VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV FYZIKÁLNÍHO INŽENÝRSTVÍ
FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF PHYSICAL ENGINEERING

GENEROVÁNÍ NÁHODNÝCH ČÍSEL POMOCÍ MAGNETICKÝCH NANOSTRUKTUR

RANDOM NUMBER GENERATOR BASED ON MAGNETIC NANOSTRUCTURES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. ROMAN JÍRA

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. MICHAL URBÁNEK, Ph.D.

BRNO 2015

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav fyzikálního inženýrství
Akademický rok: 2013/14

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Roman Jíra

který/která studuje v **magisterském studijním programu**

obor: **Fyzikální inženýrství a nanotechnologie (3901T043)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Generování náhodných čísel pomocí magnetických nanostruktur

v anglickém jazyce:

Random number generator based on magnetic nanostructures

Stručná charakteristika problematiky úkolu:

Generování velkého množství opravdu náhodných čísel nachází využití zejména v kryptografii a v Monte Carlo simulacích. Jednou z možností pro rychlé generování náhodných čísel je využití magnetických nanostruktur. Cílem diplomové práce je návrh koncepce generátoru náhodných čísel, založeném na náhodném přepínání stavů v magnetickém vortexu.

Cíle diplomové práce:

Proveďte rešeršní studii k problematice generování náhodných čísel, zvláštní kapitolu věnujte problematice generování náhodných čísel pomocí magnetických nanostruktur.

Sestavte koncept generátoru náhodných čísel založeném na principu generování náhodných vortexových stavů v magnetických nanodiscích.

Připravte vzorky a experimentálně ověřte navržený koncept.

Seznam odborné literatury:

COEY, J. Magnetism and magnetic materials. 1st pub. New York: Cambridge University Press, 2010, xii, 614 s. ISBN 978-0-521-81614-4.

Vedoucí diplomové práce:Ing. Michal Urbánek, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2013/14.

V Brně, dne 22.11.2013

L.S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA STROJNÍHO INŽENÝRSTVÍ DĚKANÁT

prof. RNDr. Tomáš Šikola, CSc.
Ředitel ústavu

prof. RNDr. Miroslav Doupovec, CSc., dr. h. c.
Děkan

Abstrakt
Generování náhodných čísel může být založeno na fyzikálních jevech, v nichž vystupuje pravděpodobnost, na algoritmech, které využívají především složité či jednosměrné matematické funkce, případně na kombinaci obou těchto přístupů. Magnetický vír je základním stavem magnetizace, který vzniká v magnetických mikro- a nanostrukturách vhodného tvaru, rozměrů a materiálu. Vhodnými podmínkami při vzniku tohoto stavu magnetizace lze zajistit, že veličiny, kterými ho lze popsat, mají náhodný charakter. V rámci této práce je představen koncept generátoru skutečně náhodných čísel, který využívá náhodného přepínání stavů magnetického víru. Následně je provedena jeho realizace a experimentální generování náhodných čísel, která byla poté podrobena statistické analýze.

Summary
Random number generation can be based on physical events with probabilistic character, or on algorithms that use complex or one-way functions, alternatively on both of these approaches. A magnetic vortex is a basic state of magnetization that forms in magnetic micro- and nanostructures of an appropriate shape, dimensions and material. Quantities of the magnetic vortex form randomly if ambient conditions are chosen eligibly. A concept of a true random number generator using a random switching of states of the magnetic vortex is presented in this thesis. This concept is realized and random numbers were experimentally generated and numbers were statistically analysed.

Klíčová slova
magnetický vír, cirkulace magnetizace, anizotropní magnetorezistivita, generátor náhodných čísel, skutečně náhodná čísla

Keywords
magnetic vortex, circulation of magnetisation, anisotropic magnetoresistance, random number generator, true random numbers

JÍRA, R. *Generování náhodných čísel pomocí magnetických nanostruktur*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2015. 82 s. Vedoucí Ing. Michal Urbánek, Ph.D.

Prohlašuji, že jsem předloženou diplomovou práci vypracoval samostatně za odborného vedení Ing. Michala Urbánka, Ph.D. Dále prohlašuji, že veškeré podklady, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury.

V Brně dne 29. května 2015

.....

Bc. Roman Jíra

Na tomto místě děkuji především Ing. Michalu Urbánkovi, Ph.D. za výborné vedení, rady a věcné připomínky. Dále děkuji členům skupiny zabývající se magnetismem, především Bc. Marku Vaňatkovi, Bc. Lukáši Flajšmanovi a Igoru Turčanovi. Mé poděkování též patří Mgr. Slávku Licehammerovi za konzultace v oblasti náhodných čísel a kryptografie. Děkuji i Ing. Janě Štohanzlové za podporu při psaní této závěrečné práce. Děkuji též svým rodičům, bez jejichž podpory by tato práce nevznikla.

Analýzy vzorků byly provedeny ve Sdílené laboratoři přípravy a charakterizace nanostruktur CEITEC VUT a hrazeny z projektu CEITEC - open access LM2011020.

Bc. Roman Jíra

Obsah

1 Úvod

Nanotechnologie stojí v současné době v centru pozornosti, a to jak ze strany vědců zkoumajících rozličné vlastnosti nanostruktur a procesy s nimi spojené, tak ze strany průmyslových odvětví hledajících jejich vhodnou aplikaci a následnou masovou produkci. Obor, který studuje využití spinu elektronu, potažmo s ním spojený magnetický moment, se nazývá spintronika, případně spinelektronika. Název pochází z roku 1996 jako akronym pro *spin transport electronics* [1]. Mezi jevy, které jsou ve spintronice zahrnuté, patří i magnetické víry.

Magnetický vír je jedním z možných stavů magnetizace mikro- a nanostruktur, který je podmíněn především vhodnými rozměry a materiálem struktury. K úplnému popisu jeho vlastností jsou dostatečné dvě na sobě nezávislé veličiny, které se nazývají polarita jádra a cirkulace křivek magnetizace. Nanostruktury s magnetickými víry se jeví jako vhodný kandidát např. pro paměťová úložiště o vysokých kapacitách [2], senzory magnetického pole [3], členy logických obvodů [4] či bipolární tranzistory [5].

Náhodná čísla, tedy řetězce čísel, jejichž jednotlivé číslice nejsou závislé na ostatních číslicích, nacházejí využití například v loteriích, hazardních hrách, počítačových simulacích a modelování, moderním šifrování či i pro umění. Náhodná čísla lze generovat buď pomocí zařízení založených na fyzikálních jevech, ve kterých vystupuje pravděpodobnost, nebo pomocí algoritmů využívajících matematické postupy. Z fyzikálních jevů je možné využívat například házení kostek, ruletu, radioaktivitu [6, 7], výstřelový šum v elektronických obvodech [8], atmosférický šum [9], šum světelného zdroje v optoelektronických obvodech [10, 11, 12, 13] či průchod jednotlivých fotonů skrze dělič svazku [14]. Algoritmy, které generují náhodná čísla, mohou být založené např. na jednosměrných matematických funkcích [15] či logických operacích a bitových přesunech [16]. Poměrně běžné je i propojení generátoru čísel skutečně náhodných a pseudonáhodných, kdy čísla skutečně náhodná slouží jako některé vstupní parametry pro generaci čísel pseudonáhodných. Kromě využití některých výše uvedených fyzikálních jevů do této kategorie lze zařadit i biometriku, kdy jako vstupní parametry pseudonáhodného generátoru slouží lidské tělo, resp. jeho vybrané části či jeho projevy [17].

V rámci této práce je navržen koncept generátoru, který vhodně zvoleným způsobem manipuluje se stavem magnetických veličin v nanostrukturách a na základě zvolené veličiny vytváří náhodná čísla. Díky zvoleným fyzikálním procesům jde o čísla skutečně náhodná. V současné době generátor náhodných čísel založený na variaci veličin magnetických vírů neexistuje, jde tedy o novátorský přístup na poli generátorů náhodných čísel.

V předložené práci jsou nejprve popsány principy elektromagnetismu na atomové úrovni, projevy magnetismu ve strukturách o velikostech v řádu desítek až stovek nanometrů, zřetel je kladen na popis vlastností magnetických vírů. Následující kapitola se věnuje náhodným číslům, jejich vlastnostem a způsobům jejich tvorby. Dále některým generátorům fyzickým i softwarovým a způsobům testování jejich náhodnosti, s přihlédnutím k vhodnosti testovaných generátorů ke kryptografickému využití. Následující kapitola se týká samotného návrhu konceptu generátoru skutečně náhodných čísel. Zde je popsána idea, na které je princip generátoru založen. Jsou zde představeny jednotlivé části generátoru včetně podrobnějšího popisu jejich funkcí. Pozornost je věnována i metodám, které byly využity při jednotlivých krocích výroby vzorků. Další kapitola se týká vyrobených vzorků, jsou zde popsány konkrétní parametry při jejich výrobě a proces jejich opti-

malizace. Poslední kapitola je věnována analýze dat, která jsou získávána z navrženého a experimentálně připraveného generátoru. Vygenerovaná náhodná čísla jsou podrobena statistickým testům a na jejich základě je hodnocena kvalita generátoru náhodných čísel.

2 Magnetické víry

Magnetický vír je pojmenování jedné z možných konfigurací magnetizace, která vzniká v nanostrukturách vhodných rozměrů, tvarů a materiálů.

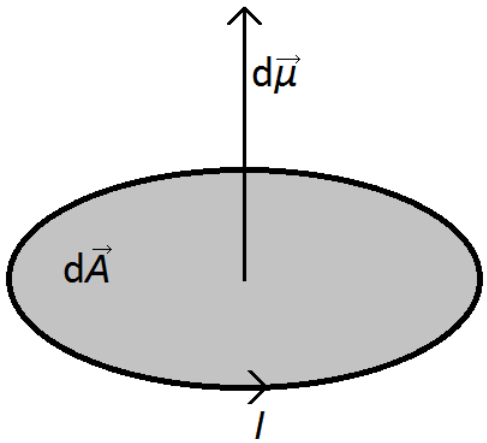
Před tím, než bude pozornost zaměřena na magnetické víry, bude podrobněji popsán magnetismus na elementární úrovni, některé charakteristické veličiny spjaté s magnetickým polem, vznik a vlastnosti doménové struktury a některé jevy s ní spojené a vybrané magnetické vlastnosti materiálů. Poté budou podrobněji představeny magnetické víry, způsob a podmínky jejich vzniku, vlastnosti a především jejich chování ve vnějším magnetickém poli. Následně bude pozornost věnována vybraným metodám použitelných a již používaných pro pozorování vlastností magnetických vírů. Závěr této kapitoly se týká možností využití magnetických vírů, a to jak teoretickým návrhům, tak i zařízením experimentálně testovaných, případně i již používaných v praxi.

2.1 Magnetismus malých rozměrů

2.1.1 Magnetický moment

Magnetismus se na elementární úrovni projevuje pomocí magnetického momentu $\vec{\mu}$. V rámci atomu je magnetický moment vykazován jak jednotlivými elektrony, tak i protony v jádře. Vzhledem k poměru hmotností protonu a elektronu je magnetický moment elektronu $\vec{\mu}_\mathrm{e}$ o tři řády větší než magnetický moment protonu $\vec{\mu}_\mathrm{p}$, protože magnetický moment je nepřímo úměrný hmotnosti částice. Nadále se tedy budeme zabývat pouze magnetickým momentem elektronu a magnetický moment protonu budeme zanedbávat.

Uvažujme nyní uzavřenou smyčku o infinitezimální ploše $\mathrm{d}\vec{A}$, kterou protéká elektrický proud I, jak je naznačeno na obrázku 2.1. Popsané smyčce přísluší magnetický moment $\mathrm{d}\vec{\mu} = I \cdot \mathrm{d}\vec{A}$. Pokud vezmeme v úvahu smyčku o ploše $\vec{A}$, lze ji rozdělit na infinitezimálně malé plošky $\mathrm{d}\vec{A}$. U sousedních smyček dochází vlivem opačně tekoucího elektrického proudu k vyrušení jeho působení, výsledný proud tedy protéká pouze na okraji plochy $\vec{A}$. V tomto případě je magnetický moment uzavřené smyčky roven $\vec{\mu} = I \cdot \vec{A}$.



Obrázek 2.1: Elektrický proud I protékající smyčkou o infinitezimální ploše $\mathrm{d}\vec{A}$ a příslušný infinitezimální magnetický moment $\mathrm{d}\vec{\mu}$.

Vezmeme-li v úvahu klasickou kvantovou mechaniku, moment hybnosti elektronu je tvořen dvěma složkami, kterými jsou orbitální a spinový moment hybnosti.

Pohyb elektronu po dráze okolo jádra atomu je spjat s orbitálním momentem hybnosti $\vec{L}$. Velikost L orbitálního momentu hybnosti je kvantovaná a lze ji určit jako

$$L = \hbar \cdot \sqrt{l \cdot (l+1)}, \tag{2.1}$$

kde l je orbitální kvantové číslo nabývající hodnot 0, 1, 2, ..., n_q, přičemž n_q je hlavní kvantové číslo nabývající hodnot 1, 2, 3, ... [18] a $\hbar$ redukovaná Planckova konstanta.

Orbitu elektronu je možné považovat za uzavřenou smyčku, kterou protéká proud ve směru opačném, než se elektron pohybuje. Vztah orbitálního magnetického momentu $\vec{\mu_{orb}}$ a orbitálního momentu hybnosti $\vec{L}$ lze vyjádřit vztahem

$$\vec{\mu}_\mathrm{orb} = \gamma \cdot \vec{L}, \tag{2.2}$$

kde γ je faktor závislosti mezi momenty magnetickým a hybnosti a nazývá se gyromagnetický poměr [19]. Gyromagnetický poměr není konstanta, jeho hodnota je závislá na tom, o které momenty hybnosti (orbitální či spinový) se jedná. V tomto případě je jeho hodnota $\gamma = -e/(2 \cdot m_\mathrm{e})$, kde e je náboj elektronu a m_e hmotnost elektronu. Směr orbitálního momentu hybnosti elektronu je opačný než směr orbitálního magnetického momentu.

Vzhledem ke kvantovému charakteru veličin je možné určit pouze z-složku orbitálního magnetického momentu. Vztah pro tuto složku přechází do tvaru

$$\mu_\mathrm{orb,z} = -\frac{e}{2 \cdot m_\mathrm{e}} \cdot m_\mathrm{l} \cdot \hbar, \tag{2.3}$$

kde m_l je magnetické orbitální číslo, jež nabývá hodnot $m_\mathrm{l} = 0, \pm 1, \pm 2, ..., \pm l$ [19].

Vezmeme-li v úvahu Bohrův magneton μ_B, který je definován jako $\mu_B = (e \cdot \hbar)/(2 \cdot m_e)$, je možné vztah pro vyjádření orbitálního magnetického momentu zjednodušit na

$$\mu_\mathrm{orb,z} = -m_\mathrm{l} \cdot \mu_\mathrm{B}, \tag{2.4}$$

takže orbitální magnetický moment elektronu je celočíselný násobek Bohrova magnetonu.

Bohrův magneton vystupuje i v případě bezrozměrného Landého faktoru, který je též nazýván g-faktor. Tato veličina je definována jako poměr magnetického momentu vyjádřeného v Bohrových magnetonech vůči příslušnému momentu hybnosti. Pro orbitální magnetický moment elektronu je g-faktor roven jedné.

Spinový magnetický moment souvisí se spinem elektronu. Ty vykazují vlastní spinový moment hybnosti $\vec{S}$, jehož velikost dosahuje pouze jedné hodnoty S, a to

$$S = \hbar \cdot \sqrt{s \cdot (s+1)}, \tag{2.5}$$

kde s je spinové kvantové číslo nabývající hodnoty $s = 1/2$ [18]. Velikost spinového momentu hybnosti tedy je $S = \sqrt{2} \cdot \hbar$.

Ke spinovému momentu hybnosti je vázán spinový magnetický moment $\vec{\mu}_\mathrm{s}$, který je možné vyjádřit v podobném tvaru jako orbitální magnetický moment, tedy

$$\vec{\mu}_\mathrm{s} = \gamma \cdot \vec{S}, \tag{2.6}$$

ale s rozdílem v hodnotě gyromagnetického poměru, který v případě spinového magnetického momentu nabývá hodnoty $\gamma = -e/m_\mathrm{e}$ [19].

Vyjádříme-li si z-složku spinového magnetického momentu pomocí magnetického spinového čísla m_s, získáme vztah

$$\mu_{\mathrm{s,z}} = -\frac{e}{m_{\mathrm{e}}} \cdot m_{\mathrm{s}} \cdot \hbar, \tag{2.7}$$

kde m_{s} může nabývat hodnot $m_{\mathrm{s}} = \pm 1/2$ [18].

Vztáhneme-li spinový magnetický moment k Bohrovu magnetonu, získáme pro z-složku spinového magnetického momentu rovnici

$$\mu_{\mathrm{s,z}} = -2 \cdot m_{\mathrm{s}} \cdot \mu_{\mathrm{B}}, \tag{2.8}$$

přičemž ale hodnota g-faktoru 2 je pouze přibližná, vezmou-li se při jeho výpočtu v úvahu korekce vyšších řádů, g-faktor dosahuje hodnoty 2,0023 [19].

Porovnáním g-faktorů spinového a orbitálního magnetického momentu docházíme k poznatku, že spinový magnetický moment elektronu je dvojnásobný v porovnání s orbitálním magnetickým momentem téhož elektronu (bereme-li v úvahu hodnotu g-faktoru spinového magnetického momentu rovnou 2).

Elektrony vázané v atomu vykazují orbitální i spinové momenty hybnosti, u kterých dochází ke vzájemnému ovlivňování. Tato interakce mezi orbitálním a spinovým momentem hybnosti se nazývá spin-orbitální interakce. Jejich vzájemným ovlivňováním dochází ke vzniku celkového momentu hybnosti $\vec{J}$, který je možné určit formou vektorového součtu orbitálních i spinových momentů hybnosti všech elektronů v atomu pomocí vztahu

$$\vec{J} = (\vec{L}_1 + \vec{L}_2 + \vec{L}_3 + ... + \vec{L}_{\mathrm{Z}}) + (\vec{S}_1 + \vec{S}_2 + \vec{S}_3 + ... + \vec{S}_{\mathrm{Z}}), \tag{2.9}$$

ve kterém index Z vyjadřuje atomové číslo, které udává počet elektronů, resp. protonů v atomu [18].

Příslušný celkový magnetický moment $\vec{\mu}$ dle [18] následně získáme vztahem

$$\vec{\mu} = \gamma \cdot \vec{J}, \tag{2.10}$$

případně, známe-li spinové i orbitální magnetické momenty všech elektronů v atomu, můžeme celkový magnetický moment získat jejich vektorovým součtem:

$$\vec{\mu} = (\vec{\mu}_{\mathrm{orb1}} + \vec{\mu}_{\mathrm{orb2}} + \vec{\mu}_{\mathrm{orb3}} + ... + \vec{\mu}_{\mathrm{orbZ}}) + (\vec{\mu}_{\mathrm{s1}} + \vec{\mu}_{\mathrm{s2}} + \vec{\mu}_{\mathrm{s3}} + ... + \vec{\mu}_{\mathrm{s}Z}). \tag{2.11}$$

Směry orbitálního a spinového magnetického momentu a příslušného momentu hybnosti jsou navzájem opačně orientovány.

2.1.2 Magnetizace

K popisu těles, která obsahují velká množství atomů, se pro popis jeho magnetického stavu jako vhodnější jeví veličina magnetizace $\vec{M}$, která je definována jako objemová hustota magnetických momentů. Vyjádřit ji lze jako

$$\vec{M} = \frac{\sum_{i=1}^{n} \vec{\mu}_{\mathrm{i}}}{V}, \tag{2.12}$$

kde V je objem zkoumaného tělesa či jeho části a $\sum_{i=1}^{n} \vec{\mu}_{\mathrm{i}}$ je sumace všech magnetických momentů, které zkoumaný objem obsahuje.

Výsledná magnetizace tělesa závisí na několika parametrech, mezi které patří jeho tvar a rozměry, použitý materiál či přítomnost externího magnetického pole. Tyto parametry se promítají do vzájemného působení mezi jednotlivými atomy tělesa. Interakce, s nimiž je spojená příslušná stejnojmenná energie, se nazývají výměnná, magnetokrystalická anizotropní, Zeemanova a magnetostatická dipolární.

Výměnná interakce je krátkodosahová a souvisí se směry magnetizace sousedních atomů či molekul. Tato interakce působí na částice tím způsobem, že se snaží směry jejich magnetických momentů stočit do stejného směru. V případě, že jsou směry magnetizace sousedních částic paralelní, je hodnota příslušné energie nejnižší, pokud jsou antiparalelní, energie dosahuje své nejvyšší hodnoty. Podrobnější popis této i následující energie interakce (včetně vztahu pro její určení) lze nalézt v [19].

Látky, ve kterých lze popsat strukturu pomocí krystalové mřížky, obvykle vykazují i tzv. osy magnetizace. Tyto osy magnetizace mohou být tzv. snadné (angl. easy axis), podél kterých dochází k magnetizaci tělesa poměrně jednoduše, tedy není nutné k magnetizaci v tomto směru vynaložit množství energie. Osy magnetizace mohou být i tzv. těžké (angl. hard axis), podél kterých k magnetizaci dochází teprve s vynaložením větší energie než v případě osy snadné. Magnetokrystalická anizotropní interakce souvisí právě se směrem magnetizace tělesa vůči osám magnetizace. Energie jí příslušná je nejnižší, pokud je směr magnetizace tělesa shodný se směrem snadné osy magnetizace.

Třetí uvedená interakce, Zeemanova, se projevuje stáčením magnetizace tělesa ve směru vnějšího magnetického pole, ve kterém je těleso umístěno. Nejnižší hodnota příslušné energie nastává v okamžiku, kdy je směr magnetizace tělesa paralelní se směrem externího magnetického pole. Nejvyšší hodnota Zeemanovy energie nastává v okamžiku, kdy jsou směry magnetizace tělesa a vnějšího pole antiparalelní.

Poslední interakce, která byla zmíněná, je magnetostatická dipolární. Její projev je podobný interakci Zeemanově, rozdíl je ale v poli, vůči kterému dochází ke stáčení magnetizace. Oproti poli vnějšímu, jako v případě Zeemanovy interakce, dochází ke stáčení magnetizace ve směru magnetického pole indukovaného samotným tělesem.

Výsledná magnetizace tělesa je dána vzájemným působením výše popsaných interakcí. Stav magnetizace odpovídá jejich minimálnímu energiovému stavu. Důsledkem je vznik oblastí, které v sobě shlukují atomy se shodným směrem magnetického momentu. Tyto oblasti se nazývají magnetické domény.

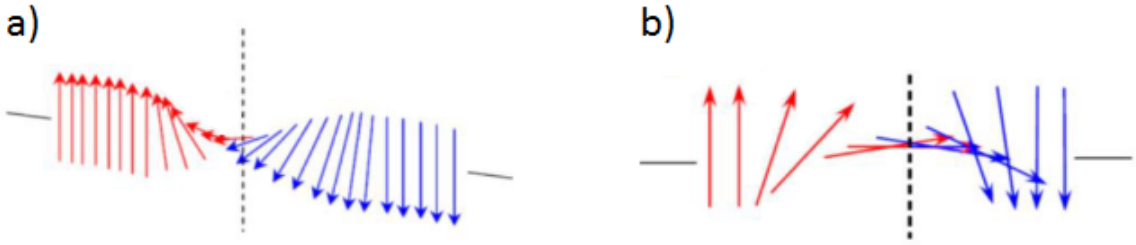
2.1.3 Magnetické domény

Magnetická doména je oblast tělesa, ve které mají částice, které jsou v ní zahrnuty, směry magnetických momentů shodné. Počet těchto domén v tělese je dán především tvary a rozměry tělesa, materiálem a působením případného vnějšího magnetického pole.

Budeme-li uvažovat těleso velmi malých rozměrů pohybujících se v řádu jednotek, maximálně desítek nanometrů, které se nenachází v externím magnetickém poli, tak v celém objemu tělesa dojde ke stočení jejich magnetických momentů do stejného směru vlivem převládajících výměnných interakcí mezi jednotlivými částicemi. Tento stav se nazývá jednodoménový a těleso se navenek chová jako dipól [20].

V případě obecného tělesa o vyšších rozměrech, než je typická vzdálenost dosahu výměnné interakce, není tato krátkodosahová interakce schopna stočit magnetické momenty všech atomů tělesa stejným směrem. Nedochází tedy k jednodoménovému stavu tělesa, ale magnetických domén v tělese vzniká více než jedna. Tělesa, jejichž stav magnetizace se skládá z více domén, se označují jako multidoménová.

Existuje-li v tělese více než jedna doména, na rozhraní mezi doménami je možné rozpoznat jejich hranice, které jsou nazývány doménovými stěnami. V těchto doménových stěnách dochází ke stáčení magnetizace mezi směry magnetizace domén. Dle směru stáčení je možné rozlišit dva druhy doménových stěn. První z nich se nazývá Blochova stěna a magnetizace se mění v rovině doménové stěny. Druhý způsob, jak dochází k oddělení sousedních magnetických domén, je Néelova stěna, v níž se směr magnetizace mění v rovině kolmé na doménovou stěnu. Grafické porovnání obou typů doménových stěn je schematicky zobrazeno na obrázku 2.2.



Obrázek 2.2: Schematické zobrazení stáčení směru magnetizace v a) Blochově a b) Néelově doménové stěně. Převzato z [22] a upraveno.

2.1.4 Vlastnosti magnetických materiálů

Podle použitého materiálu, ze kterého se těleso skládá, se v závislosti na externím poli, resp. jeho intenzitě liší výsledná magnetizace. Tato reakce na intenzitu pole může být lineární i nelineární a obvykle se popisuje pomocí veličiny nazvané magnetická susceptibilita χ. Tato veličina je definována pomocí vztahu

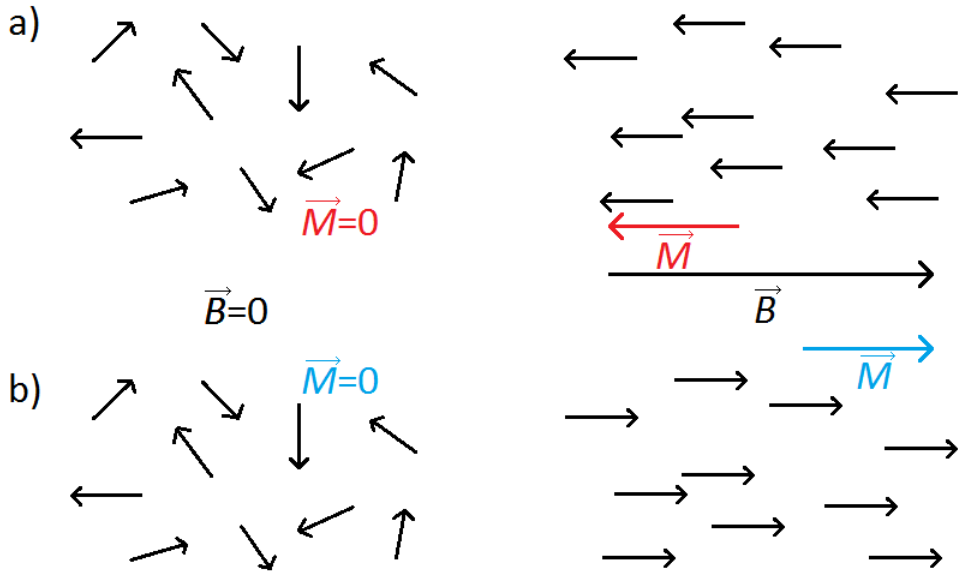
$$\vec{M} = \chi \cdot \vec{H_{\text{ext}}}, \tag{2.13}$$

kde $\vec{H}_{\text{ext}}$ je intenzita působícího magnetického pole.

Je-li závislost magnetizace $\vec{M}$ na intenzitě magnetického pole $\vec{H}_{\text{ext}}$ lineární, dělíme materiály na diamagnetické a paramagnetické. Susceptibilita diamagnetického materiálu je menší než jedna, což lze interpretovat tak, že diamagnetický materiál po vložení do externího magnetického pole toto pole zeslabuje. Mezi diamagnetické materiály patří např. uhlík, měď či zlato.

Oproti tomu je susceptibilita paramagnetického materiálu větší než jedna, tedy tento materiál externí magnetické pole zesiluje. Tyto vlastnosti vykazuje např. hliník, platina nebo uran. Grafické znázornění magnetického uspořádání diamagnetického a paramagnetického materiálu při nulovém i nenulovém magnetickém poli je uvedeno na obrázku 2.3.

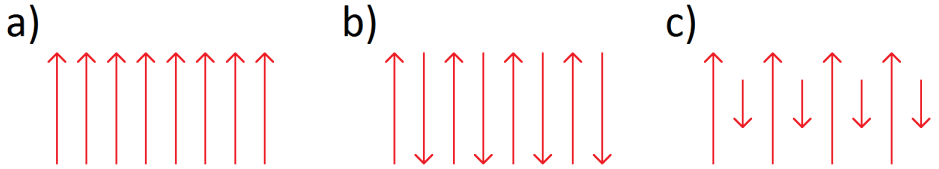
Materiály, jejichž závislost magnetizace na intenzitě magnetického pole je nelineární a nabývá hodnoty mnohem větší než 1, se nazývají feromagnetické. Typickými představiteli feromagnetických materiálů jsou železo, nikl či kobalt. Nepůsobí-li na feromagnetické těleso vnější magnetické pole, jednotlivé domény jsou uspořádané náhodně a navenek



Obrázek 2.3: Schematické znázornění magnetického uspořádání a) diamagnetického a b) paramagnetického materiálu v magnetickém poli $\vec{B}$. Vlevo materiál bez působení vnějšího magnetického pole, vpravo při jeho působení ve vyznačeném směru. Naznačena je i magnetizace materiálů $\vec{M}$.

je magnetizace tělesa nulová. Začne-li na těleso magnetické pole působit, směry magnetizace domén se začnou stáčet stejným směrem. Při dosažení dostatečné velikosti intenzity vnějšího magnetického pole jsou domény feromagnetického materiálu srovnány paralelně. Tento stav se nazývá nasycení či saturace.

