev Denis V., Loss Daniel, and Burkard Guido. Spin qubits in graphene quantum dots. *Nat Phys*, 3(3):192–196, mar 2007. 10.1038/nphys544.

[25] Makhlin Yuriy, Scohn Gerd, and Shnirman Alexander. Josephson-junction qubits with controlled couplings. *Nature*, 398(6725):305–307, mar 1999. 10.1038/18613.

[26] Lorenza Viola, Emanuel Knill, and Raymond Laflamme. Constructing qubits in physical systems. *Journal of Physics A: Mathematical and General*, 34(35):7067, 2001.

[27] B. Schumacher. Quantum coding. , 51:2738–2747, April 1995.

[28] Tim C Raplh and Geoff J Pryde. Optical quantum computation. *Progress in Optics*, 54:209–269, 2010.

[29] Marek Bula. *Experimental implementation of fibre Mach-Zehnder interferometer with variable splitting ratios.* Bachelor's thesis, Faculty of Science, Palacký University in Olomouc, 2012.

[30] Adriano Barenco. A Universal Two-Bit Gate for Quantum Computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 449(1937):679–683, 1995.

[31] David P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51:1015–1022, Feb 1995.

[32] 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, Nov 1987.

[33] B. E. A. Saleh and M. C. Teich. *Základy Fotoniky.* Český překlad Matfyzpress, UK Praha, 1995.

[34] Ludwig Zehnder. Ein neuer Interferenzrefraktor. *Zeitschrift für Instrumentenkunde*, 111:275–285, 1891.

[35] Jonatan Bohr Brask, Nicolas Brunner, Daniel Cavalcanti, and Anthony Leverrier. Bell tests for continuous-variable systems using hybrid measurements and heralded amplifiers. *Phys. Rev. A*, 85:042116, Apr 2012.

[36] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Rev. Mod. Phys.*, 77:1225–1256, Nov 2005.

[37] J. A. Levenson, I. Abram, T. Rivera, P. Fayolle, J. C. Garreau, and P. Grangier. Quantum optical cloning amplifier. *Phys. Rev. Lett.*, 70:267–270, Jan 1993.

[38] T. C. Ralph and A. P. Lund. Nondeterministic Noiseless Linear Amplification of Quantum Systems.

[39] Xiang G. Y., Ralph T. C., Lund A. P., Walk N., and Pryde G. J. Heralded noiseless linear amplification and distillation of entanglement. *Nat Photon*, 4(5):316–319, may 2010.

[40] Franck Ferreyrol, Marco Barbieri, Rémi Blandino, Simon Fossier, Rosa Tualle-Brouri, and Philippe Grangier. Implementation of a Nondeterministic Optical Noiseless Amplifier. *Phys. Rev. Lett.*, 104:123603, Mar 2010.

[41] Zavatta A., Fiurasek J., and Bellini M. A high-fidelity noiseless amplifier for quantum light states. *Nat Photon*, 5(1):52–60, 2011.

[42] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier. *Phys. Rev. Lett.*, 105:070501, Aug 2010.

[43] Kocsis S., Xiang G. Y., Ralph T. C., and Pryde G. J. Heralded noiseless amplification of a photon polarization qubit. *Nat Phys*, 9(1):23–28, jan 2013.

[44] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Valerio Scarani, Vadim Makarov, and Christian Kurtsiefer. Experimentally Faking the Violation of Bell's Inequalities. *Phys. Rev. Lett.*, 107:170404, Oct 2011.

[45] Umesh Vazirani and Thomas Vidick. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[46] David Pitkanen, Xiongfeng Ma, Ricardo Wickert, Peter van Loock, and Norbert Lütkenhaus. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Phys. Rev. A*, 84:022325, Aug 2011.

[47] Marcos Curty and Tobias Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84:010304, Jul 2011.

[48] Evan Meyer-Scott, Marek Bula, Karol Bartkiewicz, Antonín Černoch, Jan Soubusta, Thomas Jennewein, and Karel Lemr. Entanglement-based linear-optical qubit amplifier. *Phys. Rev. A*, 88:012327, Jul 2013.

[49] Eva Halenková, A. Černoch, K. Lemr, J. Soubusta, and S. Drusová. Experimental implementation of the multifunctional compact two-photon state analyzer. *Appl. Opt.*, 51(4):474–478, Feb 2012.

[50] Marek Bula, Karol Bartkiewicz, Antonín Černoch, and Karel Lemr. Entanglement-assisted scheme for nondemolition detection of the presence of a single photon. *Phys. Rev. A*, 87:033826, Mar 2013.

[51] A. Danan, D. Farfurnik, S. Bar-Ad, and L. Vaidman. Asking Photons Where They Have Been. *Phys. Rev. Lett.*, 111:240402, Dec 2013.

[52] Karol Bartkiewicz, Antonín Černoch, Dalibor Javůrek, Karel Lemr, Jan Soubusta, and Jiří Svozilík. One-state vector formalism for the evolution of a quantum state through nested Mach-Zehnder interferometers. *Phys. Rev. A*, 91:012103, Jan 2015.

[53] Tomas Jung. *A Course of Lectures on Natural Philosophy and the Mechanical Arts*, volume 104. 1804.

[54] William K. Wootters and Wojciech H. Zurek. Complementarity in the double-slit experiment: Quantum nonseparability and a quantitative statement of Bohr's principle. *Phys. Rev. D*, 19:473–484, Jan 1979.

[55] David Deutsch. Uncertainty in Quantum Measurements. *Phys. Rev. Lett.*, 50:631–633, Feb 1983.

[56] Marlan O. Scully and Kai Drühl. Quantum eraser: A proposed photon correlation experiment concerning observation and "delayed choice" in quantum mechanics. *Phys. Rev. A*, 25:2208–2213, Apr 1982.

[57] Berthold-Georg Englert. Fringe Visibility and Which-Way Information: An Inequality. *Phys. Rev. Lett.*, 77:2154–2157, Sep 1996.

[58] Shahriar S. Afshar. Violation of the principle of complementarity, and its implications. *Proc. SPIE*, 5866:229–244, 2005.

[59] Ole Steuernagel. Afshar's Experiment Does Not Show a Violation of Complementarity. *Foundations of Physics*, 37(9):1370–1385, 2007.

Appendix

Faculty
of Science

Confirmation of contribution

As the supervisor and corresponding author of Marek Bula's publications

- M. Bula, K. Bartkiewicz, A. Černoch, and K. Lemr, *"Entanglement-assisted scheme for nondemolition detection of the presence of a single photon,"* Phys. Rev. A **87**, 033826 (2013),
- E. Meyer-Scott, M. Bula, K. Bartkiewicz, A. Černoch, J. Soubusta, T. Jennewein, and K. Lemr, *"Entanglement-based linear-optical qubit amplifier,"* Phys. Rev. A **88**, 012327 (2013),

I hereby certify that Marek Bula significantly contributed to the scientific investigation presented in these publications as well as to writing of the manuscripts. The extracts of publications directly quoted in his thesis were predominantly written by him.

Olomouc, 18th April 2016

Karel

....

Mgr. Karel Lemr, Ph.D.
Joint Laboratory of Optics

Entanglement-based linear-optical qubit amplifier

Evan Meyer-Scott,[1] Marek Bula,[2] Karol Bartkiewicz,[2,*] Antonín Černoch,[3] Jan Soubusta,[3]
Thomas Jennewein,[1] and Karel Lemr[3,†]

[1]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo,
200 University Avenue W, Waterloo, Ontario, Canada N2L 3G1*

[2]*RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic,
17. listopadu 12, 771 46 Olomouc, Czech Republic*

[3]*Institute of Physics of Academy of Sciences of the Czech Republic, Joint Laboratory of Optics of PU and IP AS CR, 17. listopadu 50A,
772 07 Olomouc, Czech Republic*

(Received 6 June 2013; published 26 July 2013)

We propose a linear-optical scheme for an efficient amplification of a photonic qubit based on interaction of the signal mode with a pair of entangled ancillae. In contrast to a previous proposal for qubit amplifier by Gisin *et al.* [Phys Rev. Lett. **105**, 070501 (2010)], the success probability of our device does not decrease asymptotically to zero with increasing gain. Moreover, we show how the device can be used to restore entanglement deteriorated by transmission over a lossy channel and calculate the secure key rate for device-independent quantum key distribution.

DOI: 10.1103/PhysRevA.88.012327 PACS number(s): 03.67.Hk, 42.50.Dv, 03.67.Lx

I. INTRODUCTION

The fundamentals of quantum physics were discovered and formulated nearly a hundred years ago. Three decades ago scientists postulated that the laws of quantum physics could be used to improve capabilities of computation and communication technologies [1]. This idea sparked intense research resulting in the discovery of many quantum information protocols, some of them even with practical, modern implementations [2,3].

One such application of quantum information is quantum cryptography, comprising various quantum key distribution protocols (QKD) [4]. QKD offers unconditional security of private communications certified by the laws of quantum physics. In the real world, QKD suffers from various technological limits, especially the need to trust imperfect detectors and single photon sources, quantum channel losses, and background noise. The latter effects limit the maximum distance for unconditionally secure communications [5]. Long-distance QKD has been realized over 144 km in free-space [6] and over 260 km in an optical fiber [7]. Trust in the imperfect devices used for cryptography allows eavesdroppers to attack unintended leakages of information or control detectors, known as side channels [8].

The side channel attacks can be solved in principle by using Bell-state projection measurements or using entanglement-based protocols. The simpler approach is measurement-device-independent QKD [9–11]. In this case a projection on a Bell state in the middle of the communication line removes all detector side channels. The more complete approach is device-independent QKD (DI-QKD) [12–16] and its security is based on the loophole-free violation of a Bell inequality. DI-QKD removes all source and detector side channels but requires closing of the detector (high-efficiency detection) and locality (distant detectors) loopholes, which has not yet been achieved simultaneously [17].

For DI-QKD and other protocols requiring high-efficiency detection, a method is required to circumvent the channel losses inherent in photon transmission. In classical optical communication networks the problem of losses is solved using amplifiers of the classical signal. For quantum communication, losses are more fundamental. The quantum signals are stored in polarization or temporal modes of individual photons and any quantum amplifier is bound by the quantum limits like the no-cloning theorem [18]. Several proposals of quantum amplifiers were recently introduced, wherein the quantum limit can be circumvented by making the amplification nondeterministic. This type of amplification is called heralded noiseless amplification [19] and is already seeing successful implementation [12]. Note that there exists a complete equivalence between distribution of two-qubit entanglement and secure key distribution [20]. In other words, any quantum channel is capable of secret communication if and only if it is capable of distributing entanglement.

In this article we propose a scheme of a linear-optical qubit amplifier that can restore the attenuated qubit and is also capable of distilling deteriorated entanglement of the qubit state. Our amplifier is ready to be used in DI-QKD schemes. Moreover, it outperforms previously published proposals. In contrast to the Gisin *et al.* scheme [13], the success probability of our device does not asymptotically approach zero when increasing the amplification gain. Furthermore, in comparison to the Pitkanen *et al.* scheme [14], our device provides tunable gain and for the case of infinite gain allows better success probability due to its intrinsic elimination of the two-photon component after heralding. However, the Pitkanen *et al.* device may perform better when using a probabilistic source for the ancilla photons, due to its extra stage of heralding. The scheme by Curty and Moroder makes use of entanglement as in our device, but it is limited to infinite gain only [15], and in this regime it performs comparably to our device. Further to these works, we present a thorough investigation of the gain versus

[*] bartkiewicz@jointlab.upol.cz
[†] k.lemr@upol.cz

success probability tradeoff which is a crucial figure of merit for probabilistic amplifiers.

The paper is organized as follows. The principle of the amplifier operation is explained in Sec. II. The entanglement distillation is analyzed in Sec. III and DI-QKD is discussed in Sec. IV. Conclusions are drawn in the final Sec. V.

II. PRINCIPLE OF OPERATION

The amplifier (depicted in Fig. 1) consists of four polarizing beam splitters. Two of them (PBS$_{\text{in}}$ and PBS$_{\text{out}}$) form a Mach-Zehnder interferometer between signal input port "in" and output port "out." These polarizing beam splitters totally transmit horizontally polarized light while totally reflect light with vertical polarization. The other two are partially polarizing beam splitters, denoted as PPBS$_1$ and PPBS$_2$, and placed in their respective arms of the interferometer. PPBS$_1$ reflects vertically polarized light, while having reflectivity r for horizontal polarization. In terms of creation operators this transformation reads

$$\begin{aligned}\hat{a}^{\dagger}_{\text{in},H} &\rightarrow r\hat{a}^{\dagger}_{\text{out},H} + \sqrt{1-r^2}\hat{a}^{\dagger}_{\text{D1},H},\\ \hat{a}^{\dagger}_{a1,H} &\rightarrow -r\hat{a}^{\dagger}_{\text{D1},H} + \sqrt{1-r^2}\hat{a}^{\dagger}_{\text{out},H},\\ \hat{a}^{\dagger}_{a1,V} &\rightarrow -\hat{a}^{\dagger}_{\text{D1},V},\end{aligned}$$

where labeling of spatial modes has been adopted from Fig. 1 and H, V denote horizontal and vertical polarizations. Similarly the PPBS$_2$ reflects completely the horizontal polarization and with reflectivity r it reflects vertically polarized photons. The parameter r is to be tuned as explained below. Successful operation of the amplifier is heralded by two-photon coincidence detection on detection blocks D$_1$ and D$_2$.

To demonstrate the principle of operation, let us assume the input signal to be a coherent superposition of vacuum and a polarization-encoded single photon qubit

$$|\psi_{\text{in}}\rangle = \alpha|0\rangle + \beta_H|H\rangle + \beta_V|V\rangle,$$

where $|0\rangle$ denotes vacuum, $|H\rangle$, $|V\rangle$ denote horizontal and vertical polarization states, respectively, and the coefficients meet the normalization condition $|\alpha|^2 + |\beta_H|^2 + |\beta_V|^2 = 1$.

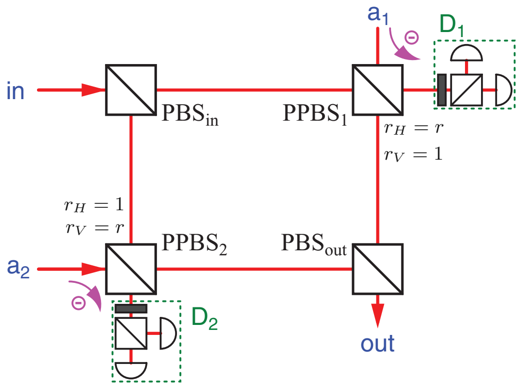


FIG. 1. (Color online) Scheme for entanglement-based linear-optical qubit amplifier as described in the text. D$_1$ and D$_2$ are standard polarization analysis detection blocks (for reference see [21]).

The amplifier makes also use of a pair of ancillary photons impinging on ports a_1 and a_2 of PPBS$_1$ and PPBS$_2$, respectively. These ancillary photons are initially in a maximally entangled Bell state of the form

$$|\Phi^{+}_{a_1a_2}\rangle = \frac{1}{\sqrt{2}}(|H_{a_1}H_{a_2}\rangle + |V_{a_1}V_{a_2}\rangle),$$

where the indices denote the ancillary photons' spatial modes.

The total state entering the amplifier composed of the signal and ancillary photons reads

$$\begin{aligned}|\psi_T\rangle &= |\psi_{\text{in}}\rangle \otimes |\Phi^{+}_{a_1a_2}\rangle\\ &= \frac{1}{\sqrt{2}}\,[\alpha|0_{\text{in}}H_{a1}H_{a2}\rangle + \alpha|0_{\text{in}}V_{a1}V_{a2}\rangle\\ &\quad + \beta_H|H_{\text{in}}H_{a1}H_{a2}\rangle + \beta_H|H_{\text{in}}V_{a1}V_{a2}\rangle\\ &\quad + \beta_V|V_{\text{in}}H_{a1}H_{a2}\rangle + \beta_V|V_{\text{in}}V_{a1}V_{a2}\rangle]\,.\end{aligned}$$

Now we inspect evolution of all the individual terms present in the previous equation. Since the successful operation of the amplifier is conditioned by a two-photon coincidence detection by D$_1$ and D$_2$ we postselect only such cases:

$$\begin{aligned}|0_{\text{in}}H_{a1}H_{a2}\rangle &\rightarrow r|0_{\text{out}}H_{\text{D1}}H_{\text{D2}}\rangle,\\ |0_{\text{in}}V_{a1}V_{a2}\rangle &\rightarrow r|0_{\text{out}}V_{\text{D1}}V_{\text{D2}}\rangle,\\ |H_{\text{in}}H_{a1}H_{a2}\rangle &\rightarrow (2r^2-1)|H_{\text{out}}H_{\text{D1}}H_{\text{D2}}\rangle,\\ |H_{\text{in}}V_{a1}V_{a2}\rangle &\rightarrow r^2|H_{\text{out}}V_{\text{D1}}V_{\text{D2}}\rangle,\\ |V_{\text{in}}H_{a1}H_{a2}\rangle &\rightarrow r^2|V_{\text{out}}H_{\text{D1}}H_{\text{D2}}\rangle,\\ |V_{\text{in}}V_{a1}V_{a2}\rangle &\rightarrow (2r^2-1)|V_{\text{out}}V_{\text{D1}}V_{\text{D2}}\rangle.\end{aligned}$$

Note that for $r = 0$ it is impossible to have more than one photon in the output mode, even for multiple photons in the input mode. Subsequently we perform polarization-sensitive detection on D$_1$ and D$_2$ in the basis of diagonal $|D\rangle \propto (|H\rangle + |V\rangle)$ and antidiagonal $|A\rangle \propto (|H\rangle - |V\rangle)$ linear polarization. This way we erase the information about the ancillary state and project the signal at the output port to

$$|\psi_{\text{out}}\rangle \propto \alpha r|0\rangle + \frac{3r^2-1}{2}\,(\beta_H|H\rangle + \beta_V|V\rangle)\,,$$

where we have incorporated the fact that only if both the detected polarizations on D$_1$ and D$_2$ are identical (DD or AA coincidences) the device heralds a successful amplification and thus only one half of the measurement outcomes contributes to success probability.

At this point we define the amplification gain G as a fraction between signal and vacuum probabilities

$$G = \frac{(3r^2-1)^2}{4r^2} \tag{1}$$

and calculate the corresponding success probability

$$P = r^2[|\alpha|^2 + G(|\beta_H|^2 + |\beta_V|^2)]. \tag{2}$$

Note that while the gain itself is input state independent, the success probability depends on both the gain and the input state parameters. This reflects the intuitive fact that it is for instance impossible to amplify a qubit that is actually not present in the input state ($\beta_H = \beta_V = 0$).