Odlišné jsou tzv. antiferomagnetické materiály, u kterých lze popsat antiparalelní konfiguraci dvou podmřížek magnetických momentů stejné velikosti. Antiferomagnetické materiály jsou např. chróm, hematit či feromagnan.



Obrázek 2.4: Schematické naznačení směrů magnetických domén v materiálu a) feromagnetickém, b) antigeromagnetickém a c) ferimegnetickém.

Z pohledu charakteru magnetické susceptibility jsou mezi feromagnetické látky řazeny i ty, které jsou nazývány ferimagnetické či zkráceně ferity. U těchto látek je také možné rozeznat dvě podmřížky antiparalelních směrů magnetických momentů, které ale nejsou stejně velké, jako v případě antiferomagnetických látek. Tuto skupinu reprezentují např. oxidy železa s oxidy dalších kovů, např. manganu či barya. Porovnání schematického znázornění magnetického uspořádání pro feromagnetické, antiferomagnetické a ferimagnetické látky je zobrazeno na obrázku 2.4.

Feromagnetické, antiferomagnetické a ferimagnetické materiály při dosažení určité teploty, přechází do stavu paramagnetického, kdy jsou směry jednotlivých domén v tělese

uspořádány náhodně. Tato teplota je nazývána Curieho teplota a hodnota této teploty se liší pro různé materiály.
Odlišný způsob dělení magnetických materiálů je založen na velikosti plochy jejich hysterezních smyček, a materiály se tak dělí na magneticky měkké a na magneticky tvrdé. V případě široké hysterezní křivky se jedná o materiály magneticky tvrdé. Jejich reprezentanty jsou oxidy železa, barya či stroncia, slitiny hliníku, niklu a kobaltu, případně magnety na bázi vzácných zemin, např. slitiny samaria a kobaltu nebo neodymu, železa a boru. Pro tyto materiály z hlediska magnetické energie převládne magnetokrystalická anizotropní energie, a po odstranění působení vnějšího magnetického pole zůstavají zmagnetizované.

Magneticky měkké materiály vykazují hysterezní křivku úzkou a patří mezi ně např. kobalt, nikl či slitiny niklu a železa (permalloy), nebo slitina železa, chrómu a hliníku. Magnetokrystalická anizotropní energie je pro tyto materiály mnohem slabší v případě materiálů magneticky tvrdých a výsledný stav magnetizace záleží na vzájemném působení mezi výměnnou a magnetostatickou interakcí [20]. Po odstranění působení vnějšího magnetického pole magneticky měkké materiály obvykle ztrácejí své magnetické vlastnosti, jejich domény se vrací do neuspořádaného stavu, ve kterém se nacházely před působením vnějšího pole.

Magneticky tvrdé materiály nachází využití jako rotory a statory elektromotorů, lineární motory, generátory či reproduktory. Typickým příkladem využití magneticky měkkých materiálů jsou transformátory a záznamová média (pevné disky).

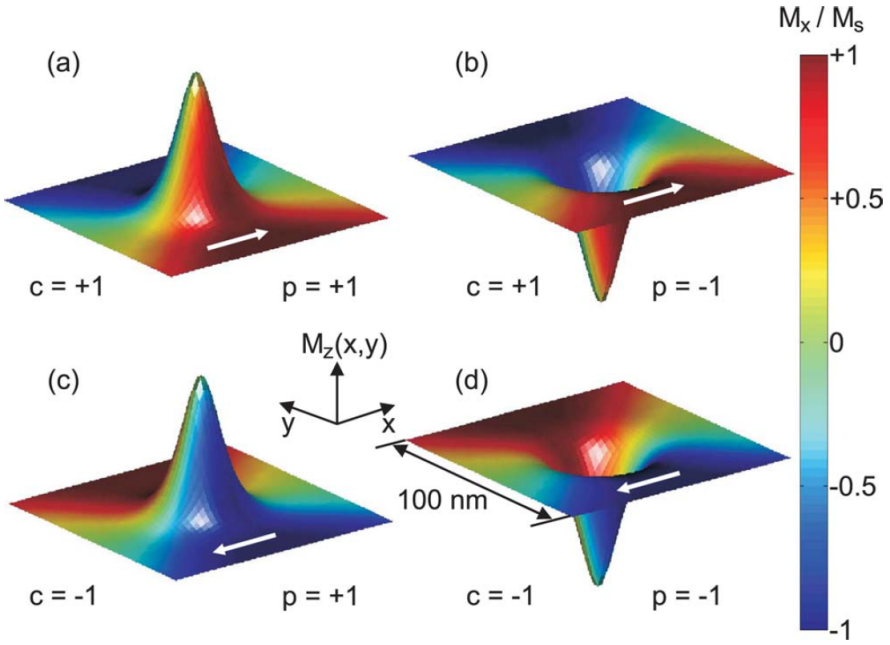
2.2 Magnetické víry

Uvažujme nyní symetrické těleso velmi malých rozměrů, které jsou ale zároveň dostatečně velké, aby nebyly atomy uspořádány v jednodoménovém stavu. Magnetizace tohoto tělesa nepřejde do obecného multidoménového stavu, místo toho dojde k uzavření křivek magnetizace do smyček rotujících v rovině tělesa.

Magnetizace tohoto tělesa přechází do stavu, který je dán minimalizací interakčních energií. V tělese dochází vlivem magnetostatické dipolární interakce k uzavření křivek magnetizace do smyček rotujících v rovině tělesa. Pokud by tato interakce působila v celém tělese, v jeho středu by nevyhnutelně došlo k singularitě. K té ale nedochází, neboť v oblasti středu tělesa začne nad magnetostatickou dipolární interakcí převládat krátkodosahová interakce výměnná, a jejím vlivem zde vystupuje magnetizace z tělesa ven kolmo k jeho povrchu. Tato oblast se nazývá jádro magnetického víru. Popsaný stav magnetizace, ve kterém dochází ke stáčení uzavřených křivek magnetizace v rovině tělesa a magnetizace v jeho středu vystupuje kolmo na rovinu stáčení křivek, se nazývá magnetický vír.

Magnetické víry jsou tedy stavy magnetizace s nejnižší energií vyskytující se v nanostrukturách tvořených magneticky měkkými materiály vhodných tvarů. Magnetický vír je možné popsat dvěma na sobě nezávislými veličinami [20, 21]. První z těchto veličin udává směr jádra víru vystupujícího z roviny stáčení magnetických křivek, nazývá se polarita,značí se p a může nabývat hodnot $+1$ pro směr nahoru, nebo -1 pro směr dolů. Druhá veličina souvisí se směrem stáčení magnetických křivek v rovině struktury a nese označení cirkulace se značkou c. Tato veličina nabývá také dvou hodnot, a to $+1$ pro stáčení křivek ve směru matematicky kladném (proti směru hodinových ručiček, dále CCW, z angl. Counter ClockWise), nebo -1 pro matematicky záporný směr stáčení (ve směru

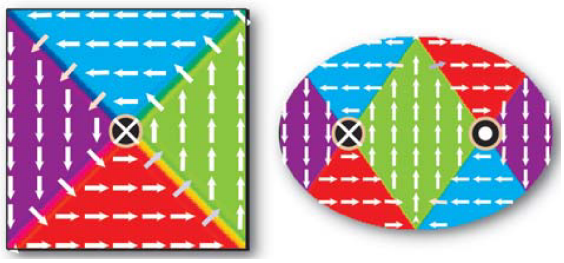
hodinových ručiček, dále CW, z angl. ClockWise). Vzhled magnetických vírů s různými hodnotami polarity a cirkulace je znázorněn na obrázku 2.5.



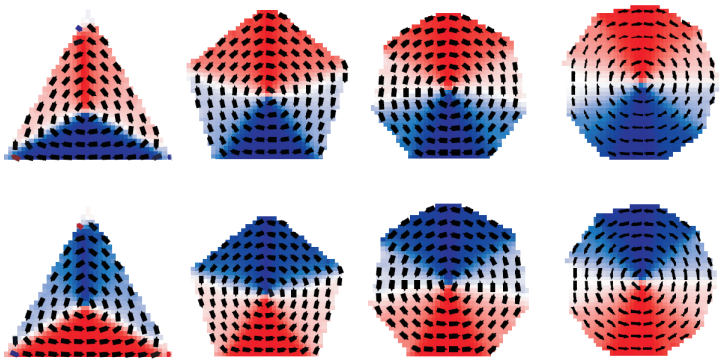
Obrázek 2.5: Zobrazení čtyř možných stavů magnetického víru s různými hodnotami cirkulace c a polarity p. Směr cirkulace v rovině je zobrazen bílými šipkami, kolmo na rovinu rotace křivek magnetizace vystupuje jádro víru udávající polaritu. Výška popisuje vystupující z-složku magnetizace M_z, barvy zobrazují x-složku magnetizace M_x vztaženou k saturační magnetizaci M_s. Převzato z [23].

Existují i dalších veličiny, pomocí kterých lze popsat stav magnetického víru, ty ale většinou bývají odvozené od polarity a cirkulace. Příkladem takové odvozené veličiny je chiralita, jejíž hodnotu lze získat vynásobením polarity a cirkulace.

Magnetický vír může vznikat nejen v kruhově symetrických discích, ale i ve strukturách dalších tvarů. Příkladem mohou být čtverce, kde se magnetická struktura nazývá Landauova struktura, eliptické disky [20] či pravidelné mnohoúhelníky [24]. V některých strukturách může docházet i ke vniku více než jednoho vírů, např. v eliptickém disku, případně v obdélníku. Na obrázku 2.6 je ukázán magnetický vír ve čtverci a pár magnetických vírů v eliptickém disku a obrázek 2.7 znázorňuje cirkulaci magnetického víru ve vybraných mnohoúhelnících. Ke vzniku magnetického víru může dojít i ve strukturách jiných tvarů, které se od zde uvedených liší.



Obrázek 2.6: Vlevo magnetický vír s polaritou směrem dolů a cirkulací proti směru hodinových ručiček ve čtvercové struktuře. Vpravo dvojice magnetických vírů opačných parametrů ve struktuře ve tvaru eliptického disku. Převzato z [20].



Obrázek 2.7: Znázornění obou směrů cirkulace magnetického víru. Zleva struktura tvaru trojúhelníku, pětiúhelníku, sedmiúhelníku a devítiúhelníku. Horní řada náleží cirkulaci ve směru a spodní proti směru hodinových ručiček. Neostré okraje tvarů mají původ v simulaci, při které bylo použito čtvercové mřížky. Převzato z [24] a upraveno.

V následujících kapitolách, nebude-li uvedeno jinak, budou popisovány vlastnosti a chování magnetického víru vzniklém ve struktuře plochého symetrického disku, a bude-li zmiňován termín magnetický vír, bude tím myšlen vír vzniklý v tomto disku.

2.3 Dynamické chování magnetického víru

Předchozí kapitola popisovala vlastnosti magnetického víru, na který nebylo nijakým způsobem působeno. V této kapitole budou popsány děje, ke kterým dochází, když magnetický vír nějakým způsobem ovlivňujeme. Bude ukázáno chování magnetického víru při působení magnetického pole a popsány procesy, kterých je možné vhodnou volbou parametrů působícího děje dosáhnout.

Proces vzniku magnetického víru, při kterém dochází k uzavření křivek magnetizace, se nazývá nukleace. Stav, kdy na vír není působeno, se nazývá klidový, a ten se ve struktuře tvaru disku vyznačuje tím, že se jádro magnetického víru nachází v jeho geometrickém středu. Proces, při kterém dochází k zániku magnetického víru, se označuje jako anihilace. Po anihilaci víru buď dochází k nukleaci nového víru, nebo je magnetizace struktury udržována v jiném stavu, než je magnetický vír. Možnosti, jakými lze anihilace dosáhnout, a podmínky nutné pro nukleaci nového víru nebo přechodu magnetizace do jiného stavu budou podrobněji popsány v následujících podkapitolách.

Děj, který sestává z anihilace původního víru a nukleace víru nového, se nazývá překlopení magnetického víru. Označení je stejné jak pro případ, že vlastnosti nového víru jsou od předchozího jiné, tak i pro případ, kdy nový vír vykazuje stejný stav jako vír předchozí.

2.3.1 Vír v magnetickém poli

Prvním způsobem, jak docílit interakce s magnetickým vírem, je jeho umístění do externího magnetického pole. Chování magnetického víru závisí na několika parametrech. Jde o směr magnetického pole vůči struktuře obsahující magnetický vír. Dále záleží na charakteru magnetického pole, tedy zda-li jde o stacionární nebo proměnné pole. V případě statického pole je rozhodujícím parametrem velikost jeho intenzity. Chování v dynamickém poli závisí na směru změny pole, tedy jde-li o pole rostoucí či klesající, a na rychlosti

změny. V případě periodického charakteru magnetického pole závisí chování magnetického víru na jeho amplitudě a periodě. Způsob interakce záleží nejen na magnetickém poli, ale také na rozměrech struktury. Struktury rozdílné velikosti nereagují na totožné magnetické pole stejným způsobem.

Uvažujme nyní magnetický vír vzniklý ve struktuře disku, na kterou je působeno magnetickým polem, jehož směr je paralelní s rovinou disku. Grafické znázornění je uvedeno na obrázku 2.8. Nejprve se zaměříme na symetrický plochý disk o průměru 200 nm, jemuž v uvedeném obrázku přísluší modrá křivka. Stav jeho magnetizace za nepřítomnosti magnetického pole je magnetický vír, jež setrvává ve své klidové poloze ve středu disku. Začněme na disk působit slabým magnetickým polem. Oblast víru, ve které je směr rotace paralelní s působícím magnetickým polem, se rozšíří, čímž dojde k vychýlení disku mimo svou klidovou polohu ve směru kolmém na působící pole. Vír s cirkulací proti směru hodinových ručiček se z pohledu směru pole posune vlevo, jak je zobrazeno ve spodní části obrázku 2.8. Pokud je cirkulace víru ve směru hodinových ručiček, vír se ve stejném poli posune vpravo. Velikost posunu je lineárně závislá na magnetickém poli, a to až do dosažení anihilačního pole H_{A}, kdy dochází k saturaci magnetizace a disk přechází do jednodoménového stavu. Pohybuje-li se magnetické pole mezi hodnotami $-H_{\mathrm{A}}$ až H_{A}, je pohyb magnetického víru vratný. Dojde-li k dosažení či překročení pole $\pm H_{\mathrm{A}}$, vír je z disku vypuzen, a nový vír v disku vzniká až při snížení pole na tzv. nukleační pole H_{N}. Cirkulace nového víru může, ale nemusí být stejná jako cirkulace anihilovaného víru [20].

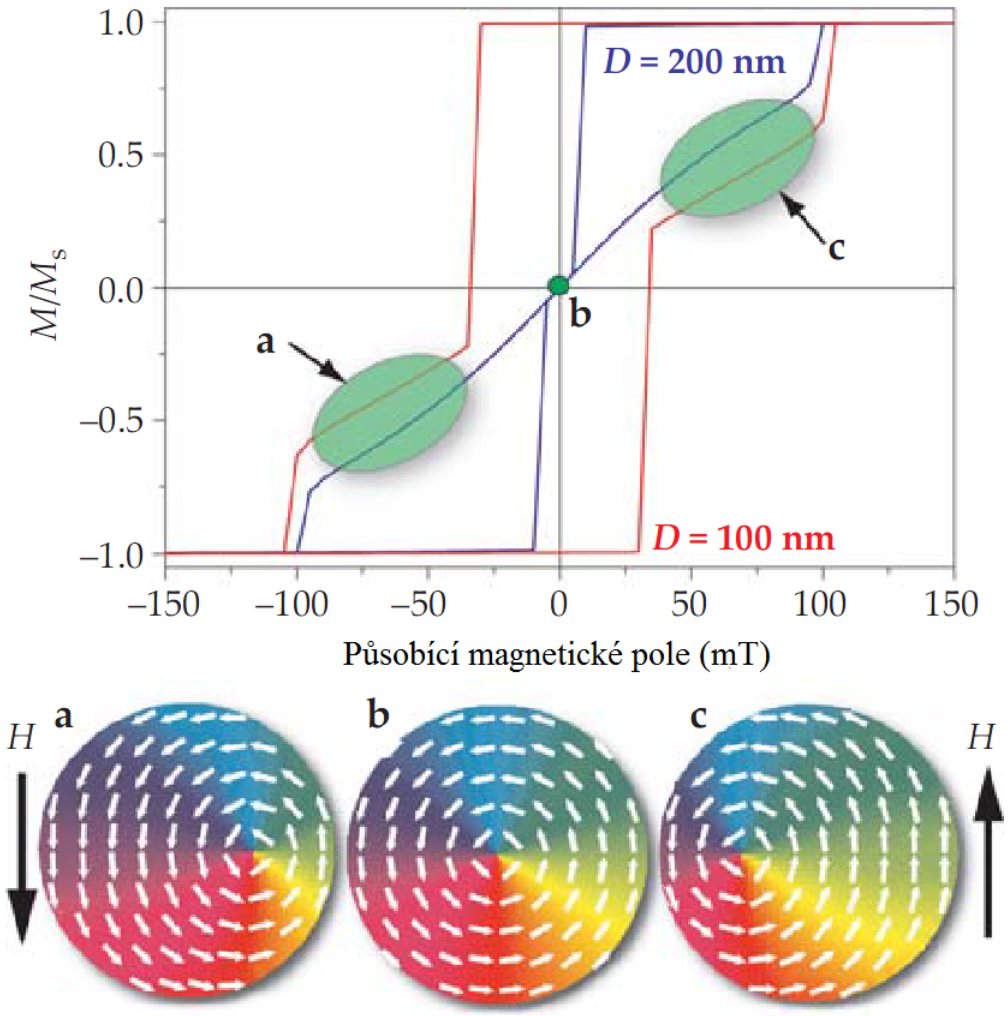
Hodnoty H_{A} a H_{N} jsou závislé na velikosti, rozměrech a materiálu disku a množství defektů disku. Velikost H_{A} se běžně pohybuje v rozmezí 0,05-0,3 T, velikost H_{N} může být i záporná, jak je ukázáno pomocí červené křivky na obrázku 2.8 [20]. V tomto případě disk o průměru 200 nm bez působení magnetického pole setrvává v jednodoménovém stavu, a teprve působením příslušného H_{N} lze iniciovat nukleaci magnetického víru.

Sledování pohybu jádra magnetického víru při jeho ovlivnění stacionárním magnetickým polem tedy umožňuje určit cirkulaci magnetizačních křivek. Pro zjištění směru jádra víru vůči rovině cirkulace křivek magnetizace, tedy polarity, je ale nutné zvolit jiný přístup.

Působí-li na disk s magnetickým vírem slabé střídavé magnetické pole, dochází nejen k periodickému pohybu jádra v závislosti na směru působícího magnetického pole, ale dochází i ke kruhovému pohybu jádra, který je označován jako gyrace, či také gyrotropický pohyb, příp. gyrotropická rotace. Vychýlením jádra z klidového stavu dochází ve struktuře k nerovnoměrnému rozložení magnetizace, což má za důsledek gyrotropickou rotaci okolo původní klidové polohy. Směr gyrotropického pohybu nezávisí na cirkulaci magnetizačních křivek v rovině disku, ale pouze na směru polarity, pomocí čehož ji je možné určit. Jestliže jádro víru směřuje dolů, tak je gyrotropický pohyb ve směru hodinových ručiček, a pokud je směr jádra nahoru, tak gyrace probíhá proti směru hodinových ručiček [20].

Možné je také využít i pulzů magnetického pole a ze zaznamenané trajektorie gyrotropního pohybu určit jak polaritu, tak cirkulaci. Toho je možné dosáhnout z toho důvodu, že reakce víru na pulz magnetického pole sestává ze dvou fází, kterými je zrychlené lineární vychýlení z klidové polohy a gyrotropická rotace. Pomocí směru vychýlení je možné určit cirkulaci, a ze směru gyrotropického pohybu polaritu [25].

Chceme-li překlopit polaritu magnetického víru, je nutné vyvolat proces, při kterém v disku vznikne dvojice vír a antivír s polaritou opačnou, než měl původní vír. Následně dochází k anihilaci antivíru s původním vírem a ve struktuře zůstává pouze nový vír s opačně orientovanou polaritou. Pro překlopení polarity magnetického víru pomocí mag-



Obrázek 2.8: Nahoře jsou zobrazeny hysterezní smyčky magnetických vírů v přiloženém magnetickém poli. Modrá křivka přísluší disku o průměru 200 nm, jehož magnetizace se při nulovém magnetickém poli nachází ve stavu víru. Působením magnetického pole dochází k vratnému vychýlení víru z klidové polohy. Je-li použito dostatečně silné pole, stav magnetizace přechází do jednodoménového stavu, ve kterém je velikost magnetizace M rovna saturační magnetizaci M_S. Červená křivka přísluší hysterezní smyčce disku o průměru 100 nm, který je při nulové velikosti pole v jednodoménovém stavu a jehož chování se od disku o průměru 200 nm liší. Dole je uvedena reakce cirkulace magnetizačních křivek na směr přiloženého pole, v a) a c) je vidět posun víru ve směru kolmém na směr působícího pole. b) je klidový stav víru, kdy magnetické pole nepůsobí. Převzato z [20] a upraveno.

netického pole ve směru kolmém k rovině disku je potřeba poměrně silné pole o velikosti okolo 0,3 T [20]. Lze ale použít i střídavé magnetické pole ve směru roviny disku, k překlopení polarity magnetického víru stačí amplituda takového pole o velikosti 1,5 mT [26].

Simulace založené na mikromagnetických výpočtech ukazují, že stav magnetického víru v nanostruktuře ve tvaru symetrického disku je možné ovládat pulzy externího magnetického pole ve směru roviny disku. Vhodnou volbou doby trvání pulzu a jeho velikosti lze iniciovat překlopení polarity nebo cirkulace bez nutnosti vytvářet disk s umělou asymetrií či působit během překlápění dalšími magnetickými poli. Pro překlopení po-

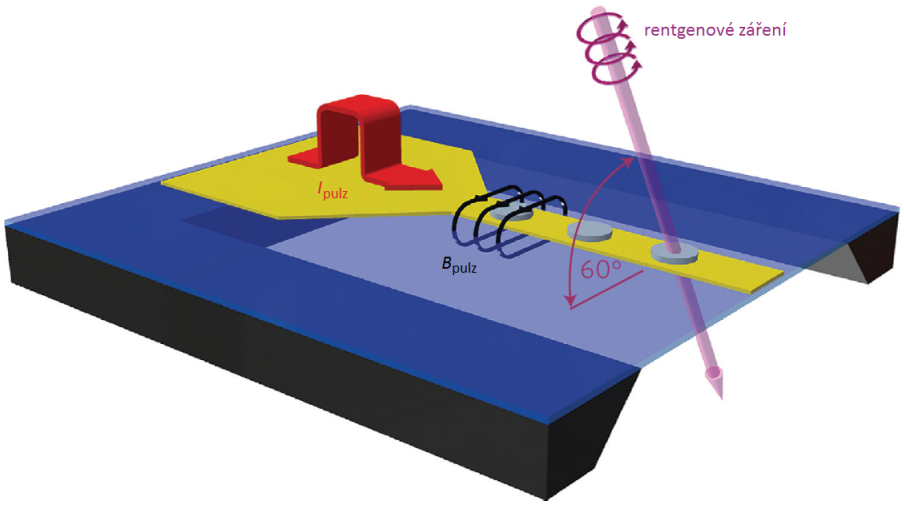
larity stačí dosáhnout dostatečně velkého pole, pomocí kterého dojde k vytvoření páru vír a antivír, načež dojde k anihilaci starého víru a antivíru. Velikost pole pro změnu cirkulace musí být dostatečná k vypuzení víru mimo strukturu, ale nesmí dosáhnout hodnoty, při které dochází k překlopení polarity. Volbou délky trvání magnetického pole je poté možno ovlivnit cirkulaci nového víru [27]. Ovládání cirkulace magnetického víru pomocí pulzů magnetického pole ve směru roviny disku bylo experimentálně ověřeno, a bylo ukázáno, že při použití pulzů lze používat pole přibližně o polovinu slabší, než kterého by bylo třeba dosáhnout při použití pole statického [28].

Doba, potřebná k přechodu cirkulace magnetizace nebo polarity jádra do nového stavu, je pro uvedené veličiny rozdílná. V případě cirkulace ji lze překlopit pomocí střídavého magnetického pole přibližně za 1 nanosekundu, tento čas se mírně liší pro disky různých rozměrů [28]. V případě polarity lze dosáhnout jejího překlopení v kratším čase, a to během několika desítek pikosekund [29, 30].

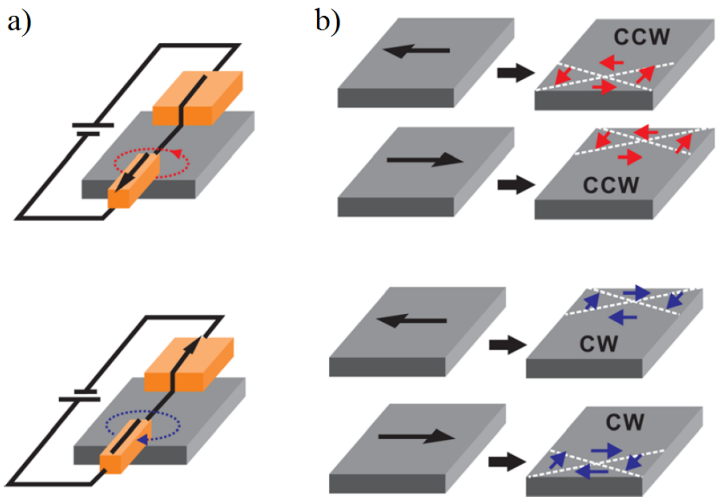
2.3.2 Další interakce s magnetickým vírem

Realizace ovlivňování magnetického víru v nanostrukturách pomocí externího magnetického pole není vždy jednoduchá. Dále je nutné vzít v úvahu, že pro cívky může být problematické provádět rychlé změny indukovaného magnetického pole. Kvůli těmto důvodům bývá využito magnetické pole, které je indukováno elektrickým proudem při průchodu vodičem, tzv. Oerstedovo pole. Některé metody zmíněné v předchozí podkapitole ostatně takto působící magnetické pole generovaly. Tato cesta se zdá být vhodnější, alespoň z hlediska snažšího provedení, které nevyžaduje cívky generující magnetické pole. Je možné využívat proudu stejnosměrného, střídavého i jednotlivých proudových pulzů. Konkrétní realizace může být provedena např. umístěním struktury s magnetickým vírem přímo na vodič, kterým elektrický proud protéká, případně průchodem elektrického proudu skrze studovanou strukturu s magnetickým vírem.

Metoda, ve které byla struktura umístěna na vodiči elektrického proudu, je již zmiňovaná studie přepínání cirkulace magnetického víru pomocí pulzů, a její provedení je zachyceno na obrázku 2.9. Proudový impulz procházející vodičem indukuje magnetické pole, a tímto polem je ovládána cirkulace disků, které jsou umístěny na vodiči.
I experimentální provedení, při kterém prochází elektrický proud přímo skrze vrstvu magnetického materiálu, může být využito pro překlápění cirkulace magnetického víru [31]. Princip, jehož koncept je zobrazený na obrázku 2.10, je založený na indukování lokálního magnetického pole na přechodu, který je tvořen kontaktem feromagnetické struktury s elektrodou z nemagnetického materiálu. Působením magnetického pole ve směru roviny struktury kolmo na směr průchodu elektrického proudu dojde k nukleaci víru, pomocí tohoto pole je následně možné ovládat i polohu víru ve struktuře či provést jeho anihilaci. Při užití symetrických elektrod může docházet k nukleaci magnetického víru náhodně u obou elektrod. Narušení symetrie elektrod, kdy je jedna užší a druhá širší, ale způsobí, že vliv lokálního magnetického pole u užší elektrody ve struktuře převládne a bude určovat cirkulaci vzniklého víru, a u širší elektrody již víry nevznikají. Cirkulaci vzniklého víru je možno ovlivňovat směrem proudu, který protéká strukturou.
Pomocí metody, využívající indukované magnetické pole střídavým proudem a struktury umístěné na vodiči, byl ukázán vliv nesymetrie struktury či přítomnosti nečistot, které se projevují asymetrií gyrotropických trajektorií jádra víru [32] příslušných pro polaritu



Obrázek 2.9: Proudový impulz I_{pulz} indukuje impulz magnetického pole B_{pulz}, pomocí kterého je ovlivňována cirkulace magnetického víru v discích umístěných na zlatém vodiči. V obrázku je také vyobrazeno rentgenové záření, které bylo využito pro zkoumání vlastností víru a které bude více diskutováno v kapitole 2.4.4. Převzato z [28] a upraveno.



Obrázek 2.10: a) Koncept nesymetrického obvodu pro ovládání cirkulace v magnetické vrstvě. b) Zobrazení cirkulace vzniklých vírů při zvoleném směru elektrického proudu a jejich vychýlení působícím magnetickým polem. Při proudu tekoucím zobrazenou strukturou dolů vzniká magnetický vír s cirkulací CCW, při proudu směrem vzhůru vzniká vír s cirkulací CW. Převzato z [31].

víru ve směru nahoru a dolů. V perfektně symetrických strukturách bez nečistot by tyto trajektorie měly být stejné pro oba stavy polarity.

Vliv nečistot na dynamické chování magnetického víru byl zkoumán i cíleně, pomocí vzorků s cíleně připravenými nečistotami [33]. Nečistoty mohou vůči magnetickému víru mít charakter buď přitažlivý, nebo odpudivý. V případě přitažlivého charakteru nečistoty po dostatečně dlouhé době dojde k posunutí klidové polohy víru na nečistotu. Je-li charakter nečistoty odpudivý, nová klidová poloha bude kompromisem mezi co největší vzdáleností jádra víru od nečistoty a stabilním uspořádáním magnetického víru. Zjištěn

byl i fakt, že je-li magnetický vír přinucen vykonávat gyrotropický pohyb poblíž nečistoty, dochází při něm k fluktuacím.

Při experimentech s ovládáním cirkulace magnetického víru pomocí magnetických pulzů bylo pozorováno, že polarita nukleovaných vírů vykazuje náhodný charakter. Aby bylo možné při ovládání cirkulace ovládat současně i polaritu, musel by se disk během překlopení nacházet v magnetickém poli o směru kolmém na rovinu disku, případně lze polaritu ovlivnit vhodným tvarem struktury [28].

Kromě pozorování cirkulace a polarity je možné také sledovat chiralitu, tedy jejich součin. Princip, jak toho lze dosáhnout, nabízí teoretická studie využívající současného působení střídavého proudu procházejícího strukturou s vírem a střídavého magnetického pole, které je kolmé na směr procházejícího proudu [23]. Toho je možné dosáhnout dvěma vodiči, z nichž spodní slouží k indukci magnetického pole a na vrchním je umístěna struktura, kterou prochází proud. Odečítání pak může být odvozeno od amplitudy gyrace magnetického víru, která je opačná pro víry s chiralitou o velikosti 1 a -1, přičemž není nutné zjišťovat aktuální hodnoty cirkulace a polarity [23].

Zajímavé možnosti pro zjišťování vlastností magnetických vírů nabízí magnetorezistivita, což je materiálová vlastnost, která způsobuje změnu elektrického odporu v závislosti na změně magnetizace materiálu. Bylo ukázáno, že magnetorezistivita je možné využít jak pro určení cirkulace víru, tak i pro sledování polarity víru.

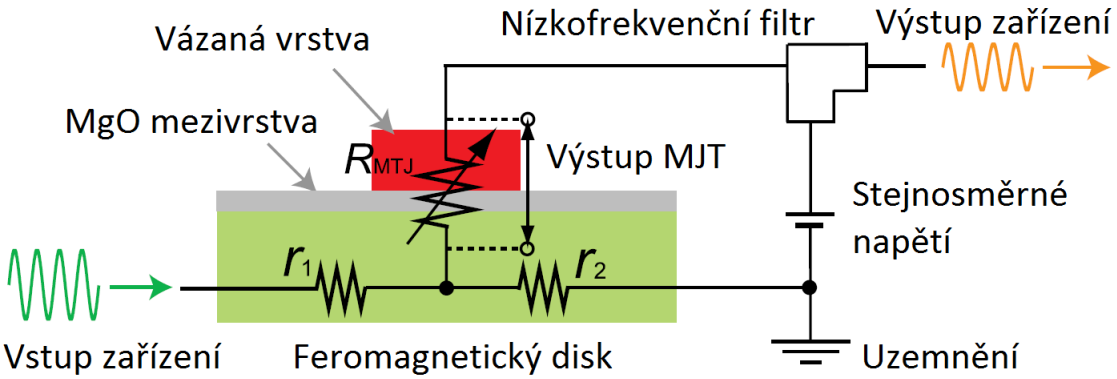
V případě určení cirkulace magnetického víru bylo využito i tzv. jevu anizotropní magnetorezistivity, při které bylo zjišťováno nerovnoměrné rozložení magnetizace disku, na který bylo působeno magnetickým polem. Tímto polem dochází k vypuzení víru mimo svou klidovou polohu, na základě signálu několika snímacích elektrod je možné určit směr posunutí, a tedy i cirkulaci magnetického víru [34, 35].

Varianta přístupu, která umožňuje sledovat vlastnosti magnetického víru v reálném čase, využívá magnetorezistivitu, resp. magnetického tunelového přechodu (dále MTJ, z angl. Magnetic Tunnel Junction). Schéma zapojení elektronického obvodu je zachyceno na obrázku 2.11. Vstupní střídavé napětí iniciuje gyrotropický pohyb magnetického víru ve feromagnetickém disku. Kvůli tomu dochází ke změně úhlu mezi magnetizací v disku a ve vázané vrstvě, což má za následek změnu odporu. Pomocí aplikovaného stejnosměrného napětí je tento odpor převáděn na napětí promítající se do výstupního signálu. Analýzou napětí na výstupu zařízení je možné získat z fázového posunu vstupního a výstupního signálu polaritu víru a z absolutní hodnoty odporu pomocí MTJ cirkulaci [36].

2.4 Metody pozorování magnetických vlastností

Rozvoj měřicích metod v několika posledních desetiletích umožnil pozorovat i magnetické vlastnosti magnetických vírů. Vzhledem k jejich zajímavým vlastnostem a předpovězeným oblastím jejich využití, které budou popsány v kapitole 2.5, na sebe magnetické víry strhávají poměrně velkou pozornost.

V této kapitole budou vybrané metody popsány. Největší pozornost bude věnována jedné ze sondových metod, mikroskopii magnetických sil, neboť jí bylo využito při experimentální kontrole správnosti navrženého konceptu, a to formou kontroly přítomnosti magnetického víru ve struktuře zvolených rozměrů. Bude popsán princip, na kterém je založena, a některé možnosti, které umožňuje.



Obrázek 2.11: Schematické zobrazení zařízení, které umožňuje sledovat polaritu magnetického víru v reálném čase na základě magnetického tunelového přechodu. R_{MTJ} je odpor magnetického tunelového přechodu, r_1 a r_2 přísluší odporům vyznačených částí feromagnetického disku. Mezivrstva z MgO slouží jako bariéra z nemagnetického materiálu mezi spodním a vrchním diskem. Převzato z [36] a upraveno.

Dále budou stručně popsány i metody využívající ke zjištění magnetických vlastností zkoumaného vzorku mikroskopii rastrovací sondou, magnetooptický Kerrův jev, elektronové mikroskopy či rentgenové záření. Zde uvedený výčet experimentálních metod není žádným způsobem definitivní, existují mnohé další metody a pokrok v již existujících metodách a hledání metod nových probíhá neustále.

2.4.1 Sondové metody

Roku 1986 byla světu představena nová metoda sondového typu, která nese název mikroskopie atomárních sil (dále AFM, z angl. Atomic Force Microscopy) [37]. Tato metoda je odvozena z propojení metod rastrovací tunelové mikroskopie (dále STM, z angl. Scanning Tunneling Microscopy) a hrotové profilometrie (v angl. Stylus Profilometry). Princip je založen na detekci sil působících mezi ostrým hrotem a zkoumaným povrchem (tedy odlišný princip než u STM, kde probíhá detekce tunelovacího proudu). Síly nemusí být obecně atomární, ale též např. magnetické či elektrostatické.

Podstatnou části měřicí sestavy pro AFM tvoří ostrý hrot. Ten je umístěn na ohebném raménku (též cantilever, původní anglický název je používán i v češtině) a působící síla je detekována sledováním velikosti prohnutí tohoto raménka. Prohnutí raménka je obvykle zaznamenáváno pomocí optických metod, například odrazem laserového paprsku od raménka do detektoru, kde dochází k vyhodnocení polohy raménka v závislosti na snímaném signálu.

Při měření AFM se obvykle používají dva módy, a to mód kontaktní a bezkontaktní. Jejich rozdíl spočívá především ve vzdálenosti hrotu od povrchu vzorku. V případě módu kontaktního je hrot udržován velmi blízko vzorku, kdy na něj působí odpudivé síly. Oproti tomu při bezkontaktním módu je vzdálenost hrotu od povrchu větší, a na hrot působí síly přitažlivé.

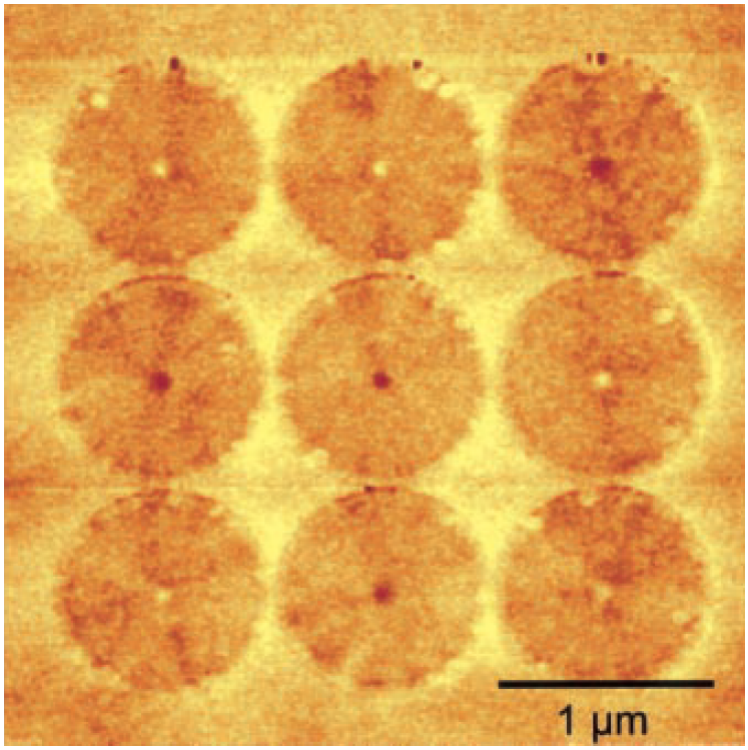
O rok později byla od AFM odvozena metoda, pomocí které lze zobrazovat magnetické vlastnosti materiálů, jež se nazývá mikroskopie magnetických sil (dále MFM, z angl. Magnetic Force Microscopy) [38]. Princip metody je v podstatě totožný jako v případě AFM, odlišný je především ze dvou hledisek. První odlišnost spočívá v použitém hrotu, v případě MFM musí být buď z magnetického materiálu, případně pokrytý vrstvou mag-

netického materiálu. Tento požadavek je nutné splnit, aby byl hrot citlivý i vůči magnetickým silám. Druhým požadavkem je poloha raménka s hrotem, která se při měření MFM nachází ve větší výšce než pro AFM měření. Vzhledem k tomu, že magnetické síly, vznikající především jako projev rozptylového magnetického pole vzorku, jsou dalekodosahové, a probíhá-li měření příliš blízko vzorku, do signálu získaného hrotem se promítá i signál příslušný topografii povrchu vzorku, čímž se interpretace získaného měření komplikuje. Měření MFM, vzhledem ke svému charakteru, probíhá vždy v bezkontaktním módu.

Měření magnetických sil je často prováděno i v tzv. lift módu, který spočívá ve dvou po sobě následujících průchodech nad povrchem vzorku. Při prvním průchodu je získána topografie vzorku a v průběhu druhého průchodu, který probíhá o předem zvolenou vzdálenost výše, jsou proměřeny magnetické síly. Pomocí těchto dvou průchodů v odlišných výškách nad vzorkem lze získat měření, ve kterých jsou od sebe projevy rozdílných sil odděleny (nedochází tedy k promítání topografie do magnetických sil apod.).

Pomocí metody MFM lze provádět měření jak amplitudy magnetické síly, tak i její gradient. Měření gradientu magnetické síly je vhodné pro měření vzorku, na kterém dochází k podstatným změnám magnetizace na relativně malé oblasti. Příkladem takovýchto změn mohou být např. doménové stěny nebo jádro magnetického víru.

Jádro magnetického víru v permalloyových strukturách bylo pomocí MFM poprvé zaznamenáno v roce 2000 [39]. Jádra vírů obou polarit ve strukturách o průměru 1 μm a výšce 50 nm jsou zobrazena na obrázku 2.12. Tím, že se podařilo jádro víru zaznamenat, byla existence magnetických vírů v daných strukturách experimentálně prokázána. Stejná skupina následně pomocí MFM studovala jádra vírů a antivírů [40] a také chování magnetických vírů v externím magnetickém poli [21].



Obrázek 2.12: Měření MFM permalloyových disků o výšce 50 nm a průměru 1 μm. Světlé a tmavé body ve středech disků odpovídají polaritám navzájem opačných směrů. Převzato z [39].

Pomocí MFM je možné magnetický vír nejen detekovat a změřit, ale při vhodně navržené konfiguraci také umožňuje vlastnosti víru ovlivňovat. Příkladem takového ovládání je změna cirkulace víru vyvolaná magnetickým polem hrotu MFM sondy [41].

Mezi tzv. sondové metody samozřejmě patří mikroskopie rastrovací sondou (dále SPM, z angl. Scanning Probe Microscopy) a metody od ní odvozené. Jedna z těchto odvozených metod se nazývá rastrovací tunelová mikroskopie (dále STM, z angl. Scanning Tunneling Microscopy) a její princip je založený na tunelovacím jevu mezi povrchem zkoumaného vzorku a hrotem sondy. Je-li využito spinově polarizovaného STM (dále SP-STM, z angl. Spin-Polarized STM) v prostředí vysokého vakua, je možné detekovat i jádro magnetického víru bez několika problémů, kterými trpí (již popsaná) MFM [42]. Jde především o lepší rozlišení, menší interakci hrotu sondy s magnetickým vírem a vyšší citlivost metody. Nevýhodou této metody je, že analyzované vzorky musí být vodivé.

2.4.2 Magnetooptický Kerrův jev

Ke zjišťování magnetických vlastností měřených vzorků je možné využít i metod optických, resp. magnetooptických. Jedna z nich spočívá ve změně polarizace dopadajícího záření při odrazu od magnetického materiálu. Popsaný jev se nazývá magnetooptický Kerrův jev (dále MOKE, z angl. Magneto-Optic Kerr effect). V případě lineární polarizace dopadajícího záření dojde odrazem ke změně polarizace na obecně eliptickou, přičemž dochází i k pootočení hlavní osy odraženého záření v závislosti na magnetizaci tělesa. Na základě analýzy odraženého záření lze pro měřený vzorek zjistit magnetizaci včetně příslušné hysterezní smyčky.

Této metody může být využito např. pro zjišťování hysterezních smyček struktur s magnetizací ve stavu magnetického víru. Naměřené smyčky umožňují například jednoduché určení velikosti magnetického pole při nukleaci a anihilaci [43].

2.4.3 Elektronová mikroskopie

Jedna z metod, pomocí které lze pozorovat magnetické vlastnosti zkoumaných vzorků pomocí elektronového mikroskopu, se nazývá Lorentzovská mikroskopie. Jde o metodu, kdy elektrony prochází vzorkem, takže je použitelná buď metoda transmisní (průchozí) elektronové mikroskopie (dále TEM, z angl. Transmission Electron Microscopy) nebo metoda rastrovací transmisní elektronová mikroskopie (dále STEM, z angl. Scanning Transmission Electron Microscopy). Metoda samotná umožňuje využít dvou odlišných uspořádání, která se nazývají Fresnelova a Foucaltova zobrazovací metoda. V obou případech jde o ovlivňování elektronů primárního svazku dopadajícího na vzorek magnetickými vlastnostmi vzorku. Experimentální využití lze nalézt např. v zobrazování magnetických domén [44] nebo cirkulace magnetických vírů, či jako komplementární metoda k MFM [45].

Další metoda, která využívá elektronových mikroskopů, resp. rastrovacích elektronových mikroskopů, je rastrovací elektronová mikroskopie se spinově polarizovanou detekcí sekundárních elektronů (dále SEMPA, z angl. Scanning Electron Microscopy with Polarization Analysis). Metoda je založena na měření polarizace spinu sekundárních elektronů, které jsou ze zkoumaného vzorku vyráženy ozařováním elektronového svazku. Tato metoda umožňuje souběžné měření polarity i cirkulace magnetického víru [46].

2.4.4 Metody založené na rentgenovém záření

Pro charakterizaci magnetických vlastností submikronových struktur je možné využít také polarizované měkké rentgenové záření. Princip rentgenové mikroskopie je obdobný, jako v případě optické mikroskopie. Rozdíl je především v použité optice, kdy je namísto čoček využito zonálních mřížek.

Kontrast metody při pozorování feromagnetických látek je založen na jevu nazvaném rentgenový magnetický cirkulární dichroismus (dále X-MCD, z angl. X-ray Magnetic Circular Dichroism). Principem je změna koeficientu absorpce kruhově polarizovaného rentgenového záření v závislosti na magnetizaci v blízkosti absorpční hrany. Ke studiu antiferomagnetických materiálů se využívá podobný princip, jen je použito lineárně polarizované rentgenové záření namísto kruhově polarizovaného (dále X-MLD, z angl. X-ray Magnetic Linear Dichroism) [47].

Existuje několik metod, které jsou od mikroskopie rentgenovým zářením odvozené. Propojení X-MCD a transmisního mikroskopu využívajícího měkkého rentgenového záření stálo za zrodem magnetické transmisní rentgenové mikroskopie (dále MTXM, z angl. Magnetic Transmission X-ray Microscopy) [47]. Podobná metoda, která ale slouží ke zkoumání povrchů vzorků, se nazývá rastrovací transmisní rentgenová mikroskopie (dále STXM, z angl. Scanning Transmission X-ray Microscopy). Metodu rastrovací transmisní rentgenové mikroskopie lze modifikovat i jako časově rozlišenou (dále TR-STXM, z angl. Time Resolved STXM), případně prostorově rozlišenou (dále SR-STXM, z angl. Space Resolved STXM).

Rentgenové záření nachází využití i v metodě zvané rentgenová fotoelektronová emisní mikroskopie (dále X-PEEM, z angl. X-ray Photo-Electron Emission Microscopy). Absorpce primárního rentgenového záření zkoumaným vzorkem generuje sekundární elektrony, které pomocí elektronové optiky o vysokém rozlišení vytvoří obraz magnetické struktury [47].

Rentgenového záření bylo využito např. pro přímé pozorování jádra magnetického víru (STXM) [32], překlápění polarity magnetického víru (STXM) [26], časového průběhu anihilace magnetického víru při dynamickém přepínání jeho cirkulace [28] (experimentální uspořádání bylo uvedeno výše na obrázku 2.9) či sledování dynamických vlastností jádra magnetického víru (X-PEEM) [25],

2.5 Využití magnetických vírů

Magnetické víry jsou zkoumány z hlediska jejich možného využití. V této kapitole bude představeno několik směrů, kterými by se mohla, případně se již začala ubírat jejich praktická aplikace.

Poměrně slibná je oblast jejich využití jako vysokorychlostního záznamového média (např. pevné disky v počítačích), proto je tomuto směru jejich aplikace věnována asi největší pozornost. Výhodou záznamového média založeného na magnetických vírech je především možnost k záznamu dat využívat dvou na sobě nezávislých veličin víru, polarity i cirkulace. Tím by jeden element, jehož velikost se může pohybovat v submikronovém měřítku, dokázal uchovávat dva bity informace, přičemž ke každému z nich lze využívat jinou metodu přístupu a zápisu nesené informace.

Návrhy, jak magnetických vírů využít jako paměťové médium, již existují. Provedení může být založeno např. na základě frekvence gyrotropického pohybu jádra víru, která se pro polarity magnetického víru směrem dolů a nahoru liší [48].

Další provedení paměti je navrženo na základě odečítání chirality magnetického víru ve struktuře. Výhodou tohoto návrhu je, že není nutné odečítat přímo polaritu nebo chiralitu, ale je zjišťována veličina tvořená jejich součinem. Nevýhodou je ztráta jednoho bitu, chiralita takto využitého víru může nabývat pouze hodnot ± 1 [23].

Jiný přístup k realizaci záznamového média může spočívat ve využití závislosti odporu materiálu na působící magnetické pole. Struktura, ve které se nachází magnetický vír, vykazuje odlišný odpor jak pro oba stavy cirkulace křivek magnetizace víru [34], tak pro stavy polarizace jádra magnetického víru [36], díky čemuž je možné cirkulaci, resp. polarizaci určit.

Doposud zmiňované aplikace magnetických vírů se týkaly symetrických disků. Existuje i odlišný přístup pro realizaci datových úložišť, který spočívá ve využití nesymetrických disků. Asymetrické tvary umožňují jednodušší a přesnější ovládání veličin magnetického víru, než je možné dosáhnout pro nanostruktury tvarů symetrických. Nesymetrické provedení disků může být ve formě kruhové úseče [49] či kruhové výseče [50], případně je možné nevyužít struktury plného disku, ale použít strukturu ve tvaru prstence [20].

Hledání vhodného využití magnetických vírů probíhá i jinými směry, než jsou datová úložiště. Vzhledem k velkému gradientu magnetického pole poblíž jádra magnetického víru by jich mohlo být využito v oblasti biotechnologie jako past pro biologicky funkcionalizované řetězce magnetických nanočástic [51].

Dalším návrhem, jak využít magnetické víry, je využít jejich vlastností jako senzory magnetického pole [3].

Kromě toho mohou nanostruktury, ve kterých vznikají magnetické víry, napomoci miniaturizaci členů logických obvodů. Příkladem může být provedení logických funkcí OR a XOR (logický součet a exkluzivní logický součet) pomocí tří vedle sebe umístěných disků [4]. Jako vstup logického členu slouží magnetické víry v krajních discích, výstupem je stav magnetického víru v prostředním disku. Princip je založen na umístění disků velmi blízko u sebe, díky čemuž dochází k ovlivňování výstupního magnetického víru víry vstupními. Pokud je použito jiné konfigurace disků s magnetickými víry, je možné realizovat i logickou funkci NOR (negovaný logický součet), která je úplným systémem logických funkcí, tzn. je možné pomocí ní realizovat logické funkce OR, NOR a NAND (negovaný logický součin), která je též úplným systémem logických funkcí.

Další možné využití magnetických vírů je ve formě tranzistoru. Tranzistor je v současné době základním prvkem elektronických obvodů, a to buď ve formě samostatné analogové součástky, nebo jako součást integrovaného obvodu. Snaha o další miniaturizaci tranzistorů bere v potaz i možnost použití magnetických vírů. V této oblasti je zatím provedena simulace a numerické výpočty, které naznačují, že magnetické víry by se mohly stát základním prvkem pro stabilní bipolární tranzistor [5].

3 Náhodná čísla

Náhodné jevy, pomocí kterých lze získávat náhodná čísla na základě pravděpodobnosti, začaly být podrobněji zkoumány v polovině 17. století, a to na základě hry v kostky. Otázkám, které se týkaly pravděpodobnosti výsledku hodu kostek, se začal zabývat Blaise Pascal, a jeho dopisy, které si vyměňoval s Pierrém de Fermatem, jsou první zdokumentovanou zmínkou o pravidlech pravděpodobnosti. Teprve v roce 1812 vyšla první fundamentální kniha o pravděpodobnosti, kterou sepsal Pierre-Simon, markýz de Laplace, ve které byly studovány náhodné jevy, aproximace náhodnosti, definice pravděpodobnosti a další. Následující fundamentální kniha v oboru pravděpodobnosti, po Laplaceovi teprve druhá, byla dílem Andreje Nikolajeviče Kolmogorova, vyšla v roce 1933, obsahovala axiomatický přístup k pravděpodobnosti a položila základ moderní teorie pravděpodobnosti [52].

Náhodné jevy, resp. náhodná čísla v současnosti nachází využití například pro hazardní hry, rozhodování v lidském chování, matematickém modelování, simulacích a výpočtech nebo pro šifrování.

Zařízení nebo algoritmus, pomocí kterého náhodná čísla získáváme, se nazývá generátor. Dle způsobu vytvoření náhodných čísel je možno generátory dělit na skutečně náhodné a pseudonáhodné. Toto rozdělení je spíše informativní, v praxi není neobvyklá ani kombinace generátoru skutečně náhodných a pseudonáhodných čísel.

Získáme-li z generátoru posloupnost čísel, je nutné zjistit, zda-li se opravdu jedná o čísla náhodná. K tomuto posouzení napomáhají testy náhodnosti, a to jak teoretické, zkoumající metodu generace čísla, tak i tzv. semiempirické, zkoumající vztahy mezi čísly v posloupnosti. Na základě výsledků těchto testů lze vyhodnotit, zda-li jsou na výstupu generátoru čísla náhodná, a dále např. jestli se hodí pro využití pro šifrování.

V této kapitole se nejprve zaměříme na vybrané vlastnosti náhodných čísel jejich generátorů. Následovat bude popis generátorů skutečně náhodných čísel s vybranými příklady. Poté budou představeny generátory pseudonáhodných čísel, včetně matematických postupů, které pro tvorbu čísel využívají, a tzv. extraktory, algoritmy, které jsou využívány pro zlepšování náhodnosti náhodných čísel. Kapitola bude uzavřena popisem testování náhodnosti čísel.

3.1 Vlastnosti náhodných čísel a generátorů

Na vlastnosti náhodných čísel i generátorů jsou kladeny určité požadavky. Tyto požadavky jsou v rámci této kapitoly shrnuty.

Prvním parametrem čísla je spojitost či diskrétnost. Dle charakteru generátoru mohou být jeho výstupem čísla spojitá či diskrétní. Toto je nutné brát v úvahu jak při využití generátoru, tak při použití testů náhodnosti čísel.

U čísel, jež jsou výstupem generátoru, nás zajímá jejich rozdělení. V případě náhodných čísel musí být rozdělení čísel rovnoměrné (uniformní), tedy každé číslo může být na výstupu se stejnou pravděpodobností, bez ohledu na čísla dřívější či budoucí. V případě hodu kostkou padá každé číslo s pravděpodobností $1/6$, v případě bitové posloupnosti 0,5.

Perioda je vlastnost, kterou lze číselně vyjádřit pouze u generátorů, které náhodná čísla vytvářejí pomocí matematických postupů. Požadavkem je, aby perioda byla co nej-

větší, tedy aby nedocházelo k opakování generované sekvence čísel. V případě náhodného fyzikálního procesu je perioda generovaných čísel považována za nekonečnou.

Další požadavek na generátor je jeho stabilita, resp. nezávislost. Jde především o stabilitu zařízení, jehož výstup by neměl reagovat na změny okolních podmínek, např. teploty, vlhkosti, magnetického pole atp. Těchto podmínek jde dosáhnout například umístěním generátoru do uzavřeného prostoru opatřeným termostatem o vhodně nastavené teplotě, do prostoru odstíněného vůči magnetickému poli atp.

V některých případech je kladen požadavek i na rychlost generování náhodných čísel. Některé generátory jsou schopné generovat jen několik náhodných čísel za sekundu, jiné za stejný časový úsek až několik stovek miliard. Před použitím generátoru pro konkrétní aplikaci je vhodné vzít rychlost generování v úvahu.

Kromě výše uvedených vlastností lze ještě určit několik aspektů, které jsou důležité pro jejich praktickou realizaci a využití. Jde především o znalost procesu a příslušných parametrů potřebných k bezchybné funkci kvalitního generátoru náhodných čísel na něm založeném, jednoduchost implementace, možnost provedení jako přenosné zařízení, možnost využití paralelních způsobů generování čísel a schopnost generování velkého množství náhodných dat [53]. Poslední jmenovaný atribut, tedy možnost generování velkého množství náhodných čísel, může být u určitých generátorů problematický, neboť pro ně je limit velikosti generovaného vzorku roven zhruba druhé odmocnině jejich periody [53].

Jako vlastnost generátoru náhodných čísel, resp. jím produkovaných čísel, lze považovat i entropii, jež udává hustotu informace. Pomocí této veličiny lze generátor náhodných čísel popsat kvantitativně.

Existují i další požadavky na generovaná náhodná čísla, které jsou zkoumány především pomocí statistických a tzv. semiempirických testů. Toto téma bude více popsáno v kapitole 3.5, která se jimi podrobněji zabývá.

3.2 Využití náhodných jevů

Náhodné jevy, resp. přímo náhodná čísla nacházejí využití pro mnohé způsoby. Jde především o hazardní hry, určité směry v umění, v matematických výpočtech a simulacích či pro kryptografii. Kromě uvedených oblastí, které budou více rozepsány, může sloužit také pro konání rozhodnutí v lidském životě, např. hodem kostkou či mincí o tom, jak se zachovat.

3.2.1 Hazardní hry

Hazardní hry, jako jsou např. hra v kostky, ruleta, loterie či některé karetní hry, jsou založeny na pravděpodobnostních jevech. Náhody využívají jak klasické hry, které se hrají fyzicky s reálnými předměty, tak v současné době i internetově provozované stránky, kde je konkrétní hra určitým způsobem zpracována pomocí algoritmů. Náhodných čísel bylo využíváno i pro britskou státní loterii od roku 1957, kdy náhodná čísla byla získávána počítačem ERNIE (akronym pro Electronic Random Number Indicator Equipment, tedy elektronické zařízení pro oznamování náhodných čísel) [54].

3.2.2 Umění

Náhody může být, poměrně překvapivě, využito i v umění. Příkladem může být tvorba dadaistické básně popsané Tristanem Tzarou. Postup spočívá v rozstříhání např. novinového článku na jednotlivá slova, jejich umístění do klobouku a následné losování. Tím, jak jsou jednotlivá slova postupně vytahována, je skládána báseň.

Kromě poezie nachází náhoda v umění uplatnění např. v malířství (např. náhodné lití barvy na plátno) či hudbě.

3.2.3 Matematické simulace

Náhodných čísel bývá běžně používáno pro matematické výpočty a simulace. Známá je metoda Monte Carlo pocházející z roku 1949 [55], u které je výpočet založen na náhradě výpočtů pravděpodobnostních integrálů procesů za vzorky sestávající z řetězů simulací jednotlivých dějů procesu.

Pomocí metody Monte Carlo je možno provádět výpočty určitých integrálů, odhadovat výsledky integrálů funkcí více proměnných, odhadovat nevlastní integrály obsahující integrand se singularitou či jdoucí přes neomezenou oblast, řešit některé lineární rovnice a jejich soustavy nebo odhadovat, zda-li je číslo prvočíslem [56].