Let us analyze the results further. As expected the gain $G = 1$ is obtained for $r = 1$ with success probability $P = 1$

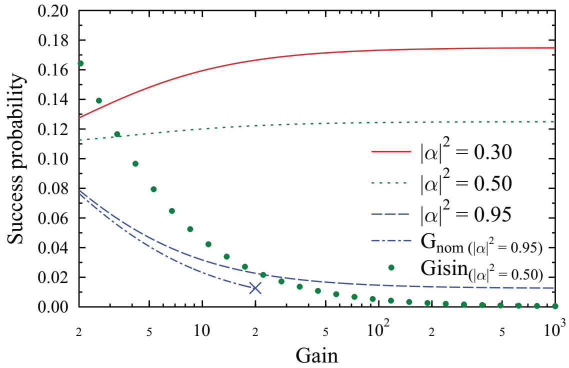


FIG. 2. (Color online) Success probability is depicted as a function of gain for three different input states parametrized by $|\alpha|^2$. For comparison, the success probability of the Gisin *et al.* scheme [13] is presented (in this case $|\alpha|^2 = 0.5$). Note that the success probability of our amplifier converges asymptotically to a nonzero value for any state with $|\alpha|^2 \neq 1$. Success probability is also plotted as a function of nominal gain G_{nom} for the case of $|\alpha|^2 = 0.95$. Note that according to its definition (3), the nominal gain is upper bounded by the value of 20 in this particular case (blue X symbol).

independent on the input state. On the other hand, an infinite gain is obtained for $r = 0$ with success probability of $P = (|\beta_H|^2 + |\beta_V|^2)/4$. In this particular case, it is however possible to increase the success probability twice by including also detection coincidences DA and AD accompanied by a feed-forward operation $V \to -V$ on the output state. Note that this regime is suitable for nondemolition presence detection of the qubit [22]. Figure 2 depicts the tradeoff between success probability and gain for three different input states containing different amounts of vacuum.

In a recent paper [12], its authors proposed also another measure of amplifier performance—the nominal gain G_{nom} defined as

$$G_{\text{nom}} \equiv \frac{G}{|\alpha|^2 + G(|\beta_H|^2 + |\beta_V|^2)} = \frac{r^2 G}{P}. \tag{3}$$

While the ordinary gain G describes how much the qubit to vacuum intensity ratio has been increased under the amplification procedure, the nominal gain shows how much the overall success probability of finding the qubit state has increased. For this reason, the nominal gain is bound by the inverse value of the initial qubit probability (e.g., for $|\beta_H|^2 + |\beta_V|^2 = 0.2$, the maximum value of nominal gain is 5 and in this case the vacuum state is completely eliminated). Figure 2 depicts the success probability as a function of nominal gain for one particular initial state ($|\alpha|^2 = 0.95$).

It is worth noting that in contrast to the Gisin *et al.* scheme [13], the success probability does not decrease asymptotically to 0 with increasing gain (also illustrated in Fig. 2 for comparison). One may however suggest that in the case of infinite gain, the scheme performs exactly as well as standard teleportation. While this is indeed true, standard teleportation does not allow us to tune the amplification gain and therefore the superposition of vacuum and qubit state collapses either onto vacuum or qubit state. In contrast, our scheme allows for the coherent superposition of these two terms to be maintained. Keeping coherence between vacuum and qubit terms is crucial for instance in all applications involving dual rail encoding.

III. AMPLIFICATION-BASED ENTANGLEMENT DISTILLATION

Quantum entanglement is one of the key ingredients in quantum communications. It can be used for teleportation [23], quantum cryptography [24], or remote state preparation [25]. It is also very sensitive to losses and decoherence occurring in the communication channel [26–28]. For this reason, entanglement distillation—the way of improving entanglement of a state subjected to some degradation—is a very important tool in quantum communications [29,30]. In this section we show how the amplifier can be used to distill entanglement on an example entangled state in dual-rail encoding.

Suppose an unknown polarization qubit $|\psi\rangle$ is distributed in two spatial modes creating thus maximally entangled state of the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\psi 0\rangle + |0\psi\rangle). \tag{4}$$

States of vacuum and qubit superposition are needed in various quantum communication protocols (e.g., quantum secret sharing [31]) and are indispensable in implementations combining spatial and polarization encoding [32–34]. Now let us consider a lossy channel with transmissivity $1 \geqslant T > 0$ used to distribute the second spatial mode of this entangled state. This channel would deteriorate the state to

$$\hat{\rho}(\alpha,p) = (1-p)|00\rangle\langle 00| + p|\Psi_\alpha\rangle\langle\Psi_\alpha|,$$

where

$$|\Psi_\alpha\rangle = \sqrt{\alpha}|0\psi\rangle + \sqrt{1-\alpha}|\psi 0\rangle,$$

with $\alpha = T/(T+1)$ and $p = (T+1)/2$. This state belongs to the class of amplitude damped states from Ref. [28] where the entanglement and nonlocality of such states was studied. Since various measures of entanglement have different operational meaning, below we consider amplification of a few popular entanglement measures analyzed in [28] (for a review on entanglement measures see [35]). The negativity (concurrence) of the mixed state before amplification is simply $N = \frac{T}{2}$ ($C = \sqrt{T}$). After the amplification in the lossy mode the parameters of the state $\hat{\rho}(\alpha,p)$ read $\alpha = GT/(GT+1)$ and $p = \mathcal{N}(GT+1)/2$, where G denotes the gain as defined in the previous section and $\mathcal{N} = 2/(2+GT-T)$. The entanglement of $\hat{\rho}(\alpha,p)$ (see Ref. [28]) can be quantified by its concurrence

$$C = 2p\sqrt{\alpha(1-\alpha)} = \mathcal{N}\sqrt{GT},$$

which can be further used to express its negativity as

$$\begin{aligned} N &= \frac{1}{2}[\sqrt{(1-p)^2 + C^2} - (1-p)] \\ &= \frac{\mathcal{N}}{2}[\sqrt{(1-T)^2 + 4GT} - (1-T)]. \end{aligned}$$

The third prominent measure of entanglement is the relative entropy of entanglement S, but as demonstrated by Miranowicz and Ishizaka [36] finding a closed formula for S in case of the amplitude-damped states requires solving a single variable

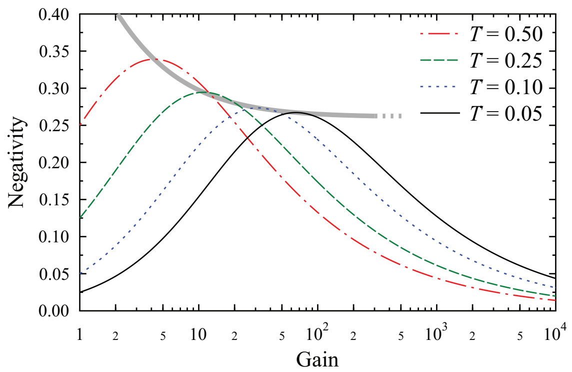


FIG. 3. (Color online) Negativity of entanglement depicted as a function of amplification gain for several different channel transmissivities T. A maximally entangled state formed of superposition of vacuum and qubit state is subjected to a channel with transmissivity T resulting in entanglement loss. Suitably set amplification gain can increase the amount of entanglement. The wide gray curve joins the maxima of negativity for all values of transmissivity T and subsequent optimal gains.

equation for which no general analytic solution is known. Hence we calculate S numerically as described in [28,36].

As shown on the example of negativity in Fig. 3 the entanglement measures are functions both of transmissivity T and gain G. The optimal gain for maximizing the entanglement is

$$G_{\mathrm{opt},N} = \frac{1}{T}[2 - T - \sqrt{2-T}(T-1)]$$

for negativity and $G_{\mathrm{opt},C} = (2-T)/T$ for concurrence. We do not present the exact expression for S and its optimal gain, but the $G_{\mathrm{opt,S}}$ curve obtained numerically is presented together with other G_{opt} curves in Fig. 4. The curves shown in Fig. 4 do not overlap, thus the optimal gain G_{opt} varies depending on the entanglement measure to be used. However, Fig. 4 suggests that for any value of $T > 0$, there is an optimal gain $G_{\mathrm{opt}} \geqslant \frac{1}{T}$ regardless of the applied entanglement measure. The entanglement measures before and after optimal amplification are depicted in Fig. 5 as functions of T. Note that for gain reaching infinity (standard teleportation), the entangled state would collapse onto the qubit state thus destroying the entanglement.

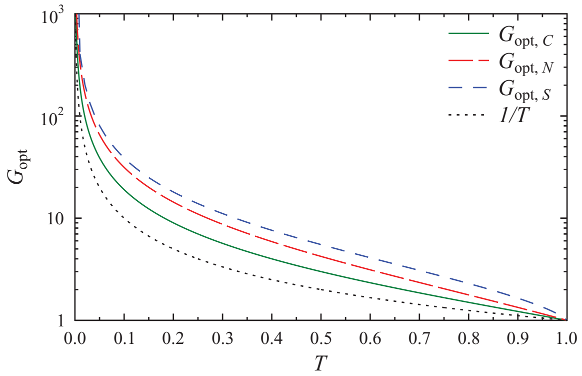


FIG. 4. (Color online) The optimal gain G_{opt} for various entanglement measures as function of channel transmissivity T. Setting the optimal gain allows to obtain the largest possible value of the selected entanglement measure for a given loss parametrized by T.

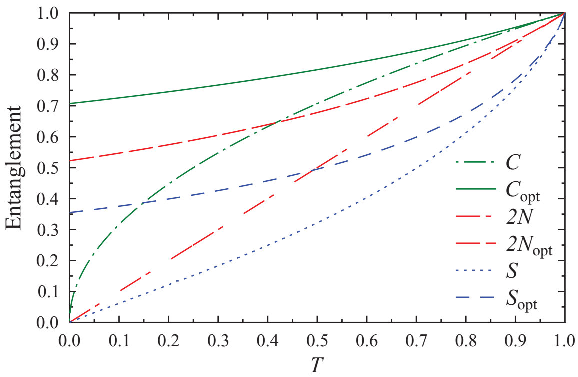


FIG. 5. (Color online) The entanglement measures before (C, N, S) and after (C_{opt}, N_{opt}, S_{opt}) optimal amplification as functions of channel transmissivity T.

The corresponding success probability of the amplification process is

$$P_{\mathrm{succ}} = \frac{r^2}{\mathcal{N}} = \frac{2G - 2\sqrt{G^2+3G}+3}{9\mathcal{N}},$$

where r follows from Eq. (1). In Fig. 3 we plot the amplified negativity as a function of the chosen gain for several different values of channel transmissivity. Note that our results for negativity, especially the expression for optimal gain $G_{\mathrm{opt},N}$, are also valid for logarithmic negativity $\log_2(2N+1)$ which is a concave function of N providing an upper bound to the distillable entanglement [37,38] given that the state was predistilled using the above-described procedure.