Monte Carlo má využití i pro modelování v rámci teorii hromadné obsluhy, což je např. telefonní síť, benzínová stanice, pojišťovací společnost či databázové systémy v aplikacích internetových obchodů [56]. Byla využita i k modelování optimální polohy detektoru v experimentu COMPASS (akronym z angl. COmmon Muon and Proton Apparatus for Structure and Spectroscopy, tedy Společné mionové a protonové zařízení pro zkoumání struktury a spektroskopii) na urychlovači Super Proton Synchrotron (dále SPS) ve vědeckém středisku CERN (zkratka z Conseil Européen pour la Recherche Neucléaire, tedy Evropská rada pro jaderný výzkum) [57].

V současnosti se jako metoda Monte Carlo označuje použití náhodných veličin pro numerické výpočty, ale někdy se tak označuje jakékoliv použití počítačem generovaných náhodných čísel v programech (tedy např. i pro náhodné animace) [56].

Pro možnost opakování simulací či jejich kontroly je vhodnější využívat generátory pseudonáhodných čísel, které při stejných vstupních parametrech generují totožné posloupnosti čísel.

3.2.4 Kryptografie

Cílem šifrování je přenesení informace od odesilatele k příjemci bez toho, aby povahu informace zjistil kdokoliv jiný. Kryptografie nabízí nástroje, jakými toho dosáhnout. Je možné rozlišit dva směry kryptografie, a to tzv. klasickou a kvantovou kryptografii.

Počátky klasického šifrování lze vysledovat až do období starověkého Egypta v době přibližně 2000 let př. n. l., kdy bylo k zapsání informace použito hieroglyfů se speciálními významy [58]. Vývoj dále spočíval v posouvání či zaměňování písmen, a to o několik pozic, pomocí speciálních tabulek či pomocí speciálních přístrojů, z nichž je známý především německý šifrovací přístroj Enigma [59].

Dosud popsané metody lze označit jako symetrické, tedy že každému znaku či skupině znaků byl přiřazen znak jiný a pro šifrování i dešifrování byl používán stejný klíč. Roku 1976 byla navrhnuta metoda asymetrická spočívající v šifrování pomocí veřejného klíče

a dešifrování klíčem tajným, přestože zároveň nedošlo k její implementaci [60]. Ta byla poprvé provedena v roce 1978 jakožto protokol RSA [61], a později jako protokol ElGamal z roku 1985 [62].

Kvantová kryptografie je metoda poměrně mladá, jak její název napovídá, je založena na jevech kvantové fyziky, především na polarizaci fotonů, resp. na Einsteinově-Podolského-Rosenova paradoxu. Teoretický základ metody byl představen v roce 1984 a již na přelomu 80. a 90. let 20. století došlo k úspěšnému experimentálnímu provedení [63].

U šifrovaného přenosu informace existuje určitá šance, že bude odposloucháván či prolomen a informace zjištěna někým nežádoucím. Výjimkou je Vernamova šifra či též jednorázová tabulková šifra pocházející z roku 1917, u které je i matematicky dokázáno, že je neprolomitelná. K přenášené informaci je přičten zcela náhodný klíč o délce stejné, jako je délka zprávy, který je u příjemce odečten, přičemž každý klíč je nutné použít pouze jednou [58].

Náhodných čísel může být pro šifrování využito např. pro generování klíčů či dalších parametrů potřebných pro šifrování. Konkrétními oblastmi pro využití kryptografie jsou např. komunikační a informační systémy, ochrana autorských dat na optických discích, platební systém (3D secure), elektronické volby, elektronické peníze či řízení přístupu ke službám po síti [64].

3.3 Generátory skutečně náhodných čísel

Skutečně náhodnými čísly jsou označována čísla, která obvykle vznikají na základě nějakého fyzikálního jevu, který je spjat s pravděpodobností. Z toho důvodu jsou tyto generátory označovány jako generátory skutečně náhodných čísel (dále TRNG, z angl. True Random Number Generator).

Pomineme-li historické generátory (kostky, tahání loterie, házení mince atp.), moderní generátory náhodných čísel využívají fyzikální jevy, ve kterých nějakým způsobem vystupuje náhodnost. Často jde tedy o jevy kvantově mechanického charakteru, jakými jsou např. radioaktivita, jevy vyskytující se v elektronických obvodech či optoelektronika, případně jevy chaotické, kam lze zařadit např. atmosférické jevy. Pro generaci náhodných čísel jde ale využít i člověka, a to buď pomocí vybraných partií těla, nebo pomocí jeho chování.

V této kapitole jsou zmiňovány i vybrané procesy, kterých je využito k produkci náhodných čísel, která jsou brána jako vstupní parametry generátorů čísel pseudonáhodných. Tohoto postupu je využíváno např. u přístrojů, jejichž součástí není hardwarový generátor náhodných čísel, ale je možné nějakým způsobem čísla generovat pomocí jejich programového vybavení, či v případech, kdy kombinace generátoru skutečně náhodných a pseudonáhodných čísel zlepšuje vlastnosti náhodných čísel, např. z hlediska jejich využití pro šifrování.

Nyní budou vybrané fyzikální jevy či chaotické procesy podrobněji popsány, včetně nastínění principu generátorů, které je využívají.

3.3.1 Radioaktivita

Poločas rozpadu částice udává, za jakou dobu dojde v látce k rozpadu poloviny obsažených částic. Tento pohled je makroskopický, na atomární úrovni není možné přesně určit, u kterého atomu či molekuly nastane v daný okamžik rozpad. Poločas rozpadu je tedy veličina statistického charakteru, a je možné radioaktivního rozpadu prvků využít pro generátor náhodných čísel.

Typický příklad provedení generátoru, který je založený na radioaktivitě, spočívá v detekování částic vznikajících při radioaktivním rozpadu vhodně zvoleného prvku. Může jít například o izotop americia 241 sloužící jako zdroj částic pro scintilační detektor, jehož výstupem je analogový signál, který je následně zesílen a převeden do bitové podoby k dalšímu zpracování [6].

Podobné je využití izotopu cesia 137, jehož radioaktivní rozpad je zaznamenáván Geigerovou-Müllerovou trubicí, která je propojena s počítačem [7]. Tato metoda je provozována online pomocí webové stránky[1], na které je možné získat skutečně náhodná čísla online.

3.3.2 Elektronika

Generátory náhodných čísel, které jsou založeny na elektronických prvcích či zařízeních, často využívají šumu. Hlavním důvodem je, že typickou vlastností šumu je, že nelze přesně určit jeho časový průběh. Je možné rozeznat několik druhů šumu, které se od sebe liší především svým původem. Jde o šum tepelný (Johnsonův), výstřelový, blikavý, generačně-rekombinační a praskavý [65]. Šum je možno dělit i dle jeho frekvenčního spektra na různé barvy (využití analogie se světlem). Rozlišení dle barev tedy dává šum bílý, růžový, hnědý, modrý, purpurový, šedý, červený, oranžový, zelený a černý [65].

Pro generování náhodných čísel se používá především bílý šum, neboť je zastoupen přibližně stejně pro všechny vlnové délky. Může jít například o zařízení, která jsou určena přímo pro generování šumu, tzv. šumátory [65]. Příkladem může být také šum, který je získáván z obrazového a zvukového signálu webové kamery s mikrofonem [66]. Obecně by bylo možné používat jako zdroj šumu jakoukoliv elektronickou součástku, od rezistorů, přes diody (např. Zenerovu), po tranzistory a další součástky. Jít může nejen o analogové součástky, ale i o součástky digitální, např. logická hradla [8].

Může jít ale také o využití elektroenergetické sítě, kdy se náhodná čísla odvozují od měření špičkových výkonů v elektrické síti.

3.3.3 Optoelektronika

Náhodná čísla bývají často generována i na základě vlastností částic zprostředkovávajících interakci v elektromagnetickém poli, fotonů. Může jít např. o jejich interakci s optickými prvky, případně o využití specifických vlastností záření získávaného pomocí laserů.

Rozšířená je metoda generování skutečně náhodných čísel založená na šumu signálu laserů provozovaných na nízké úrovni intenzity signálu, resp. na fluktuaci kvantové fáze [10, 11, 12]. Protože je zesílená spontánní emise kvantový jev, nedochází k ní v předem určeném čase, ale náhodně. Z toho důvodu obsahuje produkovaný signál i šumovou složku,

[1] https://www.fourmilab.ch/hotbits/

která je po oddělení od zbytku signálu využita ke generování náhodných čísel. Jakožto šumovou složku lze považovat nestejnou frekvenci příslušnou jednotlivým fotonům záření.

Další experimentálně testovaná metoda je založená na detekování spektrálně oddělených šumových signálech ze superluminiscenční diody emitující světlo [13]. Tato metoda umožňuje získávat i několik signálů náhodných dat z jednoho zdroje světla současně, a to použitím filtrů, přes které emitované světlo prochází.

Další možnost, jak využít jednotlivých fotonů pro generování náhodných čísel, spočívá v náhodném výběru průchodu fotonu mezi dvěma optickými dráhami, které se od sebe liší délkou [14]. Dle okamžiku dopadu fotonu na detektor je možné rozlišit, zda-li foton procházel kratším či delším vlnovodným vláknem, a dle toho je mu přiřazena jedna bitová hodnota.

Princip generátoru skutečně náhodných čísel založený na průchodu fotonů děličem svazku byl úspěšně adaptován komerční sférou. Světové prvenství drží švýcarská společnost ID Quantique [67], která začala nabízet kvantové generátory náhodných čísel v roce 2004. Kromě prodeje generátorů náhodných čísel, např. ve formě USB zařízení či zásuvné karty pro osobní počítač, se jmenovaná společnost zabývá i kvantovou kryptografií.

3.3.4 Chaotické jevy

Chaotickými jevy lze označit takové jevy, které sice jsou deterministické, ale i malá odchylka počátečního stavu způsobí totožným jevům značně rozdílný průběh. Mezi tyto jevy lze zařadit například oblast meteorologie, do které spadá i atmosférický šum vznikající v důsledku úderů blesků při bouřkách, či turbulentní proudění, ale i pohyb planet ve Sluneční soustavě.

Mezi generátory náhodných čísel využívající chaotické jevy je možné zahrnout projekt LavaRand a jeho nástupce LavaRnd. Původní generátor LavaRand zpracovával fotografie hmoty plovoucí uvnitř lávové lampy do binárního řetězce, který sloužil jako vstupní parametr algoritmického generátoru. Nástupce LavaRnd již nevyužíval fotografie lávových lamp, ale obraz ke zpracování byl zachycován pomocí webové kamery s nasazeným krytem čočky. Internetová stránka generátoru LavaRand byla v provozu v letech 1997 až 2001, ale i v současnosti je zmiňována jako příklad online generátoru náhodných čísel, poté ji nahradila stránka projektu LavaRnd, která ale od ledna roku 2014 není v provozu [68].

Princip, nastíněný projektem LavaRand, tedy pořízení fotografie chaotického jevu, její zpracování do bitové posloupnosti a využití pro pseudonáhodný generátor, je v současnosti vhodný např. pro běžné mobilní telefony, které generátorem skutečně náhodných čísel vybavené nejsou [69]. Alternativou k fotoaparátu může u mobilních zařízení, tabletů či dalších podobných elektronických zařízení být např. mikrofon, rádiový přijímač, video kamera, dotykový displej či modul pro globální polohovací systém (GPS, z angl. Global Positioning System) [70].

Dalším vhodným způsobem, jak generovat náhodná čísla pomocí chaotického jevu, je využití atmosférického šumu [9]. Původ tohoto atmosférického šumu je především v bouřích, resp. v blescích. Princip generátoru je založený na snímání signálu rádia, jehož přijímač nesnímá žádnou rádiovou stanici, ale právě tento šum. Ten je následně využit pro další zpracování.

3.3.5 Lidské tělo a chování

Ke generování náhodných čísel je možné využít i samotného člověka. Může jít například o některé charakteristické prvky těla. Lze použít například otisky prstů, oční duhovku, lidskou tvář či hlas [17]. Popsané atributy lidského těla jsou pro každého jedince unikátní, lze jich tedy vhodným způsobem využít pro generování čísel.

Využít lze i určitého lidského chování, které často bývá nepředvídatelné. I přesto chovat se opravdu náhodně je pro člověka složité, ale je možné ho tomu naučit [71]. Protože ale sebevzdělávání pro náhodné chování není příliš běžné, pokud je třeba získat lidským chováním náhodné číslo, je vhodnější tak činit bez vědomí člověka a průběžně. Je-li člověk vyzván, aby nějakou činnost vykonával náhodně, velmi často při jejím provádění dojde k opakování určitého vzoru či vzorů a náhodnost se vytrácí. Příkladem použitelných činností může být sledování aktivity uživatele počítače na klávesnici či pohyby myší. Možností je třeba i sledování četnosti vysílání nebo přijímání dat (nikoliv konkrétní data) přes připojení na internet atp, ale některých těchto postupů lze pro generování využívat i bez lidského zásahu, např. komunikace po síti ve formě automatických aktualizací. Obvykle ale uvedené vlastnosti či chování člověka neslouží přímo jako zdroj náhodných čísel, ale jen jako vstupní atributy pro nějaký algoritmický generátor, což bude více popsáno dále.

3.3.6 Využití magnetických vírů

Vzhledem ke svým vlastnostem se pro využití jakožto generátor náhodných čísel nabízí i struktury, ve kterých dochází k opakované nukleaci a anihilaci magnetických vírů při absenci vnějšího magnetického pole.

V současné době dle odborné literatury ani dle veřejně dostupných patentů neexistuje generátor skutečně náhodných čísel založený na vlastnostech magnetických vírů.

Problematice pravděpodobnosti u magnetických nanostruktur je věnována studie pravděpodobnosti překlopení (tzn. nukleace a následná anihilace) magnetického víru v závislosti na délce a velikosti proudového impulzu, kterým je překlopení iniciováno. Překlopení víru je studováno s ohledem na vliv termické aktivace a elektromagnetického pole [72]. Aplikace této metody je však pro využití pro koncept generátoru náhodných čísel poměrně náročná, především kvůli zaručení stability doby trvání a velikosti proudového impulsu a kvůli nutnosti stability teploty okolí a vzorku samotného.

3.4 Generátory pseudonáhodných čísel

Rozvoj výpočetní techniky, programovacích jazyků i nemožnost mít vždy po ruce generátor skutečně náhodných čísel vedlo k rozvoji jiného typu generátoru. Místo fyzikálních jevů s pravděpodobnostním charakterem jsou využity vhodné (např. složité či jednosměrné) matematické funkce, pomocí kterých jsou generována čísla, která připomínají náhodná čísla. Tato čísla, získaná pomocí algoritmů, se nazývají pseudonáhodná, a programy, pomocí kterých jsou tato čísla vypočítávána, se označují jako generátory pseudonáhodných čísel (dále PRNG, z angl. PseudoRandom Number Generator), případně generátory algoritmické či deterministické. Vlastnosti obou typů generátorů a čísel jimi produkovaných jsou již diskutovány v kapitole 3.1. Za připomenutí zde stojí největší rozdíl v produkovaných číslech, tedy jejich perioda opakování vygenerovaných posloupností. V případě

skutečně náhodných čísel perioda neexistuje, resp. je považována za nekonečnou, v případě pseudonáhodných čísel perioda existuje a je nutné ji brát na vědomí.

Dle použitých matematických postupů či funkcí lze pseudonáhodné generátory rozdělit na dva druhy, a to na lineární a nelineární. Popis jednotlivých typů generátorů včetně konkrétních příkladů jejich provedení bude uveden v následujících podkapitolách. Po představení vybraných generátorů bude nastíněna idea extraktoru, který je silným nástrojem pro zlepšování kvality náhodných čísel, ovšem na úkor použitelného množství z celkového počtu generovaných čísel.

Jiná metoda, která navyšuje kvalitu čísel, resp. jejich náhodnost, spočívá ve využití skutečně náhodných čísel jako vstupních atributů generátoru pseudonáhodných čísel. Některé z těchto generátorů pseudonáhodných čísel již byly popsány v rámci předchozí kapitoly, další příklady budou uvedeny u jednotlivých typů PRNG. U těchto generátorů, resp. kombinací více generátorů, kdy výstup TRNG je vstupem PRNG, se používá označení entropické generátory náhodných čísel. Použitím skutečně náhodných čísel, která se navíc v čase mění, jako vstupu PRNG s dobrými statistickými vlastnostmi lze získat náhodná čísla dostatečné kvality, které lze použít pro kryptografii.

Posloupnost pseudonáhodných čísel se vyznačuje tím, že byla vytvořena pomocí matematických funkcí či různých výpočetních algoritmů. Kvalita generátoru pseudonáhodných čísel může být značně snížena použitím nevhodných vstupních parametrů, několik těchto příkladů bude také ukázáno.

Několik historických i současných způsobů implementace generátorů pseudonáhodných čísel je v následující podkapitole představeno.

3.4.1 Příklady pseudonáhodných generátorů

Jeden z prvních generátorů pseudonáhodných čísel pochází z roku 1946 a je založený na středních cifrách umocněného čísla, které slouží jako základ pro umocnění v dalším kroku. Další navržené generátory již využívají složitějších matematických funkcí. PRNG lze rozlišit na lineární a nelineární, ale toto rozdělení jen podává informaci, zda-li je použitá metoda generování lineární či není. Je vhodnější generátory členit do kategorií na základě samotné metody, podle které je pak kategorie pojmenována.

Roku 1949 byl navržen lineární kongruenční generátor (dále LCG, z angl. Linear Congruent Generator), jehož variantu navrhl Lehmer [73]. Tento generátor lze v obecném tvaru uvést rovnicí

$$X_{n+1} = (a \cdot X_n + c_{\mathrm{LCG}}) \bmod m, \tag{3.1}$$

kde n je přirozené číslo udávající, o který člen posloupnosti jde, m modul, přičemž $0 < m$, mod m je zbytek po celočíselném dělení dělitelem m, a násobitel, přičemž $0 \leq a \leq m$, c_{LCG} inkrement, přičemž $0 \leq c_{\mathrm{LCG}} \leq m$, X_n naposledy vygenerovaný člen posloupnosti a X_{n+1} nově generovaný člen posloupnosti náhodných čísel [73]. Pro výběr prvního, resp. nultého čísla posloupnosti platí, že $0 \leq X_0 \leq m$. Vzhledem k tomu, že první člen dává vzniknout celé posloupnosti, bývá označován jako semínko (z angl. výrazu seed).

Vlastnosti konkrétního generátoru se odvíjejí od volby těchto uvedených parametrů. Příkladem může být například volba inkrementu c_{LCG}, je-li nulový, náhodná čísla jsou generována rychleji než v případě c_{LCG} nenulového, ale na úkor velikosti periody. Varianta LCG s inkrementem $c_{\mathrm{LCG}} = 0$ se nazývá multiplikativní, a v případě $c_{\mathrm{LCG}} \neq 0$ je metoda generování označována jako smíšená [73].

Od obecného lineárního kongruenčního generátoru jsou odvozeny různé modifikace. Jedna z nich spočívá ve využití více předchozích členů vygenerované posloupnosti pro výpočet členu nového. Mezi tyto generátory patří např. zpožděný Fibonacciho generátor, který vychází z rekurzivní Fibonacciho posloupnosti (dále LFG, z angl. Lagged Fibonacci Generator). Jinou modifikací je tzv. míchání, kdy je člen posloupnosti určován pomocí více nezávislých LCG [74].

Generátory založené na lineárních posuvných registrech se zpětnou vazbou (dále LSFR, z angl. Linear Feedback Shift Register) spočívá ve změně bitů v jednotlivých registrech v průběhu každého cyklu generování. Zpětná vazba je realizována pomocí logických funkcí exkluzivního součtu (XOR), nebo exkluzivního negovaného součtu (XNOR), a to v závislosti na konkrétní implementaci generátoru.

Na operacích s obecnými registry se zpětnou vazbou (dále GSFR, z angl. Generalized Feedback Shift Register) je založený generátor nazvaný Mersenne twister [16]. Od jeho představení v roce 1998 stále vznikají modifikace od něj odvozené.

Další kategorií PRNG jsou generátory založené na součtu s přenosem (dále AWC, z angl. Add With Carry) [75]. Princip generování čísel spočívá v součtu dvou předchozích vygenerovaných číslech a tvz. přenosového bitu (angl. carry bit), tento součet je celočíselně dělen číslem 10 a zbytek je hledané nové číslo. Následující přenosový bit je nastaven jako 0 či 1 dle toho, zda-li součet přesáhl hodnotu 10. Před započetím generování je tedy nutné zvolit první dvě čísla posloupnosti a přenosový bit.

Podobnou kategorií, která je ale založena na jiném aritmetickém postupu, je rozdíl s výpůjčkou (dále SWB, z angl. Substract With Borrow) [75]. Nové číslo je generováno jako zbytek po celočíselném dělení (např. číslem 10) rozdílu, při kterém je od předpředchozího čísla odečteno číslo předchozí a přenosový bit. Je-li výsledek rozdílu kladný, stává se novým číslem posloupnosti a přenosový bit je nastaven na hodnotu 0, pokud je výsledek rozdílu záporný, k číslu se přičte 10 a přenosový bit je nastaven na hodnotu 1. Stejně jako u předchozí kategorie generátorů je před započetím výpočtů posloupnosti nutné nastavit její první dva členy a přenosový bit.

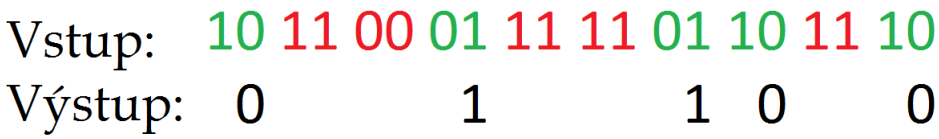
Doposud popsané generátory náhodných čísel lze vzhledem k použitým metodám nazvat jako lineární. Záměnou lineární funkce lze získat generátor nelineární. V případě multiplikativního kongruenčního generátoru se pak takový generátor označuje jako inverzivní kongruenční generátor.

Jiný typ nelineárního generátoru lze získat např. využitím vybrané mocninné funkce. Generátor, který pochází z roku 1986 a využívá kvadratickou funkci, se po svých autorech nazývá Blum Blum Shub [15].

3.4.2 Extraktory

Jako extraktor je označován matematický postup, který umožňuje ze statistického hlediska zlepšit náhodnost posloupnosti čísel, která byla získána pomocí generátoru náhodných čísel. Extraktor lze definovat jako algoritmus, který transformuje rozdělení posloupnosti čísel o slabé náhodnosti na téměř uniformní distribuci pomocí malého množství dodaných náhodných čísel [76].

Jednoduchým extraktorem je von Neumannův extraktor. Vstupní data, kterými je bitová posloupnost, jsou rozdělena na dvojice bitů. Jsou-li bity dvojice shodné (tedy hodnoty 00 a 11), tato dvojice není nijak využity. Liší-li se bity dvojice (hodnoty 01 či 10),



Obrázek 3.1: Vstup a výstup von Neumannova extraktoru.

tato dvojice se použije a na výstupu extraktoru se objeví druhá číslice této dvojice. Schematické znázornění funkce von Neumannova extraktoru je uvedeno na obrázku 3.1.

Další extraktory mohou vycházet z různých předpokladů, např. z tzv. XOR-podmínky (v angl. XOR-condition), která je založena na logické funkci exkluzivního součtu [77].

3.5 Testování generátorů náhodných čísel

Získáme-li z generátoru posloupnost čísel, před jejím použitím je nejprve vhodné zjistit, zda-li se skutečně jedná o čísla náhodná. Toho je dosaženo pomocí testování, které lze shrnout do dvou skupin. Těmito skupinami jsou testy teoretické a semiempirické. Oproti oběma jmenovaným skupinám si výsadní postavení nese test spektrální, který bude také v rámci této kapitoly přiblížen. Před provedením testů, a to jak teoretických, tak semiempirických, je obvyklé provést χ^2 test v případě diskrétní povahy testovaných čísel (např. bitová posloupnost), nebo Kolmogorovův-Smirnovům test pro čísla spojitá. S jistotou nelze říci, že při dalším průchodu generátor neselže, jde jen o zvyšování důvěry v náhodnost produkovaných čísel a posloupnost předpokládáme za náhodnou, dokud generátor v nějakém testu neselže [73]. Pokud generátor selže v některém testu, znamená to, že je nevyhovující.

Po představení základních způsobů testování náhodných čísel budou uvedeny i některé tzv. baterie testů, tedy vybrané sady testů, které byly vybrány pro zkoušení náhodnosti získaných čísel. Na základě získaných výsledků lze nejen vyjádřit, zda-li generátor produkuje náhodná čísla, ale i zda-li generovaná čísla jsou vhodná pro využití v kryptografii, což lze posoudit na základě tzv. kryptografických standardů.

Kvalitu, resp. statistické vlastnosti čísel produkovaných generátorem, je možné určit pomocí různých testů. Tyto testy mohou být použity jak pro určování kvality nových generátorů, tak pro výběr generátoru pro konkrétní užití, víme-li, jaké parametry požadujeme. Na základě některých testů je možné generátory náhodných čísel, a to jak skutečně náhodných, tak pseudonáhodných, ohodnotit pro vhodnost jejich využití pro šifrování.

3.5.1 χ^2 test

Je-li posloupnost testovaných čísel nespojitá, provádí se nejprve χ^2 test. Jde o statistický rozbor dostatečného množství na sobě nezávislých pozorování (posloupností čísel), jehož výsledkem může být konstatování, že generátor testem neprošel a čísla nejsou dostatečně náhodná, nebo že náhodnost čísel je podezřelá, případně téměř podezřelá. Je obvyklé testování provádět třikrát s různými čísly, a pokud vyjde náhodnost čísel dvakrát ze tří testů podezřelá, čísla nepovažujeme za dostatečně náhodná. Podrobnější popis procedury testování pomocí χ^2 testu je možné nalézt v [73].

3.5.2 Kolmogorovův-Smirnovův test

Je-li předmětem zkoumání reálné náhodné číslo, které může nabývat hodnot např. v intervalu $< 0, 1 >$, je základním testem Kolmogorovův-Smirnovův test (dále KS). Tento test je založen na rozdílu mezi distribuční funkcí získaných čísel $F(x)$ a tzv. empirickou distribuční funkcí $F_n(x)$, kterou je možné získat z n nezávislých pozorování náhodné veličiny X. Z porovnání jsou získány statistické koeficienty, na základě kterých je možné statisticky posoudit náhodnost podobně, jako v případě χ^2 testu uvedeném v předchozí kapitole. Test je podrobněji představen v [73].

3.5.3 Teoretické testy

Tyto testy lze popsat jako podrobení použité metody generování náhodného čísla matematické analýze kompletního výstupu generátoru. Tyto testy vychází z teorie čísel a analytického rozboru metody, pomocí které byla náhodná čísla získána. Vzhledem k tomu, že je nutné je provádět s ohledem na zvolený generátor náhodných čísel, tak zde nebudou více popisovány.

3.5.4 Semiempirické testy

Semiempirické testy lze chápat jako takové testy, které zkoumají nikoli všechny možné posloupnosti tvořené generátorem náhodných čísel, ale jako testy, které jsou vykonávány nad konkrétními posloupnostmi získanými z tohoto generátoru, popř. nad vybranými částmi posloupnosti. Při tomto testování dochází k manipulaci se skupinami čísel, která jsou vyhodnocována statisticky.

Tyto testy, přestože byly datovány již dříve, jsou poprvé komplexně shrnuty v [73], a na základě tohoto uvedeného zdroje zde budou popsány. V průběhu času se staly i určitým základem pro pozdější baterie testů, proto zde budou podrobněji uvedeny.

Ekvidistribuční (frekvenční) test je zaměřen na kontrolu, zda-li zkoumaná posloupnost vykazuje rovnoměrné rozdělení. K tomu je využito, dle charakteru posloupnosti, buď χ^2 testu nebo KS testu.

Sériový test zjišťuje, zda-li jsou v posloupnosti rovnoměrně rozdělené také dvojice po sobě jdoucích čísel. Tento test lze provést i pro trojice či čtveřice čísel.

Mezerový test je nazván dle předmětu zkoumání. V rámci tohoto je zvoleno číslo (či dvojice čísel) a sledována je vzdálenost (mezera) mezi výskyty tohoto čísla (resp. čísel). Na zjištěné počty mezer o různých velikostech je poté použit χ^2 test.

Pokerový (rozkladový) test rozdělí testovanou posloupnost čísel po pěti následujících čísel a poté v těchto pěticích prověřuje zastoupení jednotlivých čísel.

Test sběratele kupónů je založen na kontrole délek částí posloupnosti čísel, které obsahují všechna předem zvolená čísla. Příkladem, podle kterého je tento test ostatně nazván, spočívá v nasbírání celé sady různých kupónů umístěných náhodně v krabicích cereálií, a jde tedy o to, kolik krabic je nutné pro získání celé sady kupónů otevřít.

Permutační test spočívá v rozdělení posloupnosti na úseky stejné délky, a v jejich rámci je pozornost věnována tomu, zda-li všechny možné permutace jednotlivých číslic jsou rovnoměrně rozděleny.

Úsekový test v testované posloupnosti čísel zkoumá délky monotónních úseků. Může jít o úseky jak rostoucí, tak i klesající. Získané počty úseků jsou poté podrobeny statistickému rozboru.

Test maxima z t spočívá v rozdělení testované posloupnosti na kratší úseky stejné délky. Poté je pro každý tento úsek nalezeno maximum, a na zjištěná maxima všech úseků je aplikován χ^2 test.

Kolizní test zkoumá tzv. kolize generátoru. Princip testu lze popsat příkladem, kdy dochází k náhodnému házení míčků do nádob, kterých je mnohem více než míčků. Většina míčků padne do prázdné nádoby, ale může dojít i k tomu, kdy v nádobě skončí více než jeden míček. Situace, kdy je míček vhozen do urny, kde již nejméně jeden míček je, se nazývá kolize. Tento test zjišťuje počet kolizí, a aby jej generátor splňoval, musí určitý počet, ale ne příliš vysoký, vykazovat.

Narozeninový test (resp. test odstupu narozenin) lze přiblížit podobným příkladem jako test kolizní, ale zde místo míčků v nádobách jde o narozeniny v průběhu roku. Tento test posléze zkoumá počet dnů (velikost úseku posloupnosti) mezi sousedními narozeninami.

Sériový korelační test vychází z teorie statistiky, a to konkrétně z výpočtu sériového korelačního koeficientu posloupnosti a následného posouzení vzájemné závislosti čísel.

Testy vybraných posloupností zkoumají nikoliv posloupnost, která je výstupem generátoru, ale je z ní nějakým způsobem odvozena. Může tedy jít o posloupnost, která je tvořena každým druhým, třetím, ... členem původní posloupnosti. Na tuto novou posloupnost je poté možno použít výše popsané testy. Důvodem pro testování takto určených posloupností je, že programy, které využívají generátory náhodných čísel, si mohou v každém kroku zavolat stejný počet náhodných čísel, které využívají např. pro proměnné pro další výpočty. Proto je nutné, aby dostatečnou náhodnost vykazovaly i vybrané posloupnosti odvozené z generátorem vytvořené posloupnosti.

3.5.5 Spektrální test

V případě spektrálního testu, který v sobě zahrnuje vlastnosti teoretických i semiempirických testů, jde o nejsilnější známý test. Všechny dobré generátory tento test splnily a všechny špatné jím neprošly [73].

Spektrální test je založen na rozdělení testované posloupnosti na úseky o délce n tvořené po sobě následujícími členy posloupnosti. Jednotlivým úsekům je následně přiřazen charakter souřadnice v n-rozměrném prostoru, tedy pro $n = 2$ jde o dvojice následujících členů posloupnosti, které se zobrazují v rovině, v případě $n = 3$ jde o trojice po sobě jdoucích členů, které udávají souřadnice bodu v krychli atd. Vyhodnocení testu je poté založeno na rozložení a vzájemné poloze bodů v příslušném n-rozměrném prostoru. Podrobný popis tohoto testu a jeho vyhodnocení lze nalézt v [73].

3.5.6 Vybrané baterie testů

Označení baterie testů nesou sady vybraných, obvykle semiempirických testů. Pomocí baterií testů lze komplexně otestovat vlastnosti čísel produkovaných generátorem, a na základě výsledků stanovit, zda-li jsou čísla dostatečně náhodná.

Jako baterii testů by bylo možné označit i testy uvedené v [73] a již popsané v kapitole 3.5.4, přestože se tak běžně neděje. Dalšími bateriemi testů jsou např. DIEHARD [78], testy zahrnuté v SPRNG [79], softwarová knihovna implementovaná v jazyku ANSI C nazvaná TestU01 [80], sada testů popsaných v Standardu federálního zpracování informací 140-2, bezpečnostní požadavky na kryptografické moduly (dále FIPS PUB 140-2, z angl.

Federal Information Processing Standard) Národního institutu standardů a technologie Spojených států amerických (dále NIST, z angl. National Institute of Standards and Technology) [81], či vybrané testy v programu pro testování náhodných čísel ENT [82].

Baterie DIEHARD nejprve vyšla na kompaktním disku společně s připravenými daty s náhodnými čísly. Testy z kapitoly 3.5.4 byly v rámci baterie rozšířeny o další semiempirické testy. Testy v této baterii vyžadují vstupní posloupnosti ve 32bitovém formátu.

Knihovna TestU01 obsahuje empirické statistické testy pro generátory náhodných čísel. Zahrnuje jak testy pro posloupnosti reálných čísel v intervalu (0,1), tak i pro posloupnosti bitové. Kromě testů uvedených výše v kapitole 3.5.4 baterie obsahuje i další semiempirické testy.

SPRNG, kromě knihovny generátorů náhodných čísel, zahrnuje i sadu testů, které ověřují kvalitu posloupností náhodných čísel generovaných sériovými či paralelními generátory. Kromě testů semiempirických, které jsou popsané v kapitole 3.5.4, obsahuje i tzv. testy náhodnosti založené na fyzikálních jevech (dále PBRT,z angl. Physically Based Randomness Tests), kterými jsou *Isingův model* a tzv. *test náhodné procházky*.

Další baterii testů bylo možné nalézt ve FIPS PUB 140-2 [81]. V této směrnici byly předepsány 4 statistické testy, které ale byly ze současné verze dokumentu bez náhrady odstraněny. Těmito testy byly *frekvenční test* (monobit), *pokerový test*, *úsekový test* a *test dlouhých úseků*. Tyto testy byly předepsány pro bitovou sekvenci z 20000 bitů, a pokud se výsledek nějakého testu nachází mimo předepsané hodnoty, generátor je považován jako špatný. V případě monobitového testu musel být počet 1 v rozmezí $(9725 < Y < 10275)$, kde proměnná Y je v tomto i dalším popisu podmínek pro projití dřívějšími testy FIPS PUB 140-2 rozhodující parametr pro testované sekvence bitů. V případě pokerového testu je bitová posloupnost rozdělena na 5000 4bitových úseků a následně je zjištěn počet všech vyskytujících se kombinací čísel. Po vyhodnocení, jež je dáno pomocí vztahu

$$Y = \frac{16}{5000} \cdot \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000, \tag{3.2}$$

kde $f(i)$ odpovídá jednotlivým výskytům kombinací, lze v případě platnosti nerovnosti $(2,16 < Y < 46,17)$ konstatovat, že generátor testem prošel, v opačném případě generátor v testu neuspěl. Úsekový test počítá výskyt úseků o délce 1, 2, 3, 4, 5 a 6 a více stejných bitů. Povolená množství úseků těchto délek, která generátor musí pro všechny úseky splňovat, aby testem prošel, jsou uvedena v tabulce 3.1.

délka úseku	1	2	3	4	5	6+
povolené množství	2267–2733	1079–1421	502–748	223–402	90–223	90–223

Tabulka 3.1: Povolené počty úseků daných délek. Převzato z [83].

Posledním testem z této baterie byl test dlouhého úseku. Tímto testem generátor projde, pokud na jeho výstupu není úsek jedniček či nul o délce 26 či více stejných bitů. Parametry, na základě kterých se určuje, zda generátor testy projde či neprojde, byly pro testy dříve uvedené ve FIPS PUB 140-2 převzaty z publikace srovnávací FIPS PUB 140-2 vůči předchozí verzi FIPS PUB 140-1 [83].

Pro orientační zjištění vlastností generátoru lze také využít baterii testů ve formě volně přístupného programu ENT, který v sobě zahrnuje test entropie, χ^2 test, výpočet aritmetického průměru $\overline{x}$, určení hodnoty π pomocí metody Monte Carlo a koeficient sekvenční korelace [82]. Test entropie udává hustotu informace jako počet bitů o hodnotě

1 v bytu (osmi bitech). χ^2 test včetně jeho interpretace již byl popsán dříve. V případě aritmetického průměru jde o součet bytů a následné podělení jejich počtem. Pro zcela náhodné číslo by tento průměr dosáhl hodnoty 127,5. Výpočet hodnoty π pomocí metody Monte Carlo spočívá v rozdělení sekvence na 6bytové úseky, přičemž každá dvojice těchto po sobě jdoucích úseků tvoří souřadnice x a y uvnitř čtverce. Následně je určena vzdálenost každého takového bodu v čtverci a zjištěno, zda-li spadá či nespadá do kruhu čtverci vepsanému. Na základě poměru bodů uvnitř a mimo kruhu lze vypočítat hodnotu π, která by se pro posloupnost náhodných čísel (dostatečné délky) měla blížit její správné hodnotě. Koeficient sériové korelace C zjišťuje závislost bytu předchozího na bytu následujícím. Koeficient nabývá hodnot v intervalu $C \in < -1, 1 >$, v případě náhodné sekvence bude koeficient blízký nule, v případě nenáhodné sekvence se bude blížit hodnotě $|1|$.

Při použití uvedených testovacích baterií či jednotlivých testů je nutné vzít na vědomí, že jde o testování čísel z hlediska statistických vlastností. V případě PRNG lze na jejich základě jednoduše zjistit vhodnost generátoru pro uvažovanou aplikaci. V případě TRNG ale může být rozhodování na základě výsledků těchto testů ošidné, neboť takový generátor může generovat skutečně náhodná čísla, která se ale ze statistického hlediska budou jevit jako nenáhodná.

3.5.7 Kryptografické standardy generátorů

Ne každý generátor náhodných čísel je vhodný pro šifrování. Proto, aby bylo rozhodnutí podloženo nějakými argumenty či doporučeními, existují i určité kryptografické standardy generátorů.

Jednou z takových norem je např. již zmiňovaný standard FIPS PUB 140-2 [81], který je vyvinutý a vydávaný Odborem počítačové bezpečnosti NIST. V rámci tohoto standardu jsou pro kryptografické moduly (generátory) stanoveny 4 úrovně, které popisují nutnost a četnost jejich testování, dále popisuje požadavky na bezpečnost generátoru náhodných čísel z různých ohledů (např. design, implementaci či ovlivňování okolím) či seznam schválených generátorů. Tento dokument byl aktualizací již zastaralé směrnice FIPS PUB 140-1, a v době opět probíhá proces schvalování novějšího standardu FIPS PUB 140-3.

Dalším příkladem mohou být Standardy pro kryptografii s veřejným klíčem (dále PKCS, z angl. Public-Key Cryptography Standards) [84]. V tomto případě jde o skupinu standardů pro šifrování veřejným klíčem, které vychází pod hlavičkou RSA Laboratories ve spolupráci s vývojáři zaměřenými na bezpečnost z celého světa. Účelem těchto standardů je urychlení procesu jejich rozšíření, díky čemuž dojde i k navýšení bezpečnosti šifrovaných dat. První standard PKCS#1 byl uveřejněn v roce 1991, zatím posledním vydaným standardem je PKCS#15 verze 1.1.

4 Koncept generátoru a technologie výroby

Navržený generátor náhodných čísel je založený na vlastnostech magnetických vírů vznikajících v nanostrukturách vhodného tvaru, rozměrů a materiálu. Při splnění několika podmínek, kterými jsou spontánní nukleace magnetického víru v nulovém vnějším magnetickém poli, symetrie disku a nepřítomnost defektů či nečistot na disku, jsou veličiny nukleovaného víru nezávislé na stavu předcházejícího (již anihilovaného) víru.

Princip takového generátoru je postavený na myšlence sestávající z několika kroků. Nejprve v nanostruktuře ve tvaru disku nukleuje magnetický vír za nepřítomnosti externího magnetického pole. Vlastnosti tohoto víru (případně jen jedna či několik vybraných, není nutné zjišťovat všechny) jsou vyčteny a vír je dostatečně silným magnetickým polem anihilován. Poté je možné opakovat oba uvedené kroky do té doby, než bude vyčteno požadované množství dat k dalšímu zpracování.

Generátor náhodných čísel, jehož koncept je v následujícím textu podrobně představen, byl připravován pomocí přístrojů patřících do Laboratoře odboru povrchů a pevných látek Ústavu fyzikálního inženýrství Fakulty strojního inženýrství Vysokého učení technického v Brně (dále ÚFI FSI VUT) [85] a přístrojů Laboratoře přípravy a charakterizace nanostruktur Středoevropského technologického institutu (dále CEITEC, z angl. Central European Institute of Technology) [86]. Při výrobě bylo využito především metody elektronové litografie, depozice tenkých vrstev pomocí naprašování iontovým svazkem a iontového odprašování fokusovaným iontovým svazkem. Tyto metody, včetně jednotlivých provedených kroků při přípravě vzorků, jsou v této kapitole detailněji nastíněny.

4.1 Koncept generátoru

Koncept navrženého generátoru náhodných čísel v sobě zahrnuje vhodně zvolenou nanostrukturu, ve které dochází ke vzniku magnetického víru s náhodnými veličinami, a vhodně zvolenou metodou, pomocí které jsou tyto veličiny odečítány.

V této kapitole je podrobněji popsána volba vhodné nanostruktury a veličiny, která je využita ke generování náhodných čísel, dále je nastíněna zvolená metoda, jak je tato veličina odečítána, a poté je představen princip zpracování získaných dat. V závěru kapitoly je koncept a jeho jednotlivé části shrnut.

4.1.1 Struktura s magnetickým vírem

Základním elementem generátoru náhodných čísel je nanostruktura vhodného tvaru a rozměrů z magneticky měkkého materiálu, ve které je magnetizace ve stavu magnetického víru.

Vhodným tvarem struktury je symetrický plochý disk bez defektů či nečistot. V tomto případě neexistuje žádná anizotropie tvaru v rovině tělesa, takže jsou stavy cirkulace CW i CCW degenerované [24], tedy oba stavy jsou rovnocenné a při nukleaci mohou nastat se stejnou pravděpodobností

V případě disku je nutné zvolit dva parametry, a to jeho průměr a výšku, resp. tloušťku vrstvy. V případě průměru je nutné brát na zřetel, že nesmí být příliš velký, aby se v disku

stav magnetizace nacházel v podobě magnetického víru a nikoliv jako multidoménový stav, ale musí být dostatečně velký, aby samovolně nepřecházel do stavu jednodoménového. Příliš malý průměr disku může být problematický také při nanášení kontaktů. Průměr disků, které byly experimentálně testovány, leží v rozmezí od jednoho do čtyř mikrometrů.

Druhým parametrem disku je jeho výška. Ta musí být dostatečně velká, aby v nanostruktuře mohl vzniknout magnetický vír, ale přitom musí být poměr výšky a průměru disku dostatečně malý.

4.1.2 Odečítání dat

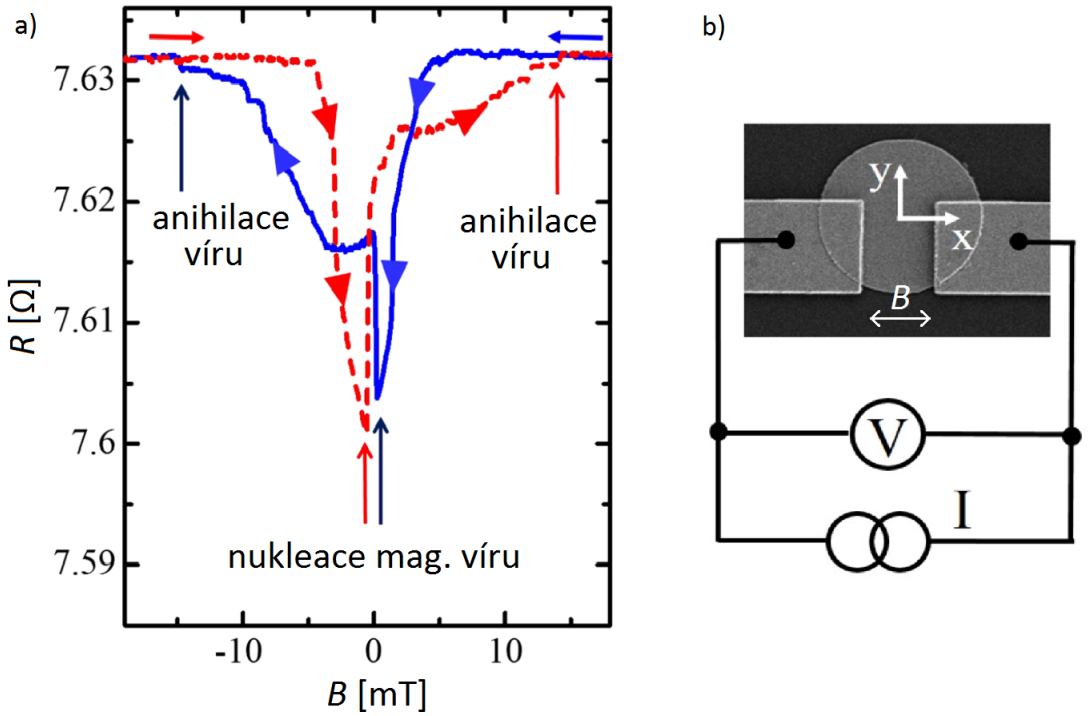
Máme-li jako nanostrukturu zvolený symetrický plochý disk a jako rozhodující veličinu cirkulaci, je nutné najít vhodnou metodu, pomocí které lze její chování jednoduše, přesně a nepříliš zdlouhavě zjišťovat.

Metoda, která těmto požadavkům vyhovuje, je např. anizotropní magnetorezistivita (dále AMR, z angl. Anisotropic MagnetoResistance). Magnetorezistivita je vlastnost materiálu, která se projevuje změnou odporu v závislosti na magnetizaci. Příklad takové závislosti odporu nanostruktury, která je ve tvaru disku a jejíž magnetizace se nachází ve stavu magnetického víru, je zachycena na obrázku 4.1, a to včetně příslušného experimentálního uspořádání. Z obrázku je patrné, že největší odpor má struktura (vč. kontaktů) v saturaci, kdy se v důsledku působení magnetického pole nachází v jednodoménovém stavu. Je-li velikost magnetického pole snižována, v určitém okamžiku dochází k téměř skokovému snížení odporu, který přísluší nukleaci magnetického víru. Křivka dále pokračuje do svého minima, které odpovídá poloze magnetického víru (resp. jádra) v oblasti mezi kontakty, a poté odpor narůstá až do další skokové změny, která značí anihilaci magnetického víru. Dalším zvyšováním magnetického pole se již odpor nezvyšuje, disk je opět v saturaci, tedy v jednodoménovém stavu.

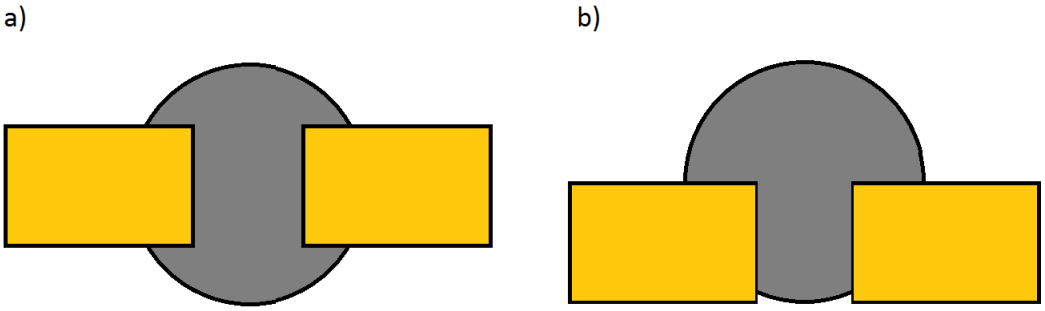
Pro určení cirkulace magnetického víru je podstatná oblast grafu poblíž nulové hodnoty externího magnetického pole, resp. směr křivky příslušející odporu v této oblasti. Je-li minima křivky dosaženo při snižování externího magnetického pole ještě před dosažením jeho nulové hodnoty, znamená to, že se magnetický vír pohybuje směrem pryč z oblasti mezi kontakty. Naopak, je-li minima křivky příslušející odporu dosaženo až po průchodu nulovou hodnotou vnějšího magnetického pole, magnetický vír se pohybuje směrem do oblasti mezi kontakty. Při znalosti směru magnetického pole, umístění kontaktů na disku a směru sklonu křivky poblíž nulové hodnoty magnetického pole je možné určit cirkulaci magnetického víru.

Tento způsob určování cirkulace magnetického víru pomocí sklonu křivky odporu disku v nulové hodnotě působícího externího magnetického pole je závislý na poloze kontaktů na disku. V případě symetrické polohy kontaktů, tedy jejich umístění přes střed disku, by sklon křivky odporu byl totožný pro obě možné cirkulace magnetického víru. Odlišný sklon pro obě cirkulace je možný jen pro asymetricky umístěné kontakty. Symetrická i asymetrická poloha kontaktů je naznačena na obrázku 4.2.

Pohyb vírů s opačnými cirkulacemi v disku vůči kontaktům ve stejném vnějším magnetickém poli je schematicky naznačen na obrázku 4.3. Uvažujme magnetické pole působící v rovině disku směrem doleva. V případě cirkulace magnetického víru proti směru hodinových ručiček v oblasti, kde je magnetické pole blízko nulové hodnoty, pohyb jádra, resp. víru směřuje mezi kontakty a odpor klesá. V případě opačné cirkulace, tedy po směru



Obrázek 4.1: a) Naměřené křivky odpovídající odporu feromagnetického disku o průměru 4 μm v magnetickém poli. Červená křivka přísluší zvyšování magnetického pole od záporných hodnot do kladných, modrá opačnému směru změny. V grafu je zřetelné, že k nukleaci dochází při stejném magnetickém poli (v absolutní hodnotě). Rozdílné jsou ale hodnoty odporu v okamžiku nukleace obou křivek, a rozdílné jsou i tvary křivek v oblasti grafu poblíž nulového magnetického pole. b) Schematické znázornění experimentálního zapojení a detail disku s kontakty pořízený elektronovým mikroskopem. V obrázku jsou naznačené směry působícího magnetického pole. Převzato z [35].



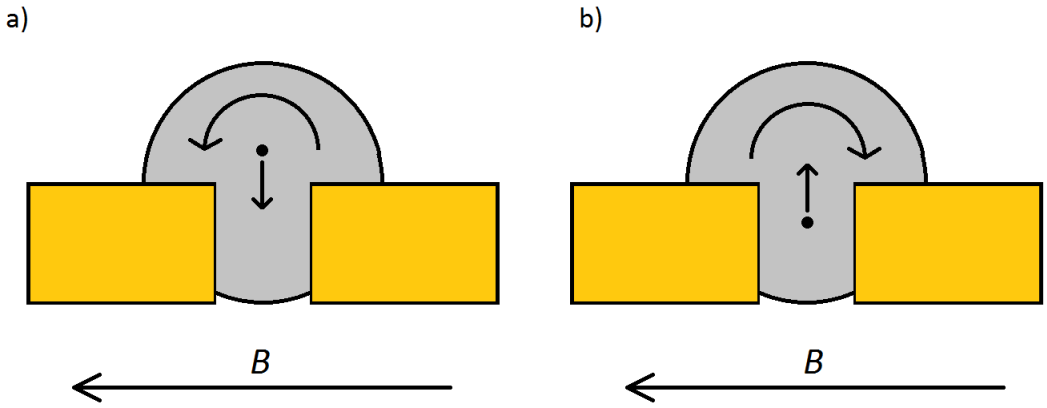
Obrázek 4.2: Disk se a) symetricky a b) asymetricky nanesenými kontakty.

hodinových ručiček, se vír pohybuje pryč od kontaktů a odpor ve stejném intervalu magnetického pole stoupá.

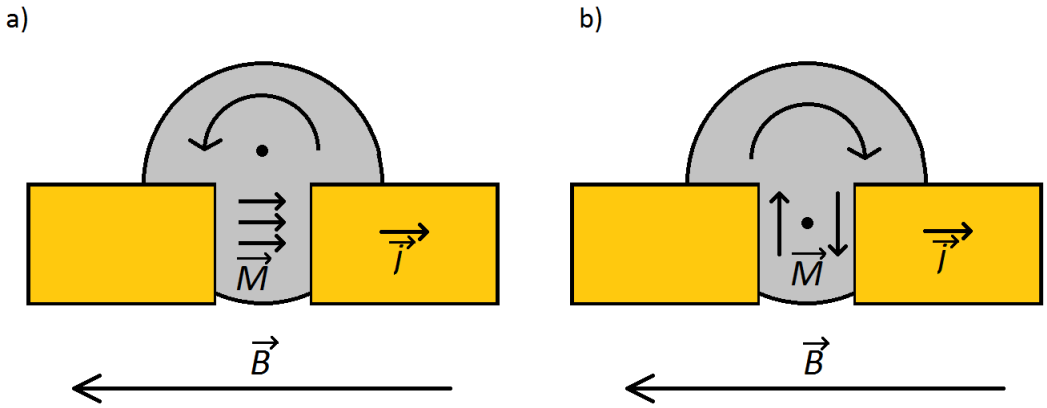
Důvodem těchto změn odporu je právě anizotropní magnetorezistivita ρ, jež závisí na úhlu φ, který svírá magnetizace $\vec{M}$ a proudová hustota $\vec{j}$, a lze ji vyjádřit jako

$$\rho(\varphi) = \rho_{\parallel} + (\rho_{\parallel} - \rho_{\perp}) \cos \varphi^2, \tag{4.1}$$

kde $\rho_{\parallel}$ je rezistivita při rovnoběžném směru magnetizace a proudové hustoty a $\rho_{\perp}$ rezistivita při kolmém směru magnetizace a proudové hustoty [19].



Obrázek 4.3: Pohybování magnetického víru v tělese disku při působení externího magnetického pole. a) V případě cirkulace proti směru hodinových ručiček a směru magnetického pole doleva dochází v uvedené konfiguraci k pohybu víru směrem do oblasti mezi kontakty. b) V případě stejného pole, ale opačného směru cirkulace, dochází k pohybu víru směrem pryč z oblasti mezi kontakty.



Obrázek 4.4: Schematické naznačení směrů magnetizace $\vec{M}$ a proudové hustoty $\vec{j}$ při poloze magnetického víru a) mimo oblast kontaktů a b) mezi kontakty.

Nejnižší hodnoty tedy AMR nabývá v případě, kdy jsou směry magnetizace $\vec{M}$ a proudové hustoty $\vec{j}$ na sebe kolmé, a nejvyšší hodnoty při směrech rovnoběžných. Schematické naznačení, jakým způsobem se takto projevuje magnetický vír v disku, je uvedeno na obrázku 4.4, na kterém je zobrazena totožná situace jako na obrázku předchozím, ovšem bezvýznačeného směru pohybu magnetického víru v disku. Nachází-li se vír mimo oblast kontaktů, proudová hustota leží ve směru rovnoběžném s magnetizací v disku, a naměřený odpor je vysoký. Nachází-li se magnetický vír mezi kontakty, magnetizace je vzhledem k proudové hustotě kolmá. Naměřený odpor je v tomto případě nejmenší.

Zjišťování směru cirkulace v navrženém konceptu generátoru náhodných čísel tedy spočívá v zaznamenávání sklonu křivky příslušné odporu poblíž nulové hodnoty externího magnetického pole. Vezme-li se v úvahu charakter cirkulace magnetizace magnetického víru, která může nabývat jen dvou hodnot, pro generování náhodných čísel lze tuto informaci jednoduše transformovat do podoby binárních čísel. Výhodou je, že není nutné stav této veličiny určovat, ale stačí první zaznamenané křivce odporu (v oblasti okolo nulové hodnoty externího magnetického pole) přiřadit jednu bitovou hodnotu (např. 0), a křivce odporu opačného směru opačnou hodnotu bitu (tedy 1). Výstupem takového generáto-

ru tedy je bitová posloupnost, resp. bitový soubor předem definované délky. Výhodou takového výstupu je, že je snadno zpracovatelný moderní výpočetní technikou.

4.1.3 Shrnutí konceptu

Koncept, který zde byl podrobněji popsán, lze jednoduše shrnout. Generátor je založen na cirkulaci magnetického víru v symetrickém plochém disku. Stav cirkulace je zjišťován pomocí anizotropní magnetorezistivity, a náhodné číslo je odvozováno od směrnice křivky odporu pro působící externí magnetické pole ve vhodně zvoleném intervalu. Zjištěná směrnice je převedena na číslo bitového charakteru tím způsobem, že záporná směrnice odpovídá hodnotě 0 a kladná směrnice odpovídá hodnotě 1. Po zjištění průběhu části křivky odpovídající odporu ve výše uvedeném intervalu pole je magnetické pole působící na disk nastaveno na hodnotu, při které je disk saturován a magnetický vír anihilovaný. Po snížení magnetického pole dochází k nukleaci nového magnetického víru a opět dochází k jeho proměření.

4.2 Procesy při výrobě generátoru

Výroba vzorku, na kterém se nachází navržený generátor náhodných čísel, sestává z několika kroků. Nejprve je nutné na vzorek nanést látku, která vhodným způsobem reaguje na ozáření elektronovým svazkem v kroku následujícím. Poté je nutné odstranit tu část materiálu, kterou má zaujímat výsledná struktura. Je-li toho dosaženo, je možné deponovat vrstvu kovu a následně provést tzv. lift-off proces, pomocí kterého na vzorku zůstane pouze původně plánovaná struktura generátoru, resp. struktura připravená v daném kroku výroby generátoru. Volitelným krokem je opracování disku pomocí fokusovaného iontového svazku, což je možné provést v rastrovacím elektronovém mikroskopu vybaveném iontovou optikou.

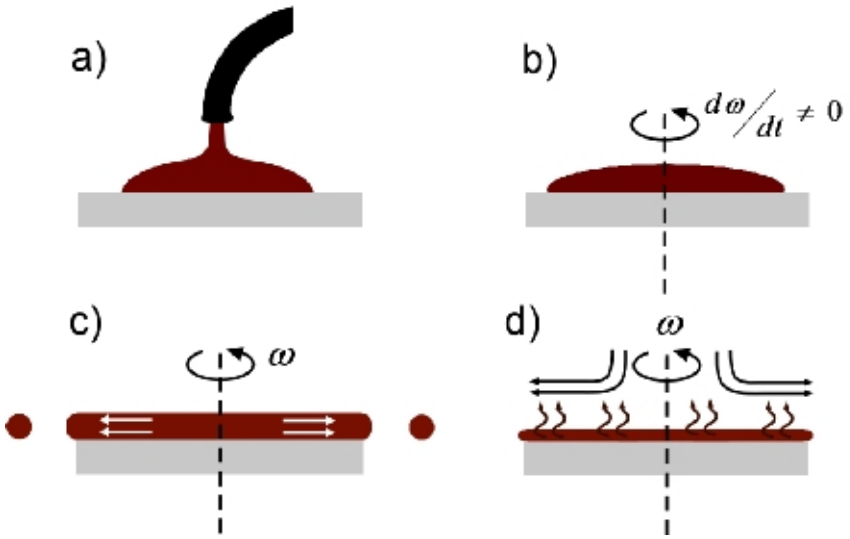
Jednotlivé kroky budou nyní podrobněji popsány. Je-li nutné vytvořit vzorek, kde se nacházejí struktury na jiných strukturách (např. pole disků na vlnovodu), je nutné pro každou strukturu provést všechny uvedené kroky zvlášť. Je-li tedy požadováno vyrobení struktury na již hotových strukturách, postup výroby začíná strukturou, která se nachází na substrátu, a následně se nanáší ta, která leží přímo na ní, dokud nejsou na vzorku připraveny všechny požadované struktury.