The above-performed calculations reveal how qubit amplification can be used for partial entanglement recovery. However in neither of the cases, the entanglement has been restored to the original maximum value due to the presence of the vacuum term $|00\rangle\langle 00|$. Recently, Mičuda *et al.* experimentally demonstrated a rather clever way to eliminate the presence of such a term [39]. They considered only vacuum and a fixed polarization single photon state, but the technique can be adopted for qubit amplification as well. Their approach is based on deliberate coherent attenuation before the state is transmitted via the lossy channel. This coherent attenuation is performed by subjecting the state to a beam splitter with transmissivity ν and subsequent postselection on vacuum in the ancillary mode. With the probability of ν, one can thus disbalance the original state (4) to $|\Psi\rangle \to |\Psi_\alpha\rangle$, where $\alpha = \nu/(\nu+1)$. The choice of attenuation factor ν influences the probability $p = (1-\nu T)/(1+\nu)$ and $\alpha = \nu T/(1-\nu T)$ in the density matrix $\hat{\rho}(\alpha,p)$ of the state $|\Psi_\alpha\rangle$ transmitted through the lossy channel. Subsequent amplification will increase α thus also the entanglement of the state. Ideally for $\nu \to 0$ and gain $G \to \infty$ the original negativity can be completely restored. Of course such parameters lead to zero success rate so there is a need for some sort of compromise. Nevertheless this

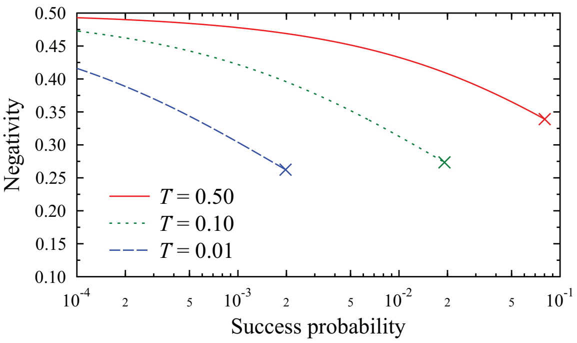


FIG. 6. (Color online) Negativity and success probability tradeoff obtained using coherent attenuation before transferring the state through a lossy channel. This tradeoff is depicted for three different values of channel transmissivity T. Even though this strategy allows us to increase the negativity arbitrarily close to $\frac{1}{2}$, the product of negativity and success probability is maximized when no coherent attenuation is used.

line of reasoning demonstrates the importance of amplification with high gain, where our amplifier outperforms the original Gisin *et al.* proposal [13].

The above mentioned compromise can be quantified using the entangling efficiency E_{eff} of the protocol [40]. The entangling efficiency is an entanglement generation measure suitable for probabilistic devices. In contrast to a more widely used entangling power [41–43], the entangling efficiency optimizes over the device parameters in order to maximize the product of success probability and negativity (or any other entanglement measure)

$$E_{\text{eff}} = \max\{P_{\text{succ}}N\}.$$

The negativity is calculated similarly as presented above using the analytical form of the density matrix. The success probability is composed of the success probability of attenuation (ν) and the success probability of amplification [Eq. (2)]. In order to find the best strategy, we perform a numerical simulation. The plot in Fig. 6 shows the tradeoff between negativity and success probability obtained when using the coherent attenuation strategy. This simulation also reveals that the product of success probability and negativity is maximized for $\nu = 1$ in all cases. So as far as the "entanglement rate" described by the entangling efficiency is concerned, the coherent attenuation does not offer any improvement. On the other hand, it is important to note that this strategy finds its merit when the goal is to achieve high negativity or high fidelity at the output.

IV. DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Photon amplifiers can find additional applications in device-independent quantum key distribution, a stronger form of entanglement-based quantum cryptography based on the violation of Bell's inequality [16]. As mentioned above, DI-QKD does not require any knowledge of Alice and Bob's measurement devices, but does require closing the detection loophole [44]. A number of ways of closing this loophole have been demonstrated, including using trapped ions [45,46] and efficient photon detection [17], but none has done so over the long distances needed for cryptography due to the intrinsic loss associated with photon transmission in fiber or free space. Gisin *et al.* recently proposed using a photon amplifier to herald incoming photons, closing the detection loophole and allowing DI-QKD [13]. In their scheme, as in the recently proposed improvements [14,15], a source of photons near Alice emits maximally entangled photon pairs. One photon is sent to Alice, which she detects directly with high efficiency, and the other photon is sent over a long channel to Bob. Bob routes the incoming photon through some heralded amplifier (e.g., the one proposed by Gisin *et al.* or by us) before detection, closing the detection loophole by performing a Bell measurement only upon successful amplification.

In order to compare the performance of the three previous amplifiers with ours, we performed numerical quantum optical simulations of the amplifiers. The initial source of entanglement was spontaneous-parametric down-conversion, with photon pair probability set to 2×10^{-3}, and both amplifiers used on-demand photon sources (two single photons for the Gisin *et al.* and Pitkanen *et al.* schemes and a maximally entangled Bell state for ours) as ancillae. To mirror a likely experimental scenario, we used bucket detectors with 95% detection efficiency and 91% coupling efficiency as herald-ing detectors, and untrusted noiseless photon-number resolving detectors with the same efficiency for the detection of the photons for the Bell test after heralding. The former are modeled on fast superconducting nanowire detectors [47] and the latter transition edge sensors [48]. We optimized all amplifiers over their tunable beam splitter reflectivity at each point. Finally we calculated the secure key rate per laser pulse from Eq. (11) of the Supplementary Material of Ref. [13]

$$R = \mu_{cc}\left[1 - h(Q) - I_E(S,\mu)\right], \tag{5}$$

where μ_{cc} is the probability of a conclusive event for both Alice and Bob, $h(Q)$ is the binary entropy function of the measured quantum bit error rate, and $I_E(S,\mu)$ is Eve's information based on the Bell inequality violation S and the ratio of inconclusive to conclusive results μ (see Eq. (23) of Ref. [13] for the full expression).

As shown in Fig. 7, our amplifier outperforms the Gisin *et al.* scheme and can also tolerate more dark counts in the heralding detectors. This is because high gain is required to close the detection loophole after a lossy channel, and, as seen above, the success probability of the Gisin *et al.* photon amplifier converges asymptotically to zero for high gain. It additionally outperforms the Pitkanen *et al.* scheme by a nearly constant factor, where this factor comes from improvements in success probability and the ratio of conclusive to inconclusive events after heralding. This is possible because in the Pitkanen *et al.* scheme, the elimination of the unwanted two-photon component even for ideal ancilla photons after heralding comes at the cost of vanishing success probability, a tradeoff our amplifier does not suffer from. The optimal key rate in this DI-QKD scenario for our amplifier occurs with $r = 0$ for all values of channel loss, such that it performs identically to the Curty and Moroder proposal [15]. However, there could be a regime (e.g., with noise in the final Bell test detectors) where

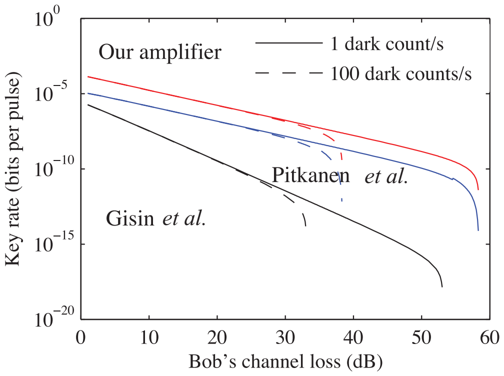


FIG. 7. (Color online) Key rate per laser pulse for device-independent quantum key distribution versus Bob's channel loss and dark counts per second in heralding detectors. Assuming 100 ps timing resolution in the heralding detectors leads to 10^{-10} and 10^{-8} dark count probability per pulse for 1 and 100 dark count/s, respectively. Our entangled photon amplifier allows more key to be extracted than the Gisin *et al.* scheme, and even shows better scaling with loss. It additionally delivers approximately 12 times the key rate of the Pitkanen *et al.* scheme.

higher success probability is needed to maximize key rate, at the cost of a larger vacuum component after the amplifier.

V. CONCLUSION

In this paper we have presented a linear-optical qubit amplifier. With the help of a maximally entangled photon pair, this device is able to change the ratio between vacuum and single qubit component, thus introducing qubit gain. In contrast to other proposals, our scheme achieves infinite gain with nonzero probability of success. Moreover, we have shown that the success probability of implementing infinite gain equals to the success probability of standard teleportation. To demonstrate the capabilities of our amplifier, we have presented two of its potential applications: entanglement distillation and quantum key distribution. First, the analysis of entanglement distillation reveals that our amplifier can at least partially improve entanglement deteriorated by lossy transmission. We have presented the calculation of optimal gain for three different measures of entanglement (negativity, concurrence, and relative entropy of entanglement) as a function of channel attenuation. Second, for device-independent quantum key distribution we have presented the significant improvement made by this amplifier over the previously proposed devices, including a key rate more than three orders of magnitude better for 100 km transmission distance. Practical implementation of the proposed scheme will be limited by available technology such as precision of optical components, detection efficiency, and delivery efficiency of ancillae.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the support by the Operational Program Research and Development for Innovations—European Regional Development Fund (Project No. CZ.1.05/2.1.00/03.0058). A.Č. acknowledges Project No. P205/12/0382 of Czech Science Foundation. K.B. and K.L. acknowledge support by Grant No. DEC-2011/03/B/ST2/01903 of the Polish National Science Centre and K.B. also by the Operational Program Education for Competitiveness—European Social Fund Project No. CZ.1.07/2.3.00/30.0041. M.B. acknowledges the financial support by Internal Grant Agency of Palacký University (No. PrF_2013_006). E.M.S. and T.J. acknowledge support from the Natural Sciences and Engineering Research Council of Canada. K.L. also acknowledges the support by the Czech Science Foundation (Grant No. 13-31000P). The authors thank Norbert Lütkenhaus for helpful suggestions.

[1] S. J. Wiesner, SIGACT News **15**, 78 (1983).

[2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2002).

[3] D. Bruß and G. Leuchs, *Lectures on Quantum Information* (Wiley-VCH, Berlin, 2006).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, Phys. Rev. Lett. **110**, 173601 (2013).

[6] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).

[7] S. Wang *et al.*, Opt. Lett. **37**, 1008 (2012).

[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[9] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[10] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, arXiv:1204.0738v3.

[11] Yang Liu *et al.*, arXiv:1209.6178v1.

[12] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, Nat. Phys. **9**, 23 (2013).

[13] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

[14] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus, Phys. Rev. A **84**, 022325 (2011).

[15] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).

[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[17] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, Nature (London) **497**, 227 (2013).

[18] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[19] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).

[20] A. Acín, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).

[21] E. Halenková, A. Černoch, K. Lemr, J. Soubusta, and S. Drusová, Appl. Opt. **51**, 474 (2012).

[22] M. Bula, K. Bartkiewicz, A. Černoch, and K. Lemr, Phys. Rev. A **87**, 033826 (2013).

[23] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[24] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[25] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Phys. Rev. Lett. **105**, 030407 (2010).

[26] Ş. K. Özdemir, K. Bartkiewicz, Y. X. Liu, and A. Miranowicz, Phys. Rev. A **76**, 042325 (2007).

[27] E. Halenková, K. Lemr, A. Černoch, and J. Soubusta, Phys. Rev. A **85**, 063807 (2012)

[28] B. Horst, K. Bartkiewicz, and A. Miranowicz, Phys. Rev. A **87**, 042108 (2013).

[29] T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **64**, 012304 (2001).

[30] Z. Zhao, J.-W. Pan, and M. S. Zhan, Phys. Rev. A **64**, 014301 (2001).

[31] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[32] K. Lemr, A. Černoch, J. Soubusta, and J. Fiurášek, Phys. Rev. A **81**, 012321 (2010).

[33] K. Lemr and A. Černoch, Opt. Commun. **300**, 282 (2013).

[34] K. Lemr, K. Bartkiewicz, A. Černoch, and J. Soubusta, Phys. Rev. A **87**, 062333 (2013).

[35] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[36] A. Miranowicz and S. Ishizaka, Phys. Rev. A **78**, 032310 (2008).

[37] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[38] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[39] M. Mičuda, I. Straka, M. Miková, M. Dušek, N. J. Cerf, J. Fiurášek, and M. Ježek, Phys. Rev. Lett. **109**, 180503 (2012).

[40] K. Lemr, A. Černoch, J. Soubusta, and M. Dušek, Phys. Rev. A **86**, 032321 (2012).

[41] P. Zanardi, Ch. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301(R) (2000).

[42] M. M. Wolf, J. Eisert, and M. B. Plenio, Phys. Rev. Lett. **90**, 047904 (2003).

[43] J. Batle, M. Casas, A. Plastino, and A. R. Plastino, Opt. Spectrosc. **99**, 371 (2005).

[44] P. Pearle, Phys. Rev. D **2**, 1418 (1970).

[45] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature (London) **409**, 791 (2001).

[46] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, Phys. Rev. Lett. **100**, 150404 (2008).

[47] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photon. **7**, 210 (2013).

[48] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).

Entanglement-based linear-optical qubit amplifier

Evan Meyer-Scott,[1] Marek Bula,[2] Karol Bartkiewicz,[2,*] Antonín Černoch,[3] Jan Soubusta,[3]
Thomas Jennewein,[1] and Karel Lemr[3,†]

[1] *Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo,*
200 University Avenue W, Waterloo, Ontario, Canada N2L 3G1

[2] *RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic,*
17. listopadu 12, 771 46 Olomouc, Czech Republic

[3] *Institute of Physics of Academy of Sciences of the Czech Republic, Joint Laboratory of Optics of PU and IP AS CR, 17. listopadu 50A,*
772 07 Olomouc, Czech Republic

(Received 6 June 2013; published 26 July 2013)

We propose a linear-optical scheme for an efficient amplification of a photonic qubit based on interaction of the signal mode with a pair of entangled ancillae. In contrast to a previous proposal for qubit amplifier by Gisin *et al.* [Phys Rev. Lett. **105**, 070501 (2010)], the success probability of our device does not decrease asymptotically to zero with increasing gain. Moreover, we show how the device can be used to restore entanglement deteriorated by transmission over a lossy channel and calculate the secure key rate for device-independent quantum key distribution.

DOI: 10.1103/PhysRevA.88.012327 PACS number(s): 03.67.Hk, 42.50.Dv, 03.67.Lx

I. INTRODUCTION

The fundamentals of quantum physics were discovered and formulated nearly a hundred years ago. Three decades ago scientists postulated that the laws of quantum physics could be used to improve capabilities of computation and communication technologies [1]. This idea sparked intense research resulting in the discovery of many quantum information protocols, some of them even with practical, modern implementations [2,3].

One such application of quantum information is quantum cryptography, comprising various quantum key distribution protocols (QKD) [4]. QKD offers unconditional security of private communications certified by the laws of quantum physics. In the real world, QKD suffers from various technological limits, especially the need to trust imperfect detectors and single photon sources, quantum channel losses, and background noise. The latter effects limit the maximum distance for unconditionally secure communications [5]. Long-distance QKD has been realized over 144 km in free-space [6] and over 260 km in an optical fiber [7]. Trust in the imperfect devices used for cryptography allows eavesdroppers to attack unintended leakages of information or control detectors, known as side channels [8].

The side channel attacks can be solved in principle by using Bell-state projection measurements or using entanglement-based protocols. The simpler approach is measurement-device-independent QKD [9–11]. In this case a projection on a Bell state in the middle of the communication line removes all detector side channels. The more complete approach is device-independent QKD (DI-QKD) [12–16] and its security is based on the loophole-free violation of a Bell inequality. DI-QKD removes all source and detector side channels but requires closing of the detector (high-efficiency detection) and locality (distant detectors) loopholes, which has not yet been achieved simultaneously [17].

For DI-QKD and other protocols requiring high-efficiency detection, a method is required to circumvent the channel losses inherent in photon transmission. In classical optical communication networks the problem of losses is solved using amplifiers of the classical signal. For quantum communication, losses are more fundamental. The quantum signals are stored in polarization or temporal modes of individual photons and any quantum amplifier is bound by the quantum limits like the no-cloning theorem [18]. Several proposals of quantum amplifiers were recently introduced, wherein the quantum limit can be circumvented by making the amplification nondeterministic. This type of amplification is called heralded noiseless amplification [19] and is already seeing successful implementation [12]. Note that there exists a complete equivalence between distribution of two-qubit entanglement and secure key distribution [20]. In other words, any quantum channel is capable of secret communication if and only if it is capable of distributing entanglement.

In this article we propose a scheme of a linear-optical qubit amplifier that can restore the attenuated qubit and is also capable of distilling deteriorated entanglement of the qubit state. Our amplifier is ready to be used in DI-QKD schemes. Moreover, it outperforms previously published proposals. In contrast to the Gisin *et al.* scheme [13], the success probability of our device does not asymptotically approach zero when increasing the amplification gain. Furthermore, in comparison to the Pitkanen *et al.* scheme [14], our device provides tunable gain and for the case of infinite gain allows better success probability due to its intrinsic elimination of the two-photon component after heralding. However, the Pitkanen *et al.* device may perform better when using a probabilistic source for the ancilla photons, due to its extra stage of heralding. The scheme by Curty and Moroder makes use of entanglement as in our device, but it is limited to infinite gain only [15], and in this regime it performs comparably to our device. Further to these works, we present a thorough investigation of the gain versus

[*] bartkiewicz@jointlab.upol.cz

[†] k.lemr@upol.cz

success probability tradeoff which is a crucial figure of merit for probabilistic amplifiers.

The paper is organized as follows. The principle of the amplifier operation is explained in Sec. II. The entanglement distillation is analyzed in Sec. III and DI-QKD is discussed in Sec. IV. Conclusions are drawn in the final Sec. V.

II. PRINCIPLE OF OPERATION

The amplifier (depicted in Fig. 1) consists of four polarizing beam splitters. Two of them ($\mathrm{PBS_{in}}$ and $\mathrm{PBS_{out}}$) form a Mach-Zehnder interferometer between signal input port "in" and output port "out." These polarizing beam splitters totally transmit horizontally polarized light while totally reflect light with vertical polarization. The other two are partially polarizing beam splitters, denoted as $\mathrm{PPBS_1}$ and $\mathrm{PPBS_2}$, and placed in their respective arms of the interferometer. $\mathrm{PPBS_1}$ reflects vertically polarized light, while having reflectivity r for horizontal polarization. In terms of creation operators this transformation reads

$$\begin{aligned}\hat{a}^\dagger_{\mathrm{in},H} &\to r\hat{a}^\dagger_{\mathrm{out},H} + \sqrt{1-r^2}\hat{a}^\dagger_{\mathrm{D1},H},\\ \hat{a}^\dagger_{a1,H} &\to -r\hat{a}^\dagger_{\mathrm{D1},H} + \sqrt{1-r^2}\hat{a}^\dagger_{\mathrm{out},H},\\ \hat{a}^\dagger_{a1,V} &\to -\hat{a}^\dagger_{\mathrm{D1},V},\end{aligned}$$

where labeling of spatial modes has been adopted from Fig. 1 and H, V denote horizontal and vertical polarizations. Similarly the $\mathrm{PPBS_2}$ reflects completely the horizontal polarization and with reflectivity r it reflects vertically polarized photons. The parameter r is to be tuned as explained below. Successful operation of the amplifier is heralded by two-photon coincidence detection on detection blocks $\mathrm{D_1}$ and $\mathrm{D_2}$.