4.2.1 Elektronový rezist

Pojmem elektronový rezist je označována látka, obvykle makromolekulární struktury, která netermicky reaguje na elektronový svazek, pokud je jím ozařována. Dle reakce je možné rezisty dělit na pozitivní, kdy dochází k narušování chemických vazeb v řetězcích makromolekul a ve vývojce jsou následně odplaveny ozářené části, a na negativní, kde v ozařovaných částech rezistu dochází ke zpevnění vazeb a při vyvolávání dochází k odstranění neozářených oblastí rezistu.

Před nanesením rezistu na vzorek je nutné jej nejprve vypéct na ploténce, aby bylo dosaženo desorpce vody ze vzorku, v případě vzorků zde popisovaných jde o teplotu 180 °C. Na takto připravený vzorek je rezist nanesen metodou rotačního lakování (z angl. spin-coating). Metoda spočívá v nanesení rezistu v tekuté formě na vzorek. Následně

dochází k rotaci vzorku, přičemž v prvních několika sekundách pomocí úhlového zrychlení dochází k rozprostření rezistu po celé ploše vzorku. Po několika sekundách se velikost úhlové rychlosti, kterou se vzorek otáčí, ustaluje a množství rezistu na vzorku je snižováno především vlivem odstředivé síly, načež, při dostatečně tenké vrstvě rezistu, převládne snižování jeho množství vlivem odpařování [87]. Popsaný princip metody je schematicky naznačen na obrázku 4.5.



Obrázek 4.5: Princip nanesení rezistu pomocí rotačního lakování. a) Nanesení tekutého rezistu na vzorek. b) Rozprostření rezistu po povrchu vzorku v průběhu uvádění vzorku do rotačního pohybu. c) Snižování množství rezistu vlivem odstředivé síly d) a vlivem vypařování. Převzato z [87].

Rezist je na vzorek nanášen v tekuté formě, proto je nutné po jeho nanesení spin-coaterem provést jeho vypečení, při kterém dochází k odstranění použitého rozpouštědla. Vypékání po nanesení rezistu probíhalo po dobu 90 sekund také při teplotě ploténky 180 °C.

Výhodou nanášení tekutého rezistu je možnost ovlivňovat výslednou tloušťku vrstvy pomocí úhlové rychlosti a úhlového zrychlení spin-coateru.

Při výrobě vzorků popsaných v této práci byl jako elektronový rezist použit polymethylmethakrylát (dále jen PMMA) o relativní molekulové hmotnosti 495000, resp. 950000. Jako rozpouštědlo byl použit anisol, koncentrace roztoků se v závislosti na požadované struktuře na vzorku pohybovala v rozmezí 2-5,5 % PMMA v anisolu.

4.2.2 Elektronová litografie

Vykreslení struktur na nanesený rezist je provedeno metodou elektronové litografie (dále EBL, z angl. Electron Beam Litography). Tento typ litografie vyžaduje rastrovací elektronový mikroskop s příslušným programovým vybavením. V případě vzorků vytvořených v rámci této práce se pracovalo na elektronových mikroskopech TESCAN Lyra3 XM a Tescan Vega. Pro přípravu struktur bylo využito programu DrawBeam, který patří do programové sady těchto mikroskopů.

Ozařování rezistu v průběhu EBL probíhá bod po bodu, jde o tzv. přímý zápis. Rastrování umožňuje odklánění elektronového svazku mimo vzorek, čímž je dosaženo ozáření pouze těch oblastí vzorku, které požadujeme.

4.2.3 Vyvolání struktur

Je-li provedena litografie, je nutné ze vzorku odstranit tu část rezistu, která tvoří požadovanou strukturu. Toho je dosaženo ve vývojce, která odplaví ozářenou část rezistu v případě pozitivního rezistu, nebo neozářenou část v případě rezistu negativního.

Vývojkou byl v našem případě roztok methylisobutyl ketonu (dále MBIK) a isopropyl alkohoholu (dále IPA) v poměru 1:3, kterou bylo na vzorek působeno po dobu 90 sekund. Okamžitě poté dochází k opláchnutí vzorku čistým IPA, čímž je dosaženo odstranění zbytků roztoku MBIK+IPA a nedochází tak k dalšímu odstraňování rezistu z oblastí vzorku, kde je jeho přítomnost požadována.

4.2.4 Depozice tenké vrstvy

Na vzorek s vyvolanou strukturou je následně nanesena vrstva kovu pomocí metody depozice iontovým svazkem (dále jen IBS, z angl. Ion Beam Sputtering). Dopadajícím iontovým svazkem je odprašován terč vybraného materiálu a vhodnou polohou terče a vzorku je kov naprašován na vzorek.

K depozici bylo využito aparatury Kaufman [88] umístěné v Laboratoři odboru povrchů a pevných látek ÚFI FSI VUT v Brně. Tato aparatura kromě IBS umožňuje i metodu depozice s asistencí iontového svazku (dále IBAD, z angl Ion Beam Assisted Deposition).

V této aparatuře je vzájemné uspořádání zdroje iontů, terče s materiálem a vzorku takové, že povrch terče s odprašovaným materiálem a vzorek svírá úhel 22°. Z toho důvodu není tloušťka vrstvy naneseného kovu na připravovaném vzorku homogenní.

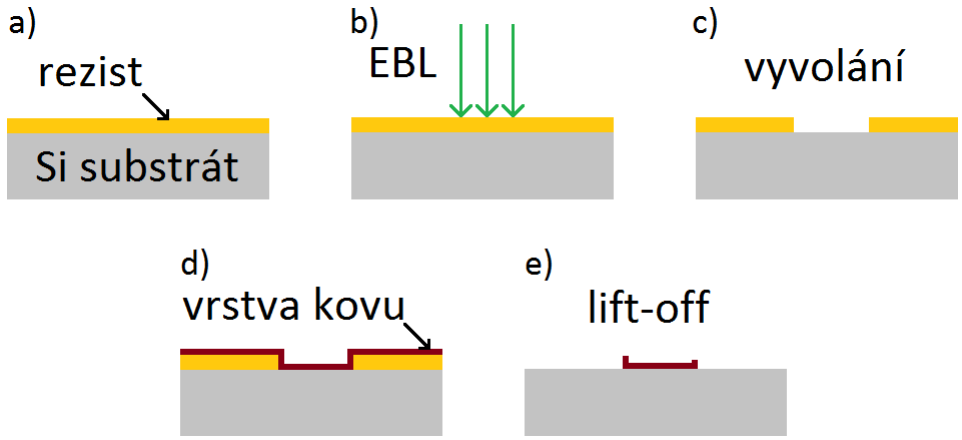
4.2.5 Lift-off proces

Nanesená vrstva kovu po depozici pokrývá celou plochu vzorku, je tedy nutné odstranit přebytečný kov, který nemá tvořit připravovanou strukturu. Tohoto je dosaženo provedením tzv. lift-off procesu.

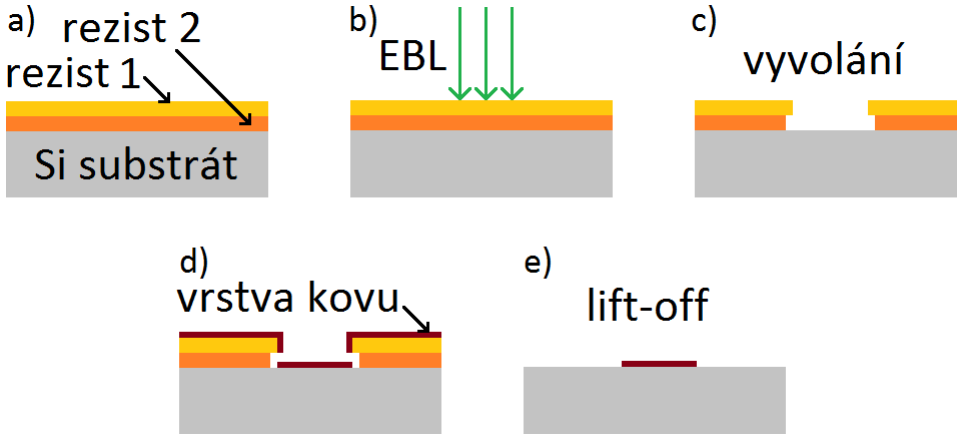
Jeho první krok spočívá v ponoření vzorku do acetonové lázně na dobu alespoň 24 hodin. Během této doby probíhá rozpouštění rezistu nacházejícího se mezi substrátem (popř. dříve nanesenou vrstvou kovu) a nově naprášeným kovem. Přebytečný kov je následně odstraněn pomocí ultrazvuku a na vzorku poté zůstává pouze kov na substrátu (resp. na již dříve nanesené vrstvě kovu), tedy požadovaná struktura.

Při depozici je kov nanášen i na stěny připravené struktury v rezistu. Z toho důvodu mohou být po lift-off procesu na výsledné struktuře i tzv. reziduální otřepy. Princip jejich vzniku při použití pozitivního rezistu je schematicky naznačen na obrázku 4.6.

Řešením může být například použití dvou vrstev rezistů o různých vlastnostech. Nejprve je na vzorek nanesena vrstva rezistu o vyšší citlivosti (např. PMMA 495k) a na ni je poté nanesena vrstva o citlivosti nižší (např. PMMA 950k). V průběhu litografického opracování reaguje vrchní vrstva rezistu s elektronovým svazkem méně než vrstva spodní. Pokud je spodní vrstva o dostatečné tloušťce, je možné tvorbu otřepů omezit, případně ji zcela zabránit. Schematicky je reakce dvou vrstev rezistu s elektronovým svazkem při elektronové litografii uvedena na obrázku 4.7.



Obrázek 4.6: Schematické naznačení vzniku reziduálních otřepů na hranách deponovaných struktur. a) Křemíkový substrát s naneseným pozitivním rezistem. b) Expozice rezistu v průběhu elektronové litografie. c) Vyvolání exponovaného rezistu. d) Depozice tenké vrstvy zvoleného materiálu. e) Výsledná struktura po provedení lift-off procesu.



Obrázek 4.7: Schematické znázornění reakce dvou vrstev rezistu s elektronovým svazkem v průběhu litografie a výsledná struktura bez reziduálních otřepů. a) Křemíkový substrát se dvěma nanesenými vrstvami pozitivního rezistu. Na substrátu se nachází vrstva s vyšší citlivostí vůči elektronovému svazku, na ní je vrstva s citlivostí nižší. b) Expozice rezistu při litografii. V případě vrstvy rezistu o vyšší citlivosti dochází k expozici větší plochy rezistu. c) Vyvolání exponovaného rezistu. Protože elektrony narušovaly molekulární řetězce v rezistu o vyšší citlivosti více, dochází po vyvolání k určitému překryvu horní vrstvy rezistu. d) Depozice tenké vrstvy zvoleného materiálu. e) Výsledná struktura po provedení lift-off procesu bez nežádoucích reziduálních otřepů.

4.2.6 Fokusovaný iontový svazek

Rastrovací elektronový mikroskop, který je vybaven příslušnou iontovou optikou, umožňuje využít iontů jak pro zobrazení vzorku, tak pro jeho opracování (iontové odprašování či leptání). V případě této práce bylo použito elektronového mikroskopu Tescan LYRA3 XM, který pro fokusovaný iontový svazek (dále FIB, z angl. Focused Ion Beam) využívá iontů galia.

Při této metodě jsou ionty urychleny pomocí vysokého napětí, které bývá obdobné jako v případě elektronů v elektronovém svazku elektronového mikroskopu. Vzhledem k rozdílu

hmotností elektronu a iontu ale při dopadu na vzorek dochází nejen k vyrážení případných elektronů, ale rovnou atomů, molekul či jejich skupin. Tato metoda je tedy vůči vzorku destruktivní, což je vhodné mít na vědomí při jejím použití.

5 Experimentální příprava generátoru

Na základě konceptu generátoru představeném v minulé kapitole byla experimentálně provedena optimalizace jednotlivých prvků a parametrů použité měřicí metody.

Příprava vzorku generátoru probíhá ve dvou krocích. Prvním krokem je nanesení disku na křemíkový substrát, které probíhá pomocí elektronové litografie a depozicí tenké vrstvy. Část vzorků byla pro další krok použita ihned po provedení lift-off procesu, druhá část vzorků prošla opracováním disku pomocí metody fokusovaného iontového svazku.

Druhým krokem bylo nakontaktování disků vodičem, resp. vlnovodem. Tento krok byl také proveden pomocí metod EBL a IBS. Po tomto kroku byl vzorek generátoru náhodných čísel připraven pro měření.

V této kapitole bude nejprve blíže přiblížena použitá měřicí metoda, poté budou popsány parametry vodivých kontaktů. Následně bude pozornost věnována parametrům disků, jednotlivým krokům při jejich optimalizaci a experimentálně zjištěné vlastnosti při použití vybraných parametrů disku. Závěrem kapitoly budou výsledky měření diskutovány.

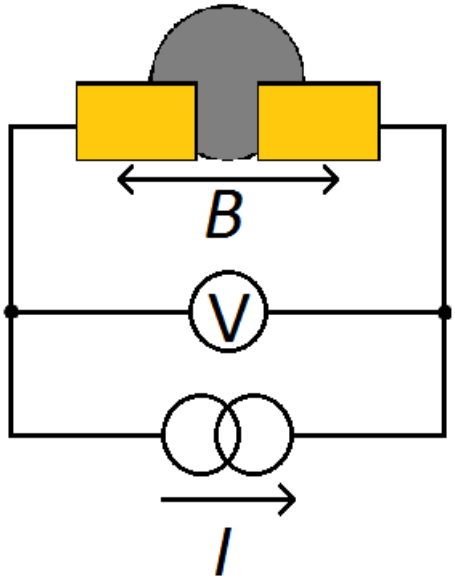
5.1 Anizotropní magnetorezistivita

Metodou, která byla zvolena pro zjišťování cirkulace magnetického víru, je anizotropní magnetorezistivita. Přestože je princip metody poměrně jednoduchý, pro její realizaci je nutné používat velmi přesné přístroje, neboť změna odporu mezi jednodoménovým stavem v saturaci a ve stavu magnetického víru činí jednotky až desítky milivoltů.

Experimentální uspořádání je schematicky naznačeno na obrázku 5.1. Zdroj stejnosměrného proudu do obvodu dodává elektrický proud o takové velikosti, aby úbytek napětí na vzorku (tedy na disku s kontakty) nepřesáhl 10 mV, velikost tohoto proudu je vždy nižší než 0,4 mA. Takto zvolená hodnota proudu je dostatečná k rozeznatelné změně odporu při měření AMR, a zároveň dostatečně malá, aby nedošlo k poškození měřeného vzorku. Magnetické pole, ve kterém se vzorek nachází, je indukováno pomocí cívky s pólovými nástavci. Mezi nimi byl vzorek umístěn, přičemž velikost pólových nástavců je dostatečně velká na to, aby magnetické pole obklopující vzorek bylo možné považovat za homogenní. Magnetické pole této cívky si zachovává lineární charakter v intervalu od -70 mT do 70 mT. Maximální velikost pole, kterému byl v průběhu měření vzorek vystaven, závisela na parametrech měřeného vzorku, a vždy byla takové velikosti, aby magnetizace disku přešla do jednodoménového stavu. Změna velikosti magnetického pole probíhá kvazistaticky, k nárůstu či poklesu, jehož velikost závisí na měřeném vzorku, dochází každých 300 ms.

Ovládání všech prvků měřicí soustavy probíhá pomocí počítače, resp. pomocí programu v programovém rozhraní Labview. S jeho pomocí je možné jednoduše nastavovat či měnit parametry i v průběhu probíhajícího měření. Ve stejném programovém rozhraní je možné pro vybrané vzorky zjišťovat zároveň sklon křivky odporu disku poblíž nulového magnetického pole.

Měření samotné sestává ze dvou kroků. Nejprve je proměřena závislost odporu na magnetickém poli. Závislost je měřena dvakrát, a to pro oba směry magnetického pole, a to od saturovaného do saturovaného stavu. Na základě několika těchto měření je možné



Obrázek 5.1: Schéma experimentálního uspořádání při měření anizotropní magnetorezistivity.

odhadnout vhodnost měřeného vzorku pro další měření, resp. pro generování náhodných čísel. Jako nevhodné vzorky jsou považovány ty, jejichž stav magnetizace nepřechází do stavu magnetického víru, ale do nějakého složitějšího multidoménového stavu, či vzorky, ve kterých nukleuje magnetický vír vždy se stejnou cirkulací. Vhodnost či nevhodnost testovaného vzorku pro další měření byla ověřována i pomocí rastrovacího elektronového mikroskopu, pomocí kterého lze odhalit např. asymetrii disku, defekt či výraznou nečistotu, která by mohla být příčinou nukleace magnetického víru se stále stejnou cirkulací.

Pokud lze vzorek na základě vizuální kontroly v rastrovacím elektronovém mikroskopu a několika měření závislosti odporu na magnetickém poli považovat za vhodný, je u něj zjišťován sklon křivky odporu v oblasti v okolí nulové hodnoty magnetického pole. Interval, ve kterém je směrnice křivky vyhodnocována, závisí na parametrech disku. Například pro disky o průměru $d = 1,5$ μm a $d = 1$ μm je určována v intervalu od -3 mT do 3 mT, odůvodnění krajních hodnot intervalu lze nalézt v následujícím textu. Poté dochází k saturaci disku, tedy anihilaci již změřeného magnetického víru, dostatečně velkým magnetickým polem, které je možné určit na základě předchozího měření celé závislosti odporu na magnetickém poli. Pole je následně sníženo tak, aby mohlo dojít k nukleaci nového magnetického víru, a cyklus proměřování sklonu poblíž nulové hodnoty, anihilace víru a nukleace víru je znovu opakován.

5.2 Kontakty disku

Kontakty jsou nezbytným prvkem pro detekci cirkulace magnetického víru metodou AMR. Aby byla zaručena jejich dobrá vodivost, byly na vzorcích připravovány ze zlata. Tloušťka nanesené vrstvy zlata je odvozena od velikosti vrstvy feromagnetického disku. V případě tloušťky kovové vrstvy disku o velikosti 50 nm a méně je tloušťka zlatého kontaktu volena 100 nm, v případě tloušťky disku 50 nm až 100 nm je tloušťka zlaté vrstvy 150 nm, přičemž stejná tloušťka, tedy 150 nm, je použita i v případě disků menší tloušťky, které

ale byly opracovány metodou fokusovaného iontového svazku. Pro obě možné tloušťky zlaté vrstvy je pod vrstvou zlata nanesena titanová adhezní mezivrstva o tloušťce 3 nm.

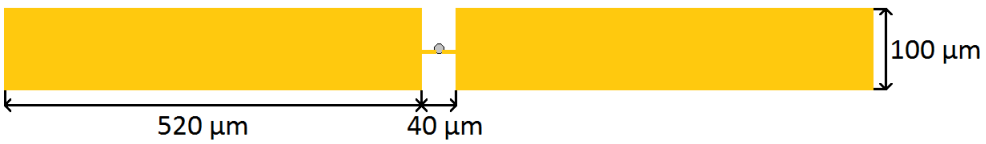
Vodivé kontakty sestávají ze dvou částí. První část je asymetricky nanesena na disku. Její důležité rozměry, tedy především šířka obou částí těchto kontaktů a mezera mezi nimi, závisí na průměru disku.

Tabulka 5.1 uvádí šířku kontaktů asymetricky nanesených na discích různých průměrů a také jejich vzájemnou vzdálenost, tedy velikost mezikontaktové mezery. Ne ve všech případech se podařilo dosáhnout přesně těchto parametrů kontaktů, je nutné je považovat jako orientační, parametry kontaktů na vyrobených vzorcích často záležely především na odchylkách či nepřesnostech při provádění elektronové litografie.

d [μm]	Šířka [[μm]]	Mezera [μm]
4,0	2,50	2,20
3,0	2,50	1,50
2,0	2,00	0,85
1,5	1,50	0,65
1,0	1,25	0,55

Tabulka 5.1: Rozměry zlatých kontaktů nanesených přímo na disky o průměru d.

Rozměry druhé části kontaktů jsou s porovnáním s předchozí větší. Šířka je pro obě jejich symetrické části 100 μm a délka 520 μm. Na obrázku 5.2 jsou zobrazeny kompletní kontakty s vyznačenými rozměry.



Obrázek 5.2: Schematické znázornění obou částí kontaktů s vyznačenými rozměry.

Po nanesení kontaktů je vzorek upevněn do keramického pouzdra, čímž je ukončen proces jeho přípravy, a je připraven pro měření.

5.3 Optimalizace parametrů disků

Fundamentálním prvkem navrženého generátoru náhodných čísel je feromagnetický disk. Tento disk by měl pro dosažení náhodné nukleace cirkulace magnetizace být symetrický, bez defektů a nečistot. Roli hrají i použitý materiál a rozměry disku, tedy jeho výška t a průměr d.

Materiál, ze kterého byly disky připraveny, je slitina niklu a železa v poměru 80:20 nazývaná permalloy (značená $Ni_{80}Fe_{20}$, případně Py).

Pro měření byly připraveny vzorky s disky o průměru $d = 4$ μm, $d = 3$ μm, $d = 2$ μm, $d = 1,5$ μm a $d = 1$ μm.

Výška disků byla testována v rozmezí od 20 do 100 nm, konkrétní použité hodnoty jsou $t = 20$ nm, $t = 30$ nm, $t = 40$ nm, $t = 50$ nm, $t = 75$ nm a $t = 100$ nm.

Snaha o nalezení disku s nejlepšími vlastnostmi pro využití pro generátor náhodných čísel spočívá v nalezení vhodné kombinace průměru a výšky disku. Oba tyto parametry byly voleny na základě studia podobné problematiky, konzultací s osobami zabývajícími se podobnou problematikou i dle výsledků měření vzorků s připravenými disky o různých

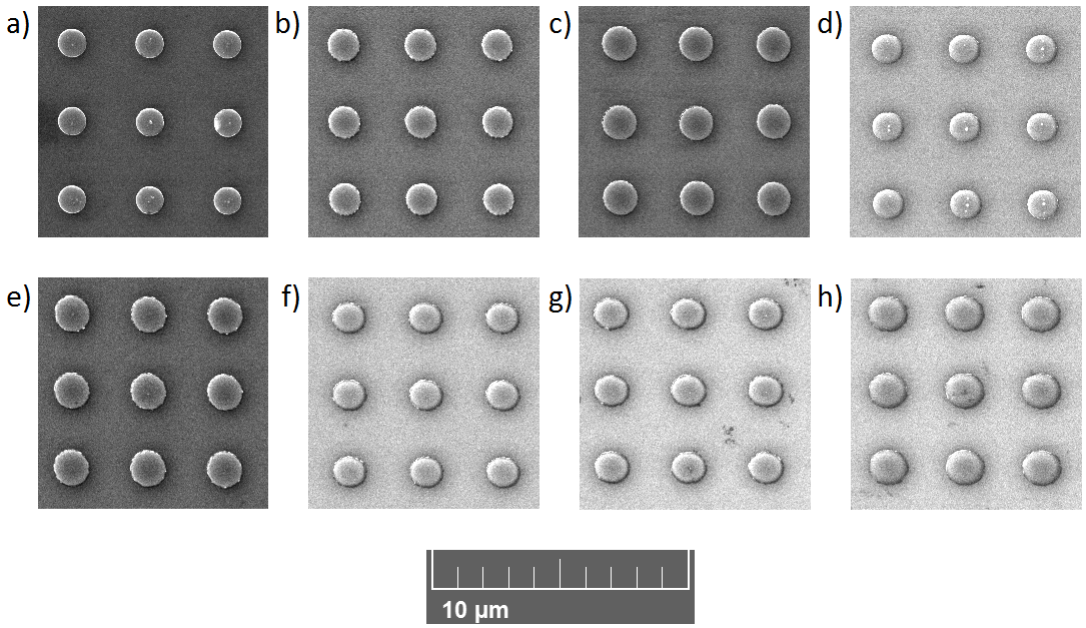
rozměrech. Podstatnou podmínkou, kterou bylo nutné splnit, byla existence (resp. vznik) magnetického víru v právě testované struktuře.

5.3.1 Stanovení dávky náboje při EBL

Před započetím přípravy vzorků samotného generátoru bylo nutné zvolit správnou velikost dávky náboje pro EBL. Pokud by byla zvolena dávka příliš malá, ozářený elektronový rezist nebude narušen dostatečně, takže při jeho vyvolávání bude odstraněn jen z části či vůbec. V opačném případě, tedy pokud by byla dávka přílš velká, by nebyly molekulové řetězce elektronového rezistu narušeny pouze v oblasti nakreslené struktury, ale i okolo ní, což může být problém především pro struktury malých rozměrů.

Vzhledem k tomu, že pro litografii byly používány dva elektronové mikroskopy, bylo nutné provést testování dávky pro oba použité mikroskopy.

Na obrázku 5.3 jsou zobrazeny části polí disků, které byly připravené elektronovým mikroskopem Tescan Vega. Dávky náboje, které byly použity při litografii jednotlivých polí, ležely v rozmezí 280 až 500 μC/cm^2, velikost dávky se postupně navyšovala.



Obrázek 5.3: Disky připravené elektronovou litografií na elektronovém mikroskopu VEGA při použití rozdílných dávek náboje. Velikosti dávek jsou a) 280 μC/cm^2, b) 320 μC/cm^2, c) 340 μC/cm^2, d) 350 μC/cm^2, e) 360 μC/cm^2,f)400 μC/cm^2, g) 450 μC/cm^2 a h) 500 μC/cm^2.

V případě elektronového mikroskopu Tescan Lyra3 XM byla velikost dávky náboje stanovena obdobným způsobem.

Vezme-li se v úvahu, že pro generaci náhodných čísel je nutné používat disky, které jsou ideálně naprosto symetrické, jako výsledná velikost dávky byla vybrána taková dávka, při jejímž použití dochází k lehkému přeexponování elektronového rezistu. Pokud by byla použita jiná struktura, např. čtverec, došlo by k jeho zakulacení. V případě disku ale tento problém nehrozí a lze tak předejít vzniku asymetrií disku kvůli nedostatečné expozici rezistu.

Dávky náboje, které byly při následující přípravě vzorků při elektronové litografii používány, byly stanoveny jako 350 μC/cm^2 pro elektronový mikroskop Vega, pro elektronový mikroskop Lyra 400 μC/cm^2 pro struktury malých rozměrů (disky, vnitřní části kontaktů) a 530 μC/cm^2 pro struktury větších rozměrů (vnější části kontaktů).

5.3.2 Dvouvrstvý rezist

Z několika snímků uvedených v předchozí podkapitole je patrné, že na některých strukturách zůstávaly tzv. reziduální otřepy. V případě větších struktur, tedy vnějších kontaktů, není problém až tak závažný, a proto se i nadále využíval jednovrstvý rezist A5,5 s relativní molekulovou hmotností 495k.

Jiný přístup ale vyžadují struktury malé, v tomto případě disky. Aby nemohlo docházet k nekontrolovatelnému ovlivňování chování veličin magnetického víru při jeho nukleaci či anihilaci, požadujeme, aby se otřepy na discích nenacházely. Proto při jejich přípravě byly pro expozici vzorku při EBL naneseny dvě vrstvy rezistů o rozdílné koncentraci pevných látek v rozpouštědle. Zkoušeny byly kombinace rezistů A2 495k+A2 950k, A2 495k+A4 950k, A4 495k+A4 950k a A5 495k+A2 950k.

Ani jedna z kombinací rezistů nedokázala úplně zamezit vzniku otřepů. Důvodem může být použití roztoků rezistů se stejným rozpouštědlem (anisol). Při nanesení svrchní vrstvy ještě tekutého rezistu zřejmě došlo k částečnému rozpuštění vrstvy již naneseného rezistu a promísení obou rozdílných rezistů. Po vytvrzení vrchní vrstvy rezistu se na vzorku proto nenachází dvě ostře oddělené vrstvy, ale místo zřetelné hranice existuje přechodová oblast. Protože nedošlo k výraznějšímu zlepšení vzhledu disků, bylo od používání dvou vrstev rezistu při přípravě vzorku upuštěno a i pro malé struktury byl používán také jednovrstvý rezist A5,5 495k.

5.3.3 Kontrola přítomnosti vírů pomocí MFM

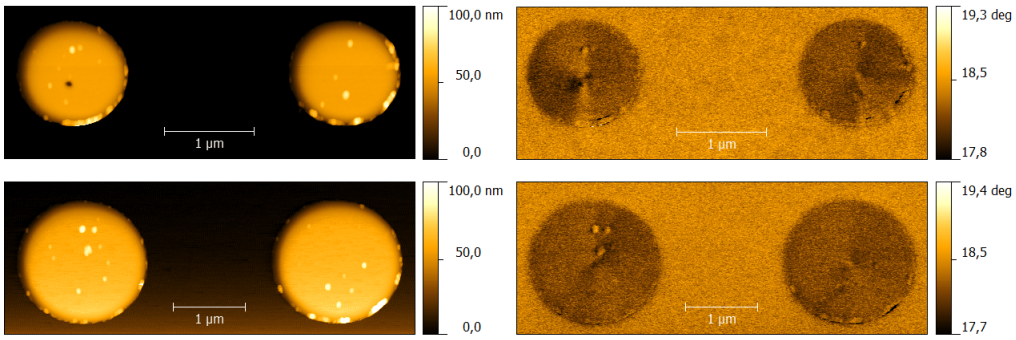
Pro vybrané rozměry disků bylo vhodné ověřit, zda-li jejich parametry umožňují nukleaci magnetických vírů. Pro tento úkol byla zvolena mikroskopie magnetických sil, jejíž princip je již popsán v kapitole 2.4.1.