To demonstrate the principle of operation, let us assume the input signal to be a coherent superposition of vacuum and a polarization-encoded single photon qubit

$$|\psi_{\mathrm{in}}\rangle = \alpha|0\rangle + \beta_H|H\rangle + \beta_V|V\rangle,$$

where $|0\rangle$ denotes vacuum, $|H\rangle$, $|V\rangle$ denote horizontal and vertical polarization states, respectively, and the coefficients meet the normalization condition $|\alpha|^2 + |\beta_H|^2 + |\beta_V|^2 = 1$.

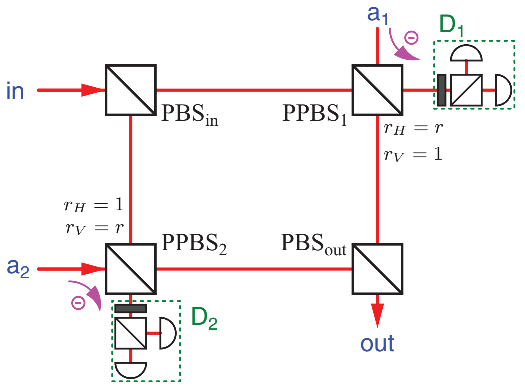


FIG. 1. (Color online) Scheme for entanglement-based linear-optical qubit amplifier as described in the text. $\mathrm{D_1}$ and $\mathrm{D_2}$ are standard polarization analysis detection blocks (for reference see [21]).

The amplifier makes also use of a pair of ancillary photons impinging on ports a_1 and a_2 of $\mathrm{PPBS_1}$ and $\mathrm{PPBS_2}$, respectively. These ancillary photons are initially in a maximally entangled Bell state of the form

$$|\Phi^+_{a_1a_2}\rangle = \frac{1}{\sqrt{2}}(|H_{a_1}H_{a_2}\rangle + |V_{a_1}V_{a_2}\rangle),$$

where the indices denote the ancillary photons' spatial modes.

The total state entering the amplifier composed of the signal and ancillary photons reads

$$\begin{aligned}|\psi_T\rangle &= |\psi_{\mathrm{in}}\rangle \otimes |\Phi^+_{a_1a_2}\rangle\\ &= \frac{1}{\sqrt{2}}[\alpha|0_{\mathrm{in}}H_{a1}H_{a2}\rangle + \alpha|0_{\mathrm{in}}V_{a1}V_{a2}\rangle\\ &\quad + \beta_H|H_{\mathrm{in}}H_{a1}H_{a2}\rangle + \beta_H|H_{\mathrm{in}}V_{a1}V_{a2}\rangle\\ &\quad + \beta_V|V_{\mathrm{in}}H_{a1}H_{a2}\rangle + \beta_V|V_{\mathrm{in}}V_{a1}V_{a2}\rangle].\end{aligned}$$

Now we inspect evolution of all the individual terms present in the previous equation. Since the successful operation of the amplifier is conditioned by a two-photon coincidence detection by $\mathrm{D_1}$ and $\mathrm{D_2}$ we postselect only such cases:

$$\begin{aligned}|0_{\mathrm{in}}H_{a1}H_{a2}\rangle &\to r|0_{\mathrm{out}}H_{\mathrm{D1}}H_{\mathrm{D2}}\rangle,\\ |0_{\mathrm{in}}V_{a1}V_{a2}\rangle &\to r|0_{\mathrm{out}}V_{\mathrm{D1}}V_{\mathrm{D2}}\rangle,\\ |H_{\mathrm{in}}H_{a1}H_{a2}\rangle &\to (2r^2-1)|H_{\mathrm{out}}H_{\mathrm{D1}}H_{\mathrm{D2}}\rangle,\\ |H_{\mathrm{in}}V_{a1}V_{a2}\rangle &\to r^2|H_{\mathrm{out}}V_{\mathrm{D1}}V_{\mathrm{D2}}\rangle,\\ |V_{\mathrm{in}}H_{a1}H_{a2}\rangle &\to r^2|V_{\mathrm{out}}H_{\mathrm{D1}}H_{\mathrm{D2}}\rangle,\\ |V_{\mathrm{in}}V_{a1}V_{a2}\rangle &\to (2r^2-1)|V_{\mathrm{out}}V_{\mathrm{D1}}V_{\mathrm{D2}}\rangle.\end{aligned}$$

Note that for $r = 0$ it is impossible to have more than one photon in the output mode, even for multiple photons in the input mode. Subsequently we perform polarization-sensitive detection on $\mathrm{D_1}$ and $\mathrm{D_2}$ in the basis of diagonal $|D\rangle \propto (|H\rangle + |V\rangle)$ and antidiagonal $|A\rangle \propto (|H\rangle - |V\rangle)$ linear polarization. This way we erase the information about the ancillary state and project the signal at the output port to

$$|\psi_{\mathrm{out}}\rangle \propto \alpha r|0\rangle + \frac{3r^2-1}{2}(\beta_H|H\rangle + \beta_V|V\rangle),$$

where we have incorporated the fact that only if both the detected polarizations on $\mathrm{D_1}$ and $\mathrm{D_2}$ are identical (DD or AA coincidences) the device heralds a successful amplification and thus only one half of the measurement outcomes contributes to success probability.

At this point we define the amplification gain G as a fraction between signal and vacuum probabilities

$$G = \frac{(3r^2-1)^2}{4r^2} \tag{1}$$

and calculate the corresponding success probability

$$P = r^2[|\alpha|^2 + G(|\beta_H|^2 + |\beta_V|^2)]. \tag{2}$$

Note that while the gain itself is input state independent, the success probability depends on both the gain and the input state parameters. This reflects the intuitive fact that it is for instance impossible to amplify a qubit that is actually not present in the input state ($\beta_H = \beta_V = 0$).

Let us analyze the results further. As expected the gain $G = 1$ is obtained for $r = 1$ with success probability $P = 1$

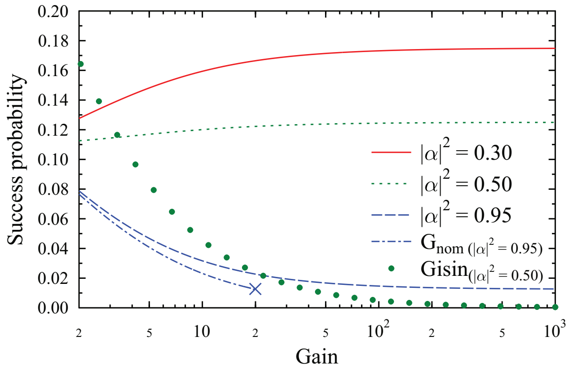


FIG. 2. (Color online) Success probability is depicted as a function of gain for three different input states parametrized by $|\alpha|^2$. For comparison, the success probability of the Gisin *et al.* scheme [13] is presented (in this case $|\alpha|^2 = 0.5$). Note that the success probability of our amplifier converges asymptotically to a nonzero value for any state with $|\alpha|^2 \neq 1$. Success probability is also plotted as a function of nominal gain G_{nom} for the case of $|\alpha|^2 = 0.95$. Note that according to its definition (3), the nominal gain is upper bounded by the value of 20 in this particular case (blue X symbol).

independent on the input state. On the other hand, an infinite gain is obtained for $r = 0$ with success probability of $P = (|\beta_H|^2 + |\beta_V|^2)/4$. In this particular case, it is however possible to increase the success probability twice by including also detection coincidences DA and AD accompanied by a feed-forward operation $V \rightarrow -V$ on the output state. Note that this regime is suitable for nondemolition presence detection of the qubit [22]. Figure 2 depicts the tradeoff between success probability and gain for three different input states containing different amounts of vacuum.

In a recent paper [12], its authors proposed also another measure of amplifier performance—the nominal gain G_{nom} defined as

$$G_{\text{nom}} \equiv \frac{G}{|\alpha|^2 + G(|\beta_H|^2 + |\beta_V|^2)} = \frac{r^2 G}{P}. \tag{3}$$

While the ordinary gain G describes how much the qubit to vacuum intensity ratio has been increased under the amplification procedure, the nominal gain shows how much the overall success probability of finding the qubit state has increased. For this reason, the nominal gain is bound by the inverse value of the initial qubit probability (e.g., for $|\beta_H|^2 + |\beta_V|^2 = 0.2$, the maximum value of nominal gain is 5 and in this case the vacuum state is completely eliminated). Figure 2 depicts the success probability as a function of nominal gain for one particular initial state ($|\alpha|^2 = 0.95$).

It is worth noting that in contrast to the Gisin *et al.* scheme [13], the success probability does not decrease asymptotically to 0 with increasing gain (also illustrated in Fig. 2 for comparison). One may however suggest that in the case of infinite gain, the scheme performs exactly as well as standard teleportation. While this is indeed true, standard teleportation does not allow us to tune the amplification gain and therefore the superposition of vacuum and qubit state collapses either onto vacuum or qubit state. In contrast, our scheme allows for the coherent superposition of these two terms to be maintained. Keeping coherence between vacuum and qubit terms is crucial for instance in all applications involving dual rail encoding.

III. AMPLIFICATION-BASED ENTANGLEMENT DISTILLATION

Quantum entanglement is one of the key ingredients in quantum communications. It can be used for teleportation [23], quantum cryptography [24], or remote state preparation [25]. It is also very sensitive to losses and decoherence occurring in the communication channel [26–28]. For this reason, entanglement distillation—the way of improving entanglement of a state subjected to some degradation—is a very important tool in quantum communications [29,30]. In this section we show how the amplifier can be used to distill entanglement on an example entangled state in dual-rail encoding.

Suppose an unknown polarization qubit $|\psi\rangle$ is distributed in two spatial modes creating thus maximally entangled state of the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\psi 0\rangle + |0\psi\rangle). \tag{4}$$

States of vacuum and qubit superposition are needed in various quantum communication protocols (e.g., quantum secret sharing [31]) and are indispensable in implementations combining spatial and polarization encoding [32–34]. Now let us consider a lossy channel with transmissivity $1 \geqslant T > 0$ used to distribute the second spatial mode of this entangled state. This channel would deteriorate the state to

$$\hat{\rho}(\alpha,p) = (1-p)|00\rangle\langle 00| + p|\Psi_\alpha\rangle\langle\Psi_\alpha|,$$

where

$$|\Psi_\alpha\rangle = \sqrt{\alpha}|0\psi\rangle + \sqrt{1-\alpha}|\psi 0\rangle,$$

with $\alpha = T/(T+1)$ and $p = (T+1)/2$. This state belongs to the class of amplitude damped states from Ref. [28] where the entanglement and nonlocality of such states was studied. Since various measures of entanglement have different operational meaning, below we consider amplification of a few popular entanglement measures analyzed in [28] (for a review on entanglement measures see [35]). The negativity (concurrence) of the mixed state before amplification is simply $N = \frac{T}{2}$ ($C = \sqrt{T}$). After the amplification in the lossy mode the parameters of the state $\hat{\rho}(\alpha,p)$ read $\alpha = GT/(GT+1)$ and $p = \mathcal{N}(GT+1)/2$, where G denotes the gain as defined in the previous section and $\mathcal{N} = 2/(2+GT-T)$. The entanglement of $\hat{\rho}(\alpha,p)$ (see Ref. [28]) can be quantified by its concurrence

$$C = 2p\sqrt{\alpha(1-\alpha)} = \mathcal{N}\sqrt{GT},$$

which can be further used to express its negativity as

$$\begin{aligned} N &= \frac{1}{2}[\sqrt{(1-p)^2 + C^2} - (1-p)] \\ &= \frac{\mathcal{N}}{2}[\sqrt{(1-T)^2 + 4GT} - (1-T)]. \end{aligned}$$

The third prominent measure of entanglement is the relative entropy of entanglement S, but as demonstrated by Miranowicz and Ishizaka [36] finding a closed formula for S in case of the amplitude-damped states requires solving a single variable

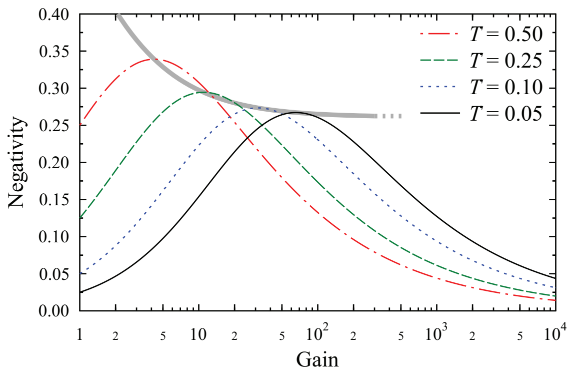


FIG. 3. (Color online) Negativity of entanglement depicted as a function of amplification gain for several different channel transmissivities T. A maximally entangled state formed of superposition of vacuum and qubit state is subjected to a channel with transmissivity T resulting in entanglement loss. Suitably set amplification gain can increase the amount of entanglement. The wide gray curve joins the maxima of negativity for all values of transmissivity T and subsequent optimal gains.

equation for which no general analytic solution is known. Hence we calculate S numerically as described in [28,36].

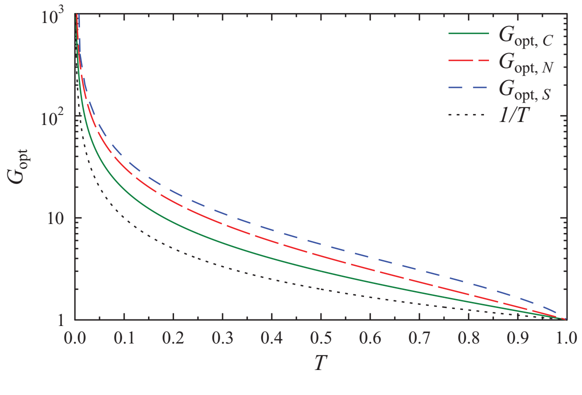


FIG. 4. (Color online) The optimal gain G_{opt} for various entanglement measures as function of channel transmissivity T. Setting the optimal gain allows to obtain the largest possible value of the selected entanglement measure for a given loss parametrized by T.

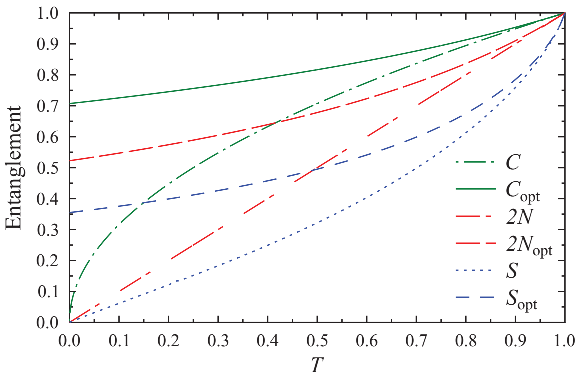


FIG. 5. (Color online) The entanglement measures before (C, N, S) and after (C_{opt}, N_{opt}, S_{opt}) optimal amplification as functions of channel transmissivity T.

As shown on the example of negativity in Fig. 3 the entanglement measures are functions both of transmissivity T and gain G. The optimal gain for maximizing the entanglement is

$$G_{\text{opt},N} = \frac{1}{T}[2 - T - \sqrt{2-T}(T-1)]$$

for negativity and $G_{\text{opt},C} = (2-T)/T$ for concurrence. We do not present the exact expression for S and its optimal gain, but the $G_{\text{opt,S}}$ curve obtained numerically is presented together with other G_{opt} curves in Fig. 4. The curves shown in Fig. 4 do not overlap, thus the optimal gain G_{opt} varies depending on the entanglement measure to be used. However, Fig. 4 suggests that for any value of $T > 0$, there is an optimal gain $G_{\text{opt}} \geqslant \frac{1}{T}$ regardless of the applied entanglement measure. The entanglement measures before and after optimal amplification are depicted in Fig. 5 as functions of T. Note that for gain reaching infinity (standard teleportation), the entangled state would collapse onto the qubit state thus destroying the entanglement.

The corresponding success probability of the amplification process is

$$P_{\text{succ}} = \frac{r^2}{\mathcal{N}} = \frac{2G - 2\sqrt{G^2 + 3G} + 3}{9\mathcal{N}},$$

where r follows from Eq. (1). In Fig. 3 we plot the amplified negativity as a function of the chosen gain for several different values of channel transmissivity. Note that our results for negativity, especially the expression for optimal gain $G_{\text{opt},N}$, are also valid for logarithmic negativity $\log_2(2N+1)$ which is a concave function of N providing an upper bound to the distillable entanglement [37,38] given that the state was predistilled using the above-described procedure.

The above-performed calculations reveal how qubit amplification can be used for partial entanglement recovery. However in neither of the cases, the entanglement has been restored to the original maximum value due to the presence of the vacuum term $|00\rangle\langle 00|$. Recently, Mičuda *et al.* experimentally demonstrated a rather clever way to eliminate the presence of such a term [39]. They considered only vacuum and a fixed polarization single photon state, but the technique can be adopted for qubit amplification as well. Their approach is based on deliberate coherent attenuation before the state is transmitted via the lossy channel. This coherent attenuation is performed by subjecting the state to a beam splitter with transmissivity ν and subsequent postselection on vacuum in the ancillary mode. With the probability of ν, one can thus disbalance the original state (4) to $|\Psi\rangle \to |\Psi_\alpha\rangle$, where $\alpha = \nu/(\nu+1)$. The choice of attenuation factor ν influences the probability $p = (1-\nu T)/(1+\nu)$ and $\alpha = \nu T/(1-\nu T)$ in the density matrix $\hat{\rho}(\alpha,p)$ of the state $|\Psi_\alpha\rangle$ transmitted through the lossy channel. Subsequent amplification will increase α thus also the entanglement of the state. Ideally for $\nu \to 0$ and gain $G \to \infty$ the original negativity can be completely restored. Of course such parameters lead to zero success rate so there is a need for some sort of compromise. Nevertheless this

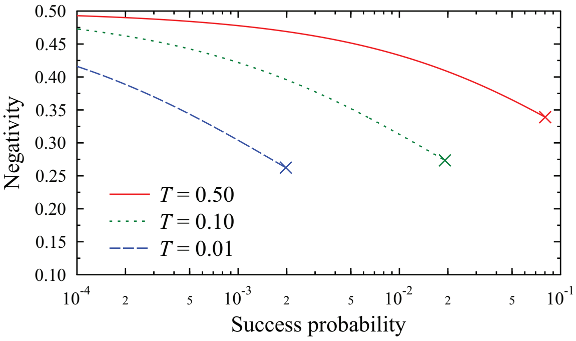


FIG. 6. (Color online) Negativity and success probability tradeoff obtained using coherent attenuation before transferring the state through a lossy channel. This tradeoff is depicted for three different values of channel transmissivity T. Even though this strategy allows us to increase the negativity arbitrarily close to $\frac{1}{2}$, the product of negativity and success probability is maximized when no coherent attenuation is used.

line of reasoning demonstrates the importance of amplification with high gain, where our amplifier outperforms the original Gisin *et al.* proposal [13].

The above mentioned compromise can be quantified using the entangling efficiency E_{eff} of the protocol [40]. The entangling efficiency is an entanglement generation measure suitable for probabilistic devices. In contrast to a more widely used entangling power [41–43], the entangling efficiency optimizes over the device parameters in order to maximize the product of success probability and negativity (or any other entanglement measure)

$$E_{\text{eff}} = \max\{P_{\text{succ}} N\}.$$

The negativity is calculated similarly as presented above using the analytical form of the density matrix. The success probability is composed of the success probability of attenuation (ν) and the success probability of amplification [Eq. (2)]. In order to find the best strategy, we perform a numerical simulation. The plot in Fig. 6 shows the tradeoff between negativity and success probability obtained when using the coherent attenuation strategy. This simulation also reveals that the product of success probability and negativity is maximized for $\nu = 1$ in all cases. So as far as the "entanglement rate" described by the entangling efficiency is concerned, the coherent attenuation does not offer any improvement. On the other hand, it is important to note that this strategy finds its merit when the goal is to achieve high negativity or high fidelity at the output.