Na obrázku 5.4 jsou zobrazeny dvojice disků o průměru $d = 1$ μm (nahoře) a průměru $d = 1,5$ μm (dole). V levé části obrázku se nachází topografie získaná pomocí AFM, v pravé části je zobrazena fáze magnetického pole, tedy změny v magnetizaci, která byla změřena pomocí MFM.

Na základě porovnání topografie a fáze magnetických sil je zřejmé, že signál v předpokládané oblasti výskytu magnetických vírů, což jsou v tomto případě středy disků, nevznikl například na nečistotě či defektu disku. Jednoznačně tedy jde o jádra magnetických vírů. Na základě těchto měření je tedy možné konstatovat, že v připravených discích magnetické víry nukleují.

5.4 Měření AMR

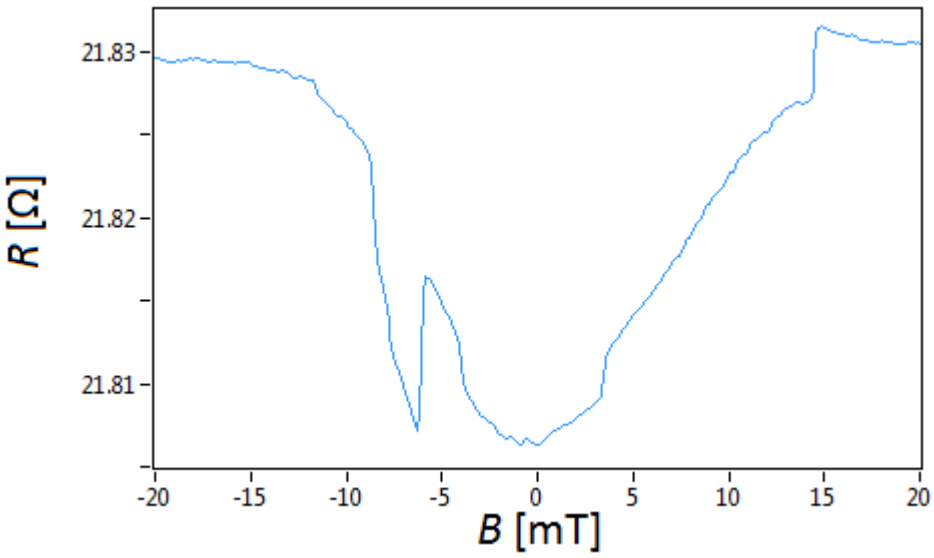
V této kapitole jsou uvedeny zjištěné poznatky pro vzorky s disky různých parametrů a jednotlivé vzorky budou podrobněji popsány. Vzhledem k množství připravených vzorků jsou vždy vybrány reprezentativní vzorky, jež popisují typické chování skupiny vzorků se stejnými parametry, a též vzorky, které se od typického chování značně liší.



Obrázek 5.4: Disky o průměru $d = 1,5$ μm (nahoře) a $d = 1,5$ μm (dole). Vlevo je zachycena topografie disků, vpravo signál fáze mikroskopie magnetických sil. Pro obě dvojice disků o uvedených průměrech jsou v obou discích rozeznatelná jádra magnetických disků, která v každé dvojici mají navzájem opačnou polaritu.

5.4.1 Disk o průměru 4 μm

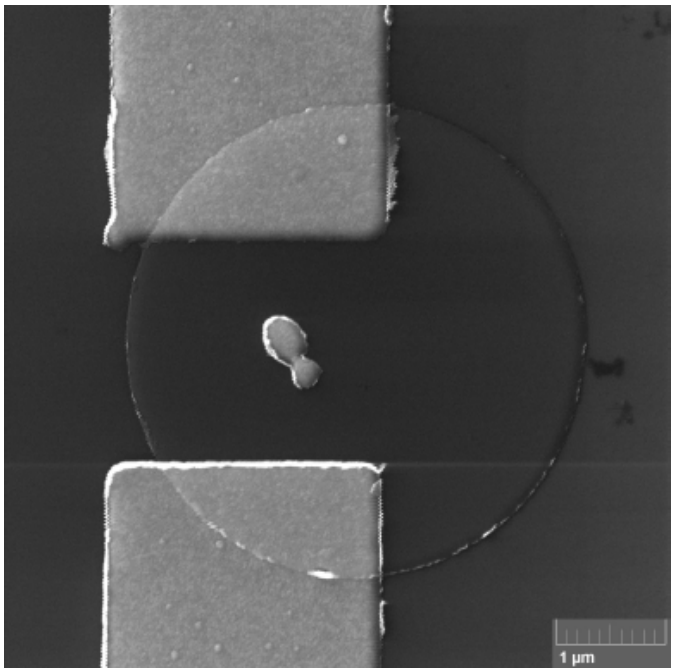
První připravené vzorky nesly disk o průměru $d = 4$ μm, a všechny byly kontaktovány po provedení lift-off procesu bez dalšího opracování disku. Na obrázku 5.5 je zachycena závislost odporu na magnetickém poli jednoho vzorku o výšce $t = 50$ nm. Na základě tvaru grafu lze říci, že magnetizace disku není ve stavu magnetického víru, ale v nějakém multidoménovém stavu. Toto je vyvozeno podle několika skokových změn odporu, které přísluší přechodům mezi stavy magnetizace. Tento disk tedy není vhodný pro generování náhodných čísel. Křivka v grafu zaznamenává hodnotu odporu v celém rozsahu použitého magnetického pole (zde od $B = -20$ mT do $B = 20$ mT).



Obrázek 5.5: Závislost odporu disku o průměru $d = 4$ μm a výšce $t = 50$ nm na působícím magnetickém poli. Skoková změna hodnoty odporu při magnetickém poli o velikosti přibližně $B = 3,5$ mT značí změnu stavu magnetizace, která v případě magnetizace ve stavu magnetického víru nenastává. V tomto případě je tedy magnetizace disku v multidoménovém stavu.

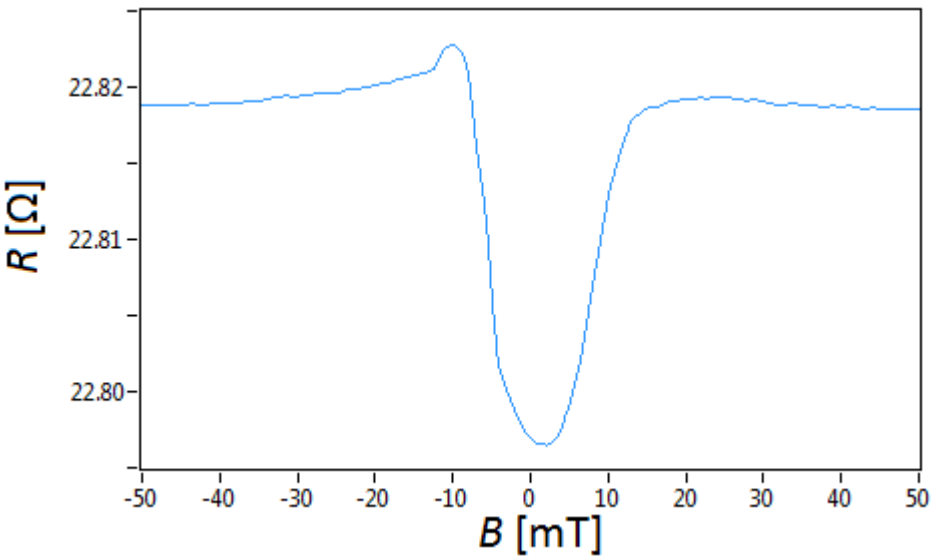
Detail disku s kontakty pořízený pomocí elektronového mikroskopu je uveden na obrázku 5.6. Na disku je patrná nečistota, která na vzorku zřejmě vznikla v průběhu výroby zlatých

kontaktů a která nebyla v průběhu lift-off procesu odstraněna. Vzhledem k tomu, že zlato je nemagnetický materiál, by tato nečistota neměla zásadním způsobem ovlivňovat stav magnetizace disku.



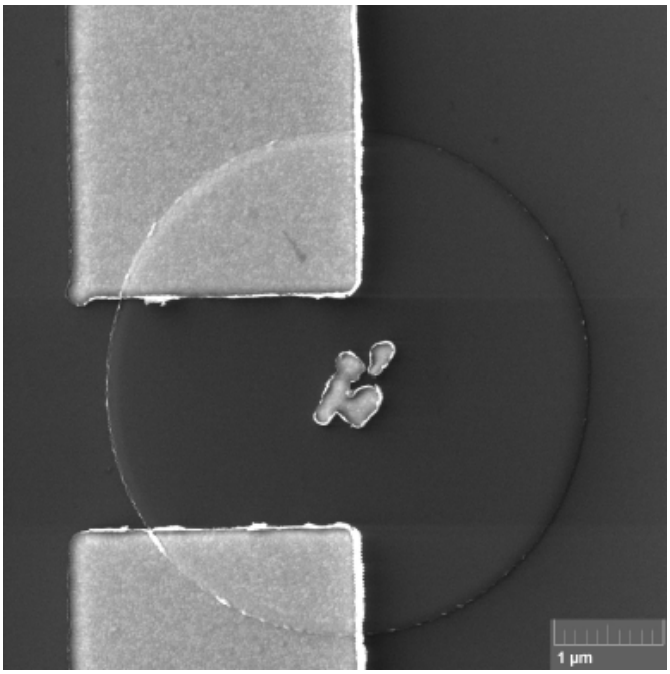
Obrázek 5.6: Detail disku o průměru $d = 4$ μm a výšce $t = 50$ nm s vodivými kontakty pořízený pomocí elektronového mikroskopu.

Další vzorek, jehož parametry jsou shodné s diskem předchozím ($d = 4$ μm, $t = 50$ nm), při měření AMR vykazoval chování typické pro magnetizaci ve stavu magnetického víru. Průběh závislosti odporu na magnetickém poli je zachycen na obrázku 5.7. Z obrázku je patrné, že minimální hodnoty odporu křivka dosahuje při přibližně $B = 2$ mT. Opakovaná měření odhalila, že v tomto disku vzniká magnetický vír stále se stejnou cirkulací.



Obrázek 5.7: Závislost odporu disku o průměru $d = 4$ μm a výšce $t = 50$ nm na působícím magnetickém poli.

Detail disku s kontakty pořízený pomocí elektronového mikroskopu je uveden na obrázku 5.8. I v tomto případě na disku zůstala rezidua zlata. Při porovnání se vzhledem předchozího vzorku, který byl zobrazen na obrázku 5.6, není patrná žádná zásadní odchylka, ale i přesto v jednom z disků magnetický vír vzniká a v druhém nikoli.



Obrázek 5.8: Detail disku o průměru $d = 4$ μm a výšce $t = 50$ nm s vodivými kontakty pořízený pomocí elektronového mikroskopu.

5.4.2 Disky o průměru 3 μm a 2 μm

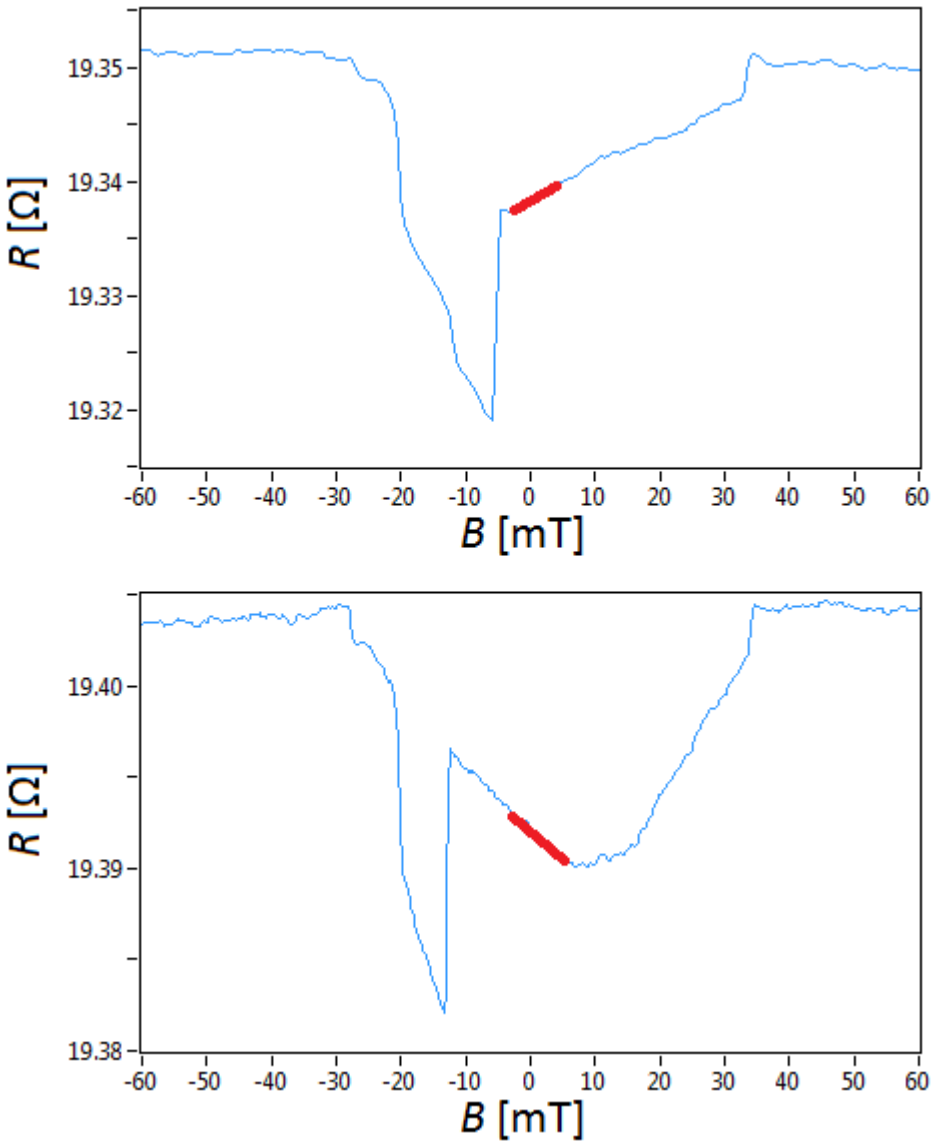
Následovala příprava vzorků s disky o průměru $d = 3$ μm a $d = 2$ μm. Výsledky měření byly podobné jako pro disky o průměru $d = 4$ μm, tedy magnetizace byla buď v multidoménovém stavu či případně ve stavu magnetického víru. V případě vzorků s magnetizací disku ve stavu magnetického víru cirkulace po nukleaci zachovávala svůj směr, tedy nedocházelo ke vzniku magnetického víru s náhodným směrem cirkulace. Z tohoto důvodu byla příprava disků o těchto průměrech opuštěna a bylo přikročeno k výrobě disků o menším průměru.

5.4.3 Disk o průměru 1,5 μm

U vzorků s diskem o průměru $d = 1,5$ μm byla úspěšně pozorována nukleace magnetického víru s oběma směry cirkulace. Stalo se tak jak pro vzorky, které byly nakontaktovány bez dalšího opracování, tak pro disky, které byly připraveny s průměrem $d = 2$ μm, ale jejich hrana byla fokusovaným iontovým svazkem odprášena a průměr disku byl snížen na $d = 1,5$ μm. Výhodou tohoto postupu je, že jsou odstraněny případné reziduální otřepy na původní hraně struktury.

Na obrázku 5.9 jsou uvedeny změřené křivky příslušející odporu v závislosti na magnetickém poli pro magnetické víry s oběma možnými směry cirkulace. Za povšimnutí stojí i rozdílná hodnota magnetického pole, ve které dochází k nukleaci magnetického víru.

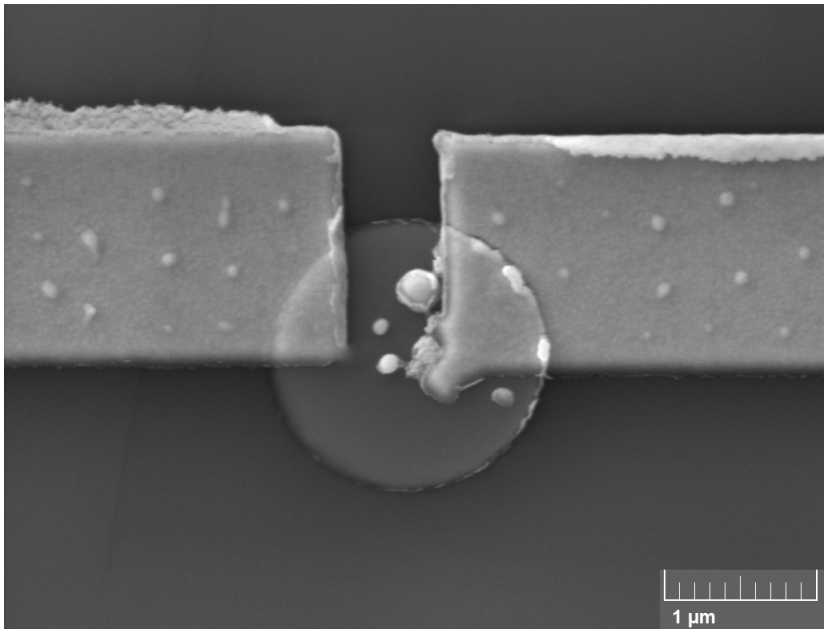
V grafu je červeně vyznačena směrnice křivky odporu v okolí nulové hodnoty magnetického pole.



Obrázek 5.9: Naměřené závislosti odporu disku o průměru $d = 1,5$ μm a výšce $t = 75$ nm v závislosti na působícím magnetickém poli pro obě možné cirkulace magnetického víru. Červeně je v grafu vyznačena směrnice křivky odporu v okolí nulové hodnoty magnetického pole.

Vzhled disku na tomto vzorku je zobrazen na obrázku 5.10, který byl pořízený pomocí elektronového mikroskopu. I v tomto případě se na disku objevují zlaté nečistoty, a navíc při přípravě došlo k defektu kontaktu. I přes tyto nedostatky měření tohoto disku poskytovalo věrohodná data.
I v případě druhého typu vzorků, tedy vzorků s disky zmenšenými pomocí metody FIB z původního průměru $d = 2$ μm na průměr $d = 1,5$ μm, byly úspěšně připraveny vzorky s magnetickými víry nukleujícími s oběma směry cirkulace.

Měření závislosti odporu na magnetickém poli jednoho z takto připravených vzorků s diskem o tloušťce 50 nm je zachyceno na obrázku 5.11. Z grafů je patrné, že nukleace



Obrázek 5.10: Detail disku o průměru $d = 1,5$ μm a výšce $t = 75$ nm s vodivými kontakty pořízený pomocí elektronového mikroskopu.

magnetických vírů s opačnými cirkulacemi vzniká při rozdílném magnetickém poli, posun z nulové činí asi $B = 4$ mT. V obou případech je sklon křivky odporu poblíž nulové hodnoty magnetického pole jednoznačný a snadno od sebe lze rozlišit magnetické víry s opačnými cirkulacemi. Směrnice změny odporu v okolí nulové hodnoty magnetického pole je v uvedeném grafu znázorněna červeně.

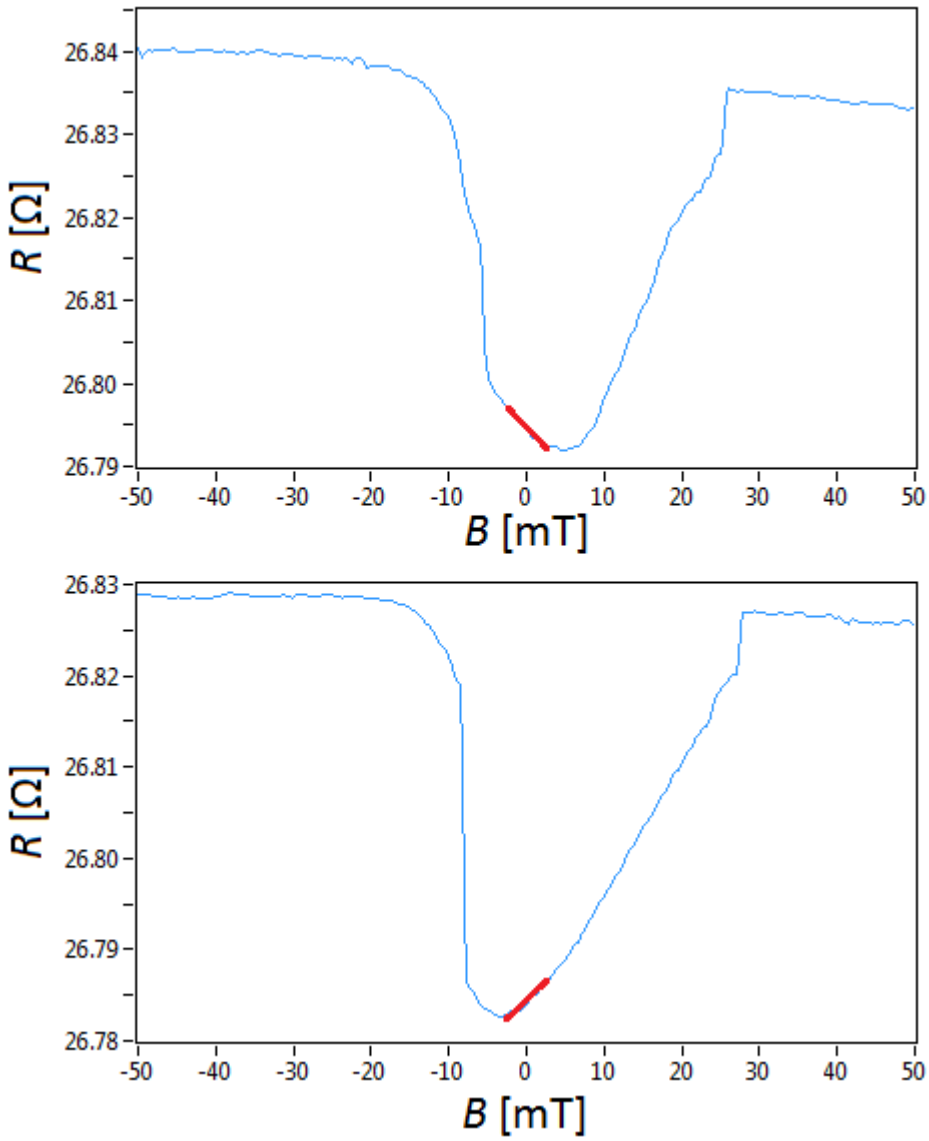
Detail tohoto disku je zachycen na obrázku 5.12. Na obrázku je patrné, že hrany disku jsou bez nežádoucích otřepů. Na druhou stranu, hrana není přesně kruhová, což je cílem použití metody FIB, nýbrž zvlněná, což je pravděpodobně způsobeno přítomností zrn materiálu, které měly díky své různé krystalografické orientaci různou odprašovací rychlost. Tento jev lze v různé míře pozorovat u všech disků opracovaných metodou FIB bez ohledu na intenzitu odprašování.

Za zmínku stojí i absence zlatých nečistot, které byly pozorovány na předchozích vzorcích. Tohoto zlepšení bylo dosaženo posunutím disku a kontaktů mimo střed zapisovacího pole pro EBL ovládacího programového rozhraní elektronového mikroskopu. Zřejmě dochází k nějakému nežádoucímu osvitu právě středové polohy tohoto pole, což může být příčinou vzniku nečistot.

5.4.4 Disk o průměru 1 μm

Další snížení průměru disku, a to na velikost $d = 1$ μm, při přípravě vzorků s magnetickými víry vznikajícími s cirkulacemi s oběma možnými směry nepřineslo žádné zlepšení. Naopak, u vzorků s disky o průměru $d = 1$ μm, a to jak u těch připravených pomocí metody lift-off, tak i u těch zmenšených na tento průměr pomocí metody FIB, nebyly zároveň naměřeny dostatečně průkazné cirkulace magnetického víru obou směrů. Byl-li signál z těchto vzorků smysluplný, tedy pokud došlo k nukleaci magnetického víru, jeho cirkulace při každé nukleaci nastávala se stejným směrem.

Příčina, proč nedošlo k úspěšné přípravě vzorku vhodného pro generování náhodných čísel s diskem o průměru $d = 1$ μm, je (pokud se neberou v úvahu případné defekty disku)

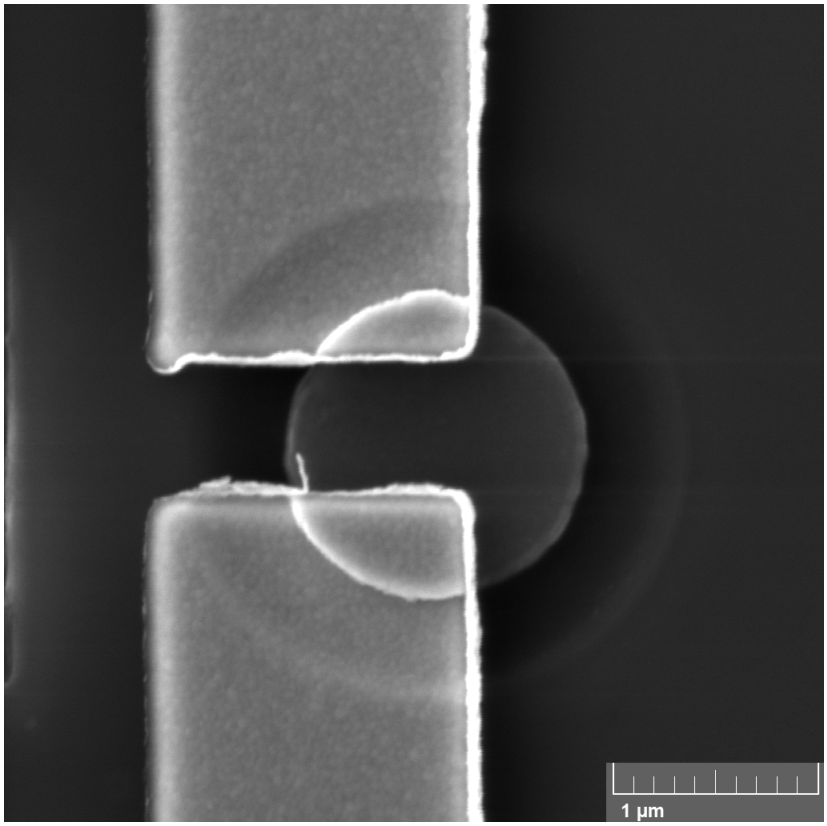


Obrázek 5.11: Naměřené závislosti odporu disku připraveného pomocí metody FIB o průměru $d = 1,5$ μm a výšce $t = 50$ nm v závislosti na působícím magnetickém poli pro magnetické víry s opačnými cirkulacemi. V grafu je červeně vyznačena i směrnice změny odporu poblíž nulové hodnoty magnetického pole.

zřejmě způsobena asymetrií disku. Ta je u připravených vzorků přítomná kvůli geometrii aparatury pro depozici tenkých vrstev (která byla zmíněna v 4.2.4). Asymetrie disku může vzniknout také při dalších procesech přípravy vzorků, především při nedokonale provedeném lift-off procesu či při úpravě velikosti disku pomocí fokusovaného iontového svazku.

5.5 Diskuze výsledků

Provedená měření ukázala, že pro generování náhodných čísel je vhodnější použít disky o menším průměru. Jedním z důvodů je, že v discích o větším průměru nemusí být stav



Obrázek 5.12: Detail disku metodou FIB zmenšeného na průměr $d = 1,5$ μm o výšce $t = 50$ nm s vodivými kontakty pořízený pomocí elektronového mikroskopu.

magnetizace vždy ve formě magnetického víru, ale může přecházet i do blíže neurčeného multidoménového stavu.

Dalším důvodem je, že u těchto disků dochází k nukleaci magnetického víru při velmi malých hodnotách magnetického pole, což má za důsledek složitější a ne vždy úplně průkazné určení směrnice závislosti odporu na magnetickém poli.

V případě snahy o příliš malé disky je nutné vzít v úvahu, že pro měření AMR je nutné na disku vytvořit kontakty, a mezi kontakty musí existovat určitý prostor, aby bylo možné pohyby víru v disku zjišťovat.

V případě disků menších průměrů hraje větší roli případná asymetrie. I malá asymetrie je vzhledem k malé ploše disku pro chování magnetického víru zásadnější, než stejná asymetrie u disku většího průměru.

Na základě výše uvedených experimentálních výsledků se jako vhodná velikost průměru disků ukázala hodnota $d = 1,5$ μm.

Na discích po provedení lift-off procesu zůstávají na hranách reziduální otřepy. Po nepříliš úspěšném pokusu o jejich eliminaci pomocí dvouvrstvého elektronového rezistu byla testována metoda fokusovaného iontového svazku, pomocí které dochází k odprášení určité části disku včetně původní hrany s otřepy, a výsledkem je disk o menším průměru (než původní disk) s vyšší symetrií. V případě příliš malého průměru disku ale touto metodou nelze získat dostatečně symetrický disk, neboť hrany disku začínají vykazovat jisté odchylky od tvaru disku, jejichž původ je zřejmě způsoben neodprášenými zrny materiálu disku. V případě výše uvedené velikosti vhodného průměru disků pro generátor ale tyto odchylky nejsou až takového rázu, aby zabraňovaly nukleaci magnetického víru s náhodnou hodnotou cirkulace.

Vliv magnetického pole má na chování magnetického víru v objemu feromagnetického disku nezanedbatelný vliv. Přestože byla oblast mezi pólovými nástavci mnohem větší než vzorek s naneseným diskem, byl při měření pozorován vliv na polohu vzorku vůči směru pole. U vzorků, jejichž kontakty nebyly zcela rovnoběžné se směrem působícího magnetického pole, často docházelo k tomu, že se magnetický vír pohyboval v disku takovým způsobem, že ze zaznamenaného měření odporu nebylo možné jednoznačně rozhodnout o směru cirkulace magnetického víru či že cirkulace magnetického víru při každé nukleaci nového víru zachovávala svůj směr.