IV. DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Photon amplifiers can find additional applications in device-independent quantum key distribution, a stronger form of entanglement-based quantum cryptography based on the violation of Bell's inequality [16]. As mentioned above, DI-QKD does not require any knowledge of Alice and Bob's measurement devices, but does require closing the detection loophole [44]. A number of ways of closing this loophole have been demonstrated, including using trapped ions [45,46] and efficient photon detection [17], but none has done so over the long distances needed for cryptography due to the intrinsic loss associated with photon transmission in fiber or free space. Gisin *et al.* recently proposed using a photon amplifier to herald incoming photons, closing the detection loophole and allowing DI-QKD [13]. In their scheme, as in the recently proposed improvements [14,15], a source of photons near Alice emits maximally entangled photon pairs. One photon is sent to Alice, which she detects directly with high efficiency, and the other photon is sent over a long channel to Bob. Bob routes the incoming photon through some heralded amplifier (e.g., the one proposed by Gisin *et al.* or by us) before detection, closing the detection loophole by performing a Bell measurement only upon successful amplification.

In order to compare the performance of the three previous amplifiers with ours, we performed numerical quantum optical simulations of the amplifiers. The initial source of entanglement was spontaneous-parametric down-conversion, with photon pair probability set to 2×10^{-3}, and both amplifiers used on-demand photon sources (two single photons for the Gisin *et al.* and Pitkanen *et al.* schemes and a maximally entangled Bell state for ours) as ancillae. To mirror a likely experimental scenario, we used bucket detectors with 95% detection efficiency and 91% coupling efficiency as herald-ing detectors, and untrusted noiseless photon-number resolving detectors with the same efficiency for the detection of the photons for the Bell test after heralding. The former are modeled on fast superconducting nanowire detectors [47] and the latter transition edge sensors [48]. We optimized all amplifiers over their tunable beam splitter reflectivity at each point. Finally we calculated the secure key rate per laser pulse from Eq. (11) of the Supplementary Material of Ref. [13]

$$R = \mu_{cc}\,[1 - h(Q) - I_E(S,\mu)]\,, \tag{5}$$

where μ_{cc} is the probability of a conclusive event for both Alice and Bob, $h(Q)$ is the binary entropy function of the measured quantum bit error rate, and $I_E(S,\mu)$ is Eve's information based on the Bell inequality violation S and the ratio of inconclusive to conclusive results μ (see Eq. (23) of Ref. [13] for the full expression).

As shown in Fig. 7, our amplifier outperforms the Gisin *et al.* scheme and can also tolerate more dark counts in the heralding detectors. This is because high gain is required to close the detection loophole after a lossy channel, and, as seen above, the success probability of the Gisin *et al.* photon amplifier converges asymptotically to zero for high gain. It additionally outperforms the Pitkanen *et al.* scheme by a nearly constant factor, where this factor comes from improvements in success probability and the ratio of conclusive to inconclusive events after heralding. This is possible because in the Pitkanen *et al.* scheme, the elimination of the unwanted two-photon component even for ideal ancilla photons after heralding comes at the cost of vanishing success probability, a tradeoff our amplifier does not suffer from. The optimal key rate in this DI-QKD scenario for our amplifier occurs with $r = 0$ for all values of channel loss, such that it performs identically to the Curty and Moroder proposal [15]. However, there could be a regime (e.g., with noise in the final Bell test detectors) where

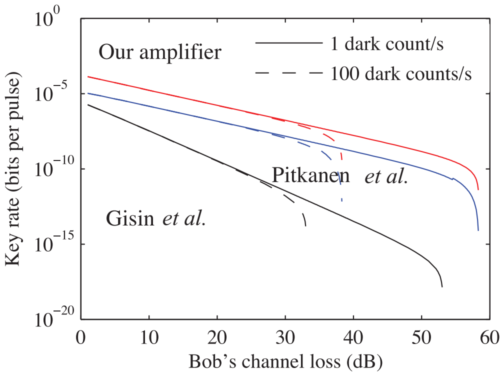


FIG. 7. (Color online) Key rate per laser pulse for device-independent quantum key distribution versus Bob's channel loss and dark counts per second in heralding detectors. Assuming 100 ps timing resolution in the heralding detectors leads to 10^{-10} and 10^{-8} dark count probability per pulse for 1 and 100 dark count/s, respectively. Our entangled photon amplifier allows more key to be extracted than the Gisin *et al.* scheme, and even shows better scaling with loss. It additionally delivers approximately 12 times the key rate of the Pitkanen *et al.* scheme.

higher success probability is needed to maximize key rate, at the cost of a larger vacuum component after the amplifier.

V. CONCLUSION

In this paper we have presented a linear-optical qubit amplifier. With the help of a maximally entangled photon pair, this device is able to change the ratio between vacuum and single qubit component, thus introducing qubit gain. In contrast to other proposals, our scheme achieves infinite gain with nonzero probability of success. Moreover, we have shown that the success probability of implementing infinite gain equals to the success probability of standard teleportation. To demonstrate the capabilities of our amplifier, we have presented two of its potential applications: entanglement distillation and quantum key distribution. First, the analysis of entanglement distillation reveals that our amplifier can at least partially improve entanglement deteriorated by lossy transmission. We have presented the calculation of optimal gain for three different measures of entanglement (negativity, concurrence, and relative entropy of entanglement) as a function of channel attenuation. Second, for device-independent quantum key distribution we have presented the significant improvement made by this amplifier over the previously proposed devices, including a key rate more than three orders of magnitude better for 100 km transmission distance. Practical implementation of the proposed scheme will be limited by available technology such as precision of optical components, detection efficiency, and delivery efficiency of ancillae.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the support by the Operational Program Research and Development for Innovations—European Regional Development Fund (Project No. CZ.1.05/2.1.00/03.0058). A.Č. acknowledges Project No. P205/12/0382 of Czech Science Foundation. K.B. and K.L. acknowledge support by Grant No. DEC-2011/03/B/ST2/01903 of the Polish National Science Centre and K.B. also by the Operational Program Education for Competitiveness—European Social Fund Project No. CZ.1.07/2.3.00/30.0041. M.B. acknowledges the financial support by Internal Grant Agency of Palacký University (No. PrF_2013_006). E.M.S. and T.J. acknowledge support from the Natural Sciences and Engineering Research Council of Canada. K.L. also acknowledges the support by the Czech Science Foundation (Grant No. 13-31000P). The authors thank Norbert Lütkenhaus for helpful suggestions.

[1] S. J. Wiesner, SIGACT News **15**, 78 (1983).
[2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2002).
[3] D. Bruß and G. Leuchs, *Lectures on Quantum Information* (Wiley-VCH, Berlin, 2006).
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[5] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, Phys. Rev. Lett. **110**, 173601 (2013).
[6] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).
[7] S. Wang *et al.*, Opt. Lett. **37**, 1008 (2012).
[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[9] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[10] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, arXiv:1204.0738v3.
[11] Yang Liu *et al.*, arXiv:1209.6178v1.
[12] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, Nat. Phys. **9**, 23 (2013).
[13] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[14] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus, Phys. Rev. A **84**, 022325 (2011).
[15] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).
[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[17] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, Nature (London) **497**, 227 (2013).
[18] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[19] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).
[20] A. Acín, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).
[21] E. Halenková, A. Černoch, K. Lemr, J. Soubusta, and S. Drusová, Appl. Opt. **51**, 474 (2012).
[22] M. Bula, K. Bartkiewicz, A. Černoch, and K. Lemr, Phys. Rev. A **87**, 033826 (2013).

[23] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[24] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[25] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Phys. Rev. Lett. **105**, 030407 (2010).

[26] Ş. K. Özdemir, K. Bartkiewicz, Y. X. Liu, and A. Miranowicz, Phys. Rev. A **76**, 042325 (2007).

[27] E. Halenková, K. Lemr, A. Černoch, and J. Soubusta, Phys. Rev. A **85**, 063807 (2012)

[28] B. Horst, K. Bartkiewicz, and A. Miranowicz, Phys. Rev. A **87**, 042108 (2013).

[29] T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **64**, 012304 (2001).

[30] Z. Zhao, J.-W. Pan, and M. S. Zhan, Phys. Rev. A **64**, 014301 (2001).

[31] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[32] K. Lemr, A. Černoch, J. Soubusta, and J. Fiurášek, Phys. Rev. A **81**, 012321 (2010).

[33] K. Lemr and A. Černoch, Opt. Commun. **300**, 282 (2013).

[34] K. Lemr, K. Bartkiewicz, A. Černoch, and J. Soubusta, Phys. Rev. A **87**, 062333 (2013).

[35] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[36] A. Miranowicz and S. Ishizaka, Phys. Rev. A **78**, 032310 (2008).

[37] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[38] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[39] M. Mičuda, I. Straka, M. Miková, M. Dušek, N. J. Cerf, J. Fiurášek, and M. Ježek, Phys. Rev. Lett. **109**, 180503 (2012).

[40] K. Lemr, A. Černoch, J. Soubusta, and M. Dušek, Phys. Rev. A **86**, 032321 (2012).

[41] P. Zanardi, Ch. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301(R) (2000).

[42] M. M. Wolf, J. Eisert, and M. B. Plenio, Phys. Rev. Lett. **90**, 047904 (2003).

[43] J. Batle, M. Casas, A. Plastino, and A. R. Plastino, Opt. Spectrosc. **99**, 371 (2005).

[44] P. Pearle, Phys. Rev. D **2**, 1418 (1970).

[45] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature (London) **409**, 791 (2001).

[46] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, Phys. Rev. Lett. **100**, 150404 (2008).

[47] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photon. **7**, 210 (2013).

[48] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).