Důvodem této vychýlené polohy vzorku vůči magnetickému poli mohou být nepřesnosti při přípravě vzorku či samotném měření. Těmi mohou být např. nepřesné umístění vzorku při elektronové litografii, nebo upevnění vzorku nesprávným způsobem do keremického pouzdra, či vychýlená poloha vzorku mezi pólovými nástavci cívky, případně kombinace některých či všech zde popsaných možností.

Podstatný je i vliv teploty okolí na výsledky měření. Vybrané vzorky byly měřeny jak při pokojové teplotě, tak při zahřívání v peci při teplotě $T = 80$ °C. Zvýšená teplota v některých případech způsobila, že cirkulace vzorku, jež při pokojové teplotě vznikala stále ve stejném směru, začala vykazovat při opakované nukleaci obě možné hodnoty. Toto odlišné chování je způsobeno tím, že zahřátím je vzorku dodána energie, pomocí které je kompenzována nepříznivá bilance energie magnetizace způsobená asymetrií či defektem disku, a stav cirkulace magnetického víru může vznikat bez ohledu na případné asymetrie či defekty, v ideálním případě náhodně. Vlivu teploty na charakter cirkulace připravených vzorků je větší pozornost věnována v následující kapitole.

6 Statistická analýza dat

Data, která jsou získána pomocí generátoru náhodných čísel, je před jejich dalším využitím nutné otestovat, např. pomocí vybraných postupů, které jsou popsané v kapitole 3.5.

Nejprve jsou uvedeny výsledky testování celých posloupností, čímž je myšlena nepřerušovaná sekvence dat z výstupu generátoru, jejíž délka je dána množstvím všech uskutečněných měření na konkrétním vzorku generátoru. Tato délka se pro jednotlivé vzorky lišila.

Aby bylo možné provést vypovídající porovnání vlastností vzorků různých parametrů za odlišných okolních podmínek, byly jako testovací data použity posloupnosti o velikosti 20000 bitů. Tyto kratší úseky byly získány jednoduše, a to použitím vždy prvních 20000 doposud netestovaných bitů celé posloupnosti získané z generátoru. Tímto rozhodnutím o množství testovaných bitů byly omezeny možnosti použití některých testů, resp. baterií, neboť ke správnému testování náhodnosti vyžadují mnohem větší objem vstupních dat.

Důvody pro volbu takové velikosti souboru vstupních dat pro testy jsou dva. Prvním důvodem je způsob měření, při kterém docházelo ke kvazistatické změně působícího magnetického pole, které se měnilo o zvolený krok každých 300 ms. Proměření cirkulace magnetického víru a následná anihilace, tedy získání jednoho bitu informace, trvalo přibližně 2,5 s. Druhým důvodem je destrukce některých vzorků, ke které došlo buď neočekávaným zkratem při měření či parazitní statickou elektřinou při manipulaci se vzorkem, a nebylo tedy možné z těchto vzorků získat větší objem dat či opakovat měření za jiných podmínek.

Pro testování byly zvoleny baterie testů ENT a testy, které dříve patřily do FIPS PUB 140-2. V případě baterie ENT byly použity testy entropie, výpočtu možné komprese dat vhodným komprimačním postupem, χ^2 test, výpočet aritmetického průměru hodnoty bytu z osmi následujících bitů $\overline{x}$ a koeficient sériové korelace C. Z této baterie nebyl použit výpočet hodnoty π metodou Monte Carlo, neboť použití nedostatečného počtu testovaných dat způsobuje jeho nepřesný, a tedy nevypovídající, výsledek. V případě baterie FIPS PUB 140-2 byly pro posloupnosti o velikosti 20000 bitů provedeny testy distribuce 0 a 1 v posloupnosti, pokerový test, úsekový test a test nejdelšího úseku. V případě delších či kratších posloupností, které byly v rámci analýzy výstupu generátoru zkoumány, byly použity totožné testy programu ENT a z baterie FIPS PUB 140-2 pouze test distribuce hodnot bitů.

Při provádění testů je nutné brát na vědomí, že testovací baterie, resp. jednotlivé testy nahlížejí na kvalitu testovaných posloupností z hlediska statistiky. V případě generátoru skutečně náhodných čísel, jenž využívá pro produkování čísel vhodně zvolený fyzikální jev, není zaručeno, že čísla na jeho výstupu, přestože budou z hlediska jejich vygenerování zcela jasně náhodná, budou náhodná i z hlediska statistiky. Proto je při provedení statistických testů na neupravovaných posloupnostech takového generátoru vhodné brát výsledky jako orientační, a v případě připravených generátorů v této práci i jako vodítko, na základě kterého bude možné určit chování generátoru za různých podmínek a následně těchto zjištění využít pro budoucí úpravy navrženého konceptu.

V této kapitole budou nejprve pro testované generátory uvedeny výsledky testů celých posloupností. Následovat budou výstupy testů obou baterií pro posloupnosti o velikosti 20000. U těchto posloupností bude porovnán charakter náhodných čísel s ohledem na parametry vzorku a okolní podmínky při generování čísel. Následovat budou vlastnosti posloupností, které vznikly z aplikace principu von Neumannova extraktoru na celé posloupnosti. Závěrem kapitoly budou zjištěné vlastnosti čísel v závislosti na přípravě generátoru a vnějších podmínkách diskutovány.

Název	d [[μm]]	t [nm]	FIB	Střed
G1	1,5	75	ne	ano
G2	1,5	30	ano	ne
G3	1,5	30	ano	ne
G4	1,5	30	ano	ne

Tabulka 6.1: Označení testovaných vzorků s uvedením jejich důležitých parametrů. Těmi jsou průměr d a výška t disku. Sloupec FIB udává, zda-li byl disk před nanesením vodivých kontaktů opracován metodou fokusovaného iontového svazku. Sloupec Střed nese informaci, zda-li se disk při EBL nacházel ve středu zápisového pole.

Pro jednodušší orientaci bude pro generátory dále využíváno notace, která je uvedena v tabulce 6.1. V tabulce jsou pro jednotlivé vzorky s připraveným generátorem náhodných čísel uvedeny průměr a výška disku, a ve sloupci označeném jako FIB se nachází informace, zda-li byl před kontaktováním disk opracován metodou fokusovaného iontového svazku či nikoliv. Sloupec Střed udává polohu disku, na které byl umístěn při přípravě struktury pro elektronovou litografii, resp. zda-li se nacházel v jejím středu či nikoliv. Tato pozice disku se ukázala být podstatná pro přítomnost či nepřítomnost nečistot zlata na povrchu disku, kdy při pozici uprostřed pole pro zápis k objevování se zlatých nečistot docházelo, ale v případě polohy disku mimo střed nikoli.

6.1 Neupravovaná data

Nejprve budou uvedeny celé posloupnosti jednotlivých generátorů. Pro odlišení posloupností získaných za různých okolních podmínek slouží přiřazené indexy ve formě písmen. V případě vzorku G1 jde o jednu posloupnost, která byla generována beze změny okolních podmínek za běžné teploty, a příslušná posloupnost G1–a sestává z 74999 bitů.

Vzorek generátoru G2 produkoval dvě různé posloupnosti za stejné (pokojové) teploty, ale při různé poloze vzorku v působícím magnetickém poli. K této změně došlo vyjmutím a opětovným vrácením vzorku mezi pólové nástavce cívky, přičemž zřejmě nedošlo k totožné poloze vzorku vůči magnetickému poli, a i tato nepatrná změna způsobila odlišný charakter generovaných čísel. Posloupnost G2–a vznikla před změnou polohy vzorku vůči poli a obsahuje 89573 bitů, posloupnost G2–b po změně polohy její velikost je 23822 bitů.

V případě vzorku G3 byla náhodná čísla generována při různých teplotách, a to při pokojové teplotě a poté při zahřívání na teplotu $T = 80$ °C. Délky posloupností jsou 26491 bitů pro nezahřívaný (G3–a) a 20000 bitů pro zahřívaný (G3–b) vzorek.

Poslední vzorek byl v průběhu celého generování zahřívaný na teplotu $T = 80$ °C. Výstupem tohoto generátoru byla posloupnost G4–a o velikosti 63603 bitů.

Pro uvedené posloupnosti jsou výsledky použitých testů baterie ENT uvedeny v tabulce 6.2 a rozložení bitů o hodnotě 0 a 1 v posloupnosti jsou zanesené v tabulce 6.3. Přestože výsledky již na první pohled nejsou uspokojivé, lze z nich zjistit několik vlastností nezpracovaných výstupních dat jednotlivých generátorů.

Výsledky testu χ^2 lze interpretovat tak, že všechny posloupnosti nejsou dostatečně náhodné. Podobně špatný výsledek ukazuje i vysoká hodnota možné komprese, která se pohybuje pro všechny posloupnosti mezi 87–90 %.

Sekvence	Entropie [–]	Komprese [%]	χ^2 [%]	$\overline{x}$ [–]	C [–]
NČ	8,0	0	10–90	127,5	0,00
G1–a	0,734395	90	0,01	48,2063	0,098146
G2–a	0,732199	88	0,01	48,2052	0,073759
G2–b	0,941601	88	0,01	48,3587	0,029178
G3–a	0,915310	88	0,01	48,3304	0,757360
G3–b	0,993521	87	0,01	48,4526	0,104772
G4–a	0,973955	87	0,01	48,5947	0,039276

Tabulka 6.2: Výsledky testů baterie ENT pro celé posloupnosti náhodných čísel. Řádek NČ značí hodnoty, kterých by dosáhla statisticky náhodná čísla. Další řádky přísluší jednotlivým posloupnostem připravených generátorů.

Sekvence	0[–]	1 [–]	0 [%]	1 [%]
G1–a	59525	15474	0,793677	0,206323
G2–a	71193	18380	0,794804	0,205196
G2–b	15277	8545	0,641298	0,358702
G3–a	17739	8752	0669624	0,330376
G3–b	10967	9053	0,54735	0,45265
G4–a	25777	39826	0,405280	0,594720

Tabulka 6.3: Distribuce bitů o hodnotě 0 a 1 pro celé posloupnosti náhodných čísel.

Výpočet aritmetického průměru hodnoty bytu $\overline{x}$ vychází u všech posloupností mezi 48,14–48,6376. Pro zcela náhodná čísla by měla vyjít hodnota 127,5, pro testované generátory je získaná hodnota přibližně 2,5krát nižší.

Koeficient sériové korelace C pro náhodná čísla dosahuje hodnoty 0. Pro téměř všechny posloupnosti se hodnota tohoto koeficientu pohybovala v rozmezí přibližně 0,04–0,10, což značí poměrně nezávislá čísla. Výjimkou je posloupnost G3–a, pro kterou vyšel koeficient $C = 0,76$, což se blíží hodnotě $C = 1$, která značí sobě závislá čísla.

Porovnání posloupností G2–a a G2–b ukazuje, že kvalitu generovaných čísel ovlivňuje umístění v magnetickém poli. Při manipulaci se vzorkem mezi měřením posloupností zřejmě došlo k rekonfiguraci polohy kontaktů na disku a kontaktů, což mělo za následek zvýšení entropie dat, dále snížení korelace, a také lepší rozložení bitů o hodnotě 0 a 1 v posloupnosti. Podrobnosti o vzájemné poloze kontaktů na disku a magnetického pole jsou již uvedeny v kapitole 5.5.

Dále je z tabulek patrné, že generování čísel při umístění vzorku do vyšší teploty, než je teplota pokojová, má na produkovaná data pozitivní vliv. K této informaci lze dospět jak porovnáním výsledků G4–a s ostatními nezahřívanými vzorky, tak přímo v rámci jednoho vzorku u posloupností G3–a a G3–b. Původ odlišného chování při různé teplotě okolí je popsaný již v kapitole 5.5.

V tabulce 6.4 jsou zaneseny výsledky testů baterie ENT pro posloupnosti o velikosti 20000 bitů. Posloupnosti této délky byly získány z dat získaných jednotlivými generátory tak, že prvních 20000 bitů bylo přiřazeno do posloupnosti s indexem 1, dalších 20000 posloupnosti 2 atp. Vzhledem ke konečnému množství získaných dat různými generátory každému vzorku přísluší jiné množství posloupností. Posloupnosti kratší než požadovaných 20000 bitů nebyly použity, neboť nesplňují délku vyžadovanou testy z baterie FIPS PUB 140-2. Tedy pro generátor G1 jsou pro testování k dispozici 3 posloupnosti vzniklé za stej-

Sekvence	Entropie [–]	Komprese [%]	χ^2 [%]	$\overline{x}$ [–]	C [–]
NČ	8,0	0	10–90	127,5	0,00
G1–1	0,844675	89	0,01	48,2723	0,117498
G1–2	0,762897	90	0,01	48,2215	0,093296
G1–3	0,659646	91	0,01	48,1709	0,010661
G2–1	0,831537	89	0,01	48,2632	0,060207
G2–2	0,606955	92	0,01	48,1489	0,056780
G2–3	0,776352	90	0,01	48,2291	0,077504
G2–4	0,731718	90	0,01	48,2049	0,039863
G2–5	0,943221	88	0,01	48,3607	0,034398
G3–1	0,881535	88	0,01	48,3002	0,827447
G3–2	0,993521	87	0,01	48,4526	0,104772
G4–1	0,985011	87	0,01	48,5720	0,034609
G4–2	0,944657	88	0,01	48,6376	0,036423
G4–3	0,983446	87	0,01	48,5756	0,042306

Tabulka 6.4: Výsledky testů baterie ENT pro posloupnosti o velikosti 20000 bitů. Řádek NČ značí hodnoty, kterých by dosáhla statisticky náhodná čísla. Další řádky přísluší jednotlivým posloupnostem připravených generátorů.

ných podmínek, pro generátor G2 celkem 5 posloupností, z toho 4 (G2–1 až G2–4) před změnou polohy v magnetickém poli a 1 po změně (G2–5), pro generátor G3 lze testovat posloupnost generovanou před zahřátím (G3–1) a po zahřátí na teplotu $T = 80$ °C (G3–2) a tři posloupnosti při teplotě $T = 80$ °C pro generátor G4. Výsledky distribučního testu, pokerového testu a testu dlouhých úseků těchto posloupností jsou uvedeny v tabulce 6.5, výsledky úsekového testu jsou rozepsány v tabulce 6.6. V tabulce 6.5 sloupec Dlouhý úsek obsahuje informaci o délce nejdelšího úseku stejných bitů a sloupec P/N udává, zda-li daná posloupnost třemi testy (frekvenční, pokerový a dlouhého úseku) úspěšně prošla (P) či neprošla (N), a pokud neprošla, tak v kolika případech. Stejně označený sloupec v tabulce 6.6 dává informaci, zda-li posloupnost splňuje požadavky na počty úseků (P), či nesplňuje, a v případě nesplnění i počet překročení daných rozmezí. Hodnoty, na základě kterých dochází k porovnání se získanými výsledky, jsou podrobněji uvedeny v kapitole 3.5.6.

Na základě porovnání posloupností o stejné délce lze nejen zjistit odlišnosti o vlastnostech výstupních dat generátoru při různých okolních podmínkách, ale také, pokud se porovnávají různé posloupnosti generované stejným generátorem, zda-li generátor nějakým zásadním způsobem nemění své vlastnosti v čase, resp. po vygenerování 20000 bitů. K nějakým zřetelným nenadálým změnám v rámci kratších úseků výše uvedené celé posloupnosti nedochází.

I v případě částí celých posloupností dle χ^2 testu nejsou všechny posloupnosti dostatečně náhodné. Podobně špatný výsledek, místy i horší, naznačuje i vysoká hodnota možné komprese jednotlivých úseků posloupností, která se pohybuje mezi 87–92 %.

Výpočet aritmetického průměru hodnoty bytu $\overline{x}$ je pro všechny posloupnosti podobný, vzájemná odchylka není větší než 0,5. Tyto hodnoty se ani nijak zásadně neliší pro hodnoty vypočtené pro celé posloupnosti.

Sekvence	0 [–]	1 [–]	0 [%]	1 [%]	Poker	Dlouhý úsek	P/N
G1–1	14555	4554	0,72775	0,27225	8118,73	425	3N
G1–2	15570	4430	0,7785	0,2215	12328,84	607	3N
G1–3	16583	3417	0,82915	0,17085	16540,83	51	3N
G2–1	14736	5264	0,7368	0,2632	7596,50	15	2N
G2–2	17023	2977	0,85115	0,14885	21853,95	83	3N
G2–3	15419	4581	0,77095	0,22905	10759,39	76	3N
G2–4	15901	4099	0,79505	0,20495	12852,66	133	3N
G2–5	12787	7213	0,63935	0,36065	1891,68	25	2N
G3–1	13996	6004	0,6998	0,3002	31823,04	9061	3N
G3–2	10967	9053	0,54735	0,45265	297,27	26	3N
G4–1	8561	11439	0,428050	0,57195	25,33	25	1N
G4–2	7248	12752	0,3624	0,6376	1163,45	13	2N
G4–3	8488	11512	0,4244	0,5756	126,15	13	2N

Tabulka 6.5: Výsledky distribučního testu, pokerového testu a testu dlouhých úseků provedeného pro posloupnosti o velikosti 20000 bitů. Výstupem distribučního testu je rozložení 1 a 0 v testované posloupnosti. Sloupec Poker udává hodnotu získanou dle příslušného postupu uvedeném v kapitole 3.5.6. Sloupec označený jako Dlouhý úsek obsahuje informaci o velikosti nejdelšího úseku tvořeného stejnými bity.

Sekvence	1 [–]	2 [–]	3 [–]	4 [–]	5 [–]	6 [–]	P/N
G1–1	1949	1191	641	443	259	962	4N
G1–2	1304	877	621	421	281	926	5N
G1–3	614	512	374	347	281	1289	5N
G2–1	11092	2603	701	211	72	57	5N
G2–2	588	445	327	259	207	1151	4N
G2–3	1323	861	634	434	309	1020	5N
G2–4	970	756	564	426	308	1075	5N
G2–5	2761	1611	1042	609	413	777	6N
G3–1	5280	461	40	47	10	166	5N
G3–2	6511	2377	1016	480	239	324	6N
G4–1	3835	2048	1156	599	368	555	6N
G4–2	8300	2831	969	357	177	118	3N
G4–3	6833	2698	1056	468	233	224	6N

Tabulka 6.6: Výsledky úsekového testu posloupností o velikosti 20000 bitů. Sloupec P/N udává, zda-li daná posloupnost testem úspěšně prošla (P) či neprošla (N), a pokud neprošla, tak v kolika případech.

Koeficient sériové korelace C naznačuje, že v rámci posloupnosti G3–1 jsou vygenerovaná čísla na sobě poměrně silně závislá (zcela závislá čísla značí $C = 1$). Pro ostatní posloupnosti je závislost mezi čísly posloupností slabá.

Výsledky frekvenčního testu, pokerového testu, úsekového testu a testu dlouhých posloupností jsou neuspokojivé. Na jejich základě by žádný z připravených vzorků generátoru testy baterie FIPS PUB 140-2 neprošel.

S přihlédnutím k testům baterie ENT lze konstatovat, že v případě generátoru G2 je rozdíl mezi posloupnostmi před (G2–1 až G2–4) a po změně polohy (G2–5) v magnetickém poli znatelný pouze ve velikosti entropie. V případě dalších testů není rozdíl příliš velký.

Změna teploty okolí se projevuje markantněji. A to jak v případě posloupností G3–1 a G3–2 získaných ze stejného generátoru, tak v případě porovnání posloupností generátoru G4 vůči posloupnostem produkovaných generátory při pokojové teplotě. V případě přímého porovnání, tedy posloupnostmi generátoru G3, bylo zahřátím dosaženo vyšší entropie dat a 8krát nižšího koeficientu sériové korelace C. V případě posloupností získaných generátorem G4 je patrná vyšší entropie a poměrně nízká hodnota koeficientu sériové korelace C vůči ostatním posloupnostem.

6.2 Použití von Neumannova extraktoru

Ve snaze o dosažení lepších výsledků statistických testů byl na čísla celých posloupností o dostatečné velikosti použit princip von Neumannova extraktoru. Ten spočívá v rozdělení posloupnosti na dvojice, a pokud se ve dvojici čísla liší, je jako náhodný bit použito číslo druhé.

V tabulce 6.7 jsou zaneseny výsledky baterie ENT pro posloupnosti generátorů, které byly zpracovány pomocí principu von Neumannova extraktoru. Jde jen o generátory G1, G2 a G4, u kterých bylo díky větším velikostem posloupností možné vygenerovat větší množství bitů. Ale i přesto nedosáhla délka takto zpracovaných posloupností ani velikosti 20000 bitů, pro G1 takto vznikla posloupnost G1–vN o velikosti 11050 bitů, pro G2 posloupnost G2–vN o 13484 bitech a pro G3 sekvence G3–vN obsahující 14593 bitů. K testování náhodnosti byly na tyto posloupnosti použity stejné testy baterie ENT jako v předchozích případech. Vzhledem k tomu, že tyto posloupnosti neměly dostatečnou délku předepsanou baterií FIPS PUB 140-2 (20000 bitů), z této baterie byl jen orientačně proveden frekvenční test bez dalšího vyhodnocení. Příslušné rozložení bitů v těchto posloupnostech získané frekvenčním testem lze nalézt v tabulce 6.8.

Sekvence	Entropie [–]	Komprese [%]	χ^2 [%]	$\overline{x}$ [–]	C [–]
NČ	8,0	0	10–90	127,5	0,00
G1–vN	1,000000	87	0,01	48,5002	0,027692
G2–vN	0,999987	87	0,01	48,4979	0,002798
G4–vN	0,999838	87	0,01	48,5075	-0,003447

Tabulka 6.7: Výsledky statistických testů baterie ENT pro posloupnosti, které vznikly zařazením von Neumannova extraktoru na výstup generátoru.

Sekvence	0 [–]	1 [–]	0 [%]	1 [%]
G1–vN	5523	5527	0,499819	0,500181
G2–vN	6766	6718	0,502149	0,497851
G4–vN	7187	7406	0,492496	0,507504

Tabulka 6.8: Distribuce bitů o hodnotě 0 a 1 pro celé posloupnosti náhodných čísel získaných z připravených generátorů s aplikací principu von Neumannova extraktoru na získaná data.

U všech vytvořených posloupností se entropie blíží či rovná 1, což je sice mírné zlepšení oproti předchozím výsledkům, ale nijak zásadní. Velikost možné komprese dat se v porov-

nání s nezpracovanými čísly také viditelně nezměnila. U nově vytvořených posloupností je možné data komprimací snížit o 87 %. Změny nedošel ani výsledek testu χ^2 a nedošlo ani k většímu navýšení hodnoty aritmetického průměru hodnoty bytu $\overline{x}$.

Ke snížení došlo u koeficientu korelace C, a to o jeden řád. Z tohoto hlediska tedy ke zlepšení vzájemné nezávislosti mezi čísly posloupnosti došlo. K výraznému zlepšení došlo v případě frekvenčního testu, tedy rozložení 1 a 0 v posloupnosti. Distribuce čísel se při použití von Neumannova extraktoru ve všech posloupnostech blíží ideální hodnotě 0,5:0,5.

6.3 Diskuze výsledků

Výsledky použitých testů na posloupnosti čísel, které byly získány z experimentálně připravených generátorů náhodných čísel dle konceptu v této práci představeném umožňují provést srovnání charakteru generovaných čísel pro vzorky připravené odlišným postupem, při různé poloze v magnetickém poli a při rozdílné teplotě při generování.

Porovnání vzorků, jejichž příprava se lišila v opracování či neopracování disku metodou fokusovaného iontového svazku před nanesením vodivých kontaktů, u kterých probíhalo získávání dat při stejných podmínkách, neodhaluje žádné viditelné rozdíly. Z hlediska vlastností náhodných čísel tedy nezáleží na zvoleném postupu při přípravě vzorku, podstatná je pouze výsledná struktura.

Při statistickém zpracování náhodných čísel získaných z připravených generátorů bylo zjištěno, že změna mezi dvěma polohami totožného vzorku způsobila jak zlepšení entropie, tak lepší rozdělení hodnoty bitů 0 a 1. Důvodem této změny byla mírně odlišná poloha vzorku v magnetickém poli, což způsobilo ovlivnění mechanismu vzniku magnetického víru, tedy vlastnosti tvořených čísel. Pro dosažení ideálních výsledků statistických testů náhodných čísel generátoru by bylo nutné působit magnetickým polem v rovině disku rovnoběžně s asymetrickými kontakty.

Generování čísel proběhlo při dvou různých teplotách okolí, a to za běžné pokojové teploty a při teplotě $T = 80$ °C. Bylo zjištěno, že pro generování čísel při vyšší teplotě dosahují čísla lepších výsledků v některých testech, především lepšího rozložení bitů v rámci posloupnosti, poté vyšší hustoty dat (entropie) a menší sériové korelace. Lze tedy konstatovat, že pro generování náhodných čísel pomocí generátoru navrženém v rámci této práce je vhodnější použít vyšší teplotu než pokojovou.

Při zpracování dat pomocí von Neumannova extraktoru lze dosáhnout lepších vlastností získaných čísel. Zlepšení se nejvíce projevilo pro rozložení bitů o hodnotách 0 a 1, jejichž poměr téměř dosahuje pro náhodná čísla ideální hodnoty 50:50. Dále došlo k mírnému zvýšení entropie dat. Lepších vlastností dosáhl i koeficient sériové korelace, jenž se o řád snížil. Nevýhodou použití tohoto extraktoru se ukázalo výrazné snížení čísel v posloupnosti v porovnání s její původní velikostí. To ale může být vyřešeno buď delší dobou generování stejnou metodou, případně vhodnou úpravou konceptu generátoru, při které by docházelo k rychlejšímu produkování dat. Další alternativou by mohlo nalezení vhodnějšího extraktoru.

Provedení testů odhalilo, že navržený generátor je ze statistického hlediska nenáhodný. Před jeho možným využitím je nutné buď upravit jeho koncept, který by zaručoval příznivější podmínky pro generování náhodných čísel, nebo zlepšit kvalitu generovaných čísel ze statistického hlediska pomocí vhodně zvoleného extraktoru.

7 Závěr

Tato práce se zabývá problematikou generování skutečně náhodných čísel pomocí magnetických nanostruktur. Pro její tvorbu byly stanoveny tři hlavní cíle. Prvním cílem bylo provedení rešeršní studie problematiky generování náhodných čísel, se zřetelem k využití magnetických vírů. Této problematice, především s ohledem na generování skutečně náhodných čísel, je věnován poměrně rozsáhlý prostor. Navíc bylo zjištěno, že využití magnetických vírů pro generování náhodných čísel je zcela novátorský koncept, tomuto přístupu se dle současné odborné literatury a veřejně dostupných patentů doposud nikdo nevěnoval. Druhým cílem bylo navržení konceptu generátoru náhodných čísel, který je založený na magnetických vírech v magnetických nanostrukturách. Tohoto cíle bylo také dosaženo, požadovaný koncept včetně vhodné měřicí metody je navržen. Poslední cíl práce sestával z přípravy vzorků a jejich experimentálního ověření. I tento cíl byl splněn. Vzorky s generátory byly připraveny a v průběhu měření optimalizovány z hlediska jejich přípravy. Následně bylo provedeno testování vlastností generovaných čísel při různých podmínkách, na základě kterého lze představený koncept nadále upravovat a zlepšovat jeho vlastnosti. Všechny zadané cíle diplomové práce tedy byly úspěšně splněny.

V rámci práce byl navržen a posléze experimentálně ověřen koncept generátoru, který je založen na elektrickém měření vlastností magnetického víru metodou anizotropní magnetorezistivity. Prvkem, ve kterém se vlivem vnějšího magnetického pole ovlivňovala magnetorezistivita, byl plochý disk z magneticky měkkého materiálu, jehož rozměry byly voleny tak, aby jeho magnetizace (v případě, kdy disk nebyl v saturovaném, tedy v jednodoménovém stavu) přecházela do tzv. magnetického víru. V závislosti na směru cirkulace magnetizace v rovině disku, tedy z jedné veličin, pomocí kterých lze popsat stav magnetického víru, bylo možné tuto veličinu určit.

Koncept generátoru spočívá z několika prvků. Element, který je zdrojem náhodnosti, je feromagnetický disk. Materiál, který byl v rámci této práce zvolen, je slitina niklu a železa v poměru 80:20, jež se nazývá permalloy. Podstatná část experimentální přípravy vzorků generátoru spočívala v optimalizaci parametrů tohoto disku, a to jak jeho rozměrů, tak i jeho výroby.

V případě jeho rozměrů bylo experimentálně zjištěno, že disky o větším průměru nejsou pro generování náhodných čísel příliš vhodné, neboť v nich není podmíněna magnetizace ve stavu magnetického víru, ale může dojít i k obecnému a blíže neurčenému multidoménovému stavu. Na druhou stranu se ukázalo, že ani příliš malý průměr disku na vzorcích nezaručil lepší vlastnosti a vznik magnetického víru. Důvod tohoto zjištění spočívá v nedostatečně symetrickém a defektu prostém vyrobeném disku, což je způsobeno především nepřesnostmi. I malá asymetrie disku o malém průměru ovlivňuje stav magnetizace mnohem zásadněji, než by ovlivňovala disk o průměru větším. Experimentálním měřením bylo zjištěno, že při přípravě vzorků generátoru metodami použitými v rámci této práce je vhodný průměr disku $d = 1,5\ \mu$m. V případě výšky disku nebylo dosaženo jednoznačného závěru. Náhodné chování při nukleaci magnetického víru bylo pozorováno u disků o výšce 30 nm a 50 nm. Rozměrem, který měl na nukleaci magnetického víru zásadnější vliv, je průměr disku.

Před dalším krokem, tedy nanesením vodivých kontaktů na připravený disk, bylo možné disk opracovat pomocí fokusovaného iontového svazku. Tímto opracováním je myšleno zmenšení disku na menší průměr. Touto procedurou lze eliminovat existenci reziduálních otřepů na hranách, které vznikají při lift-off procesu po depozici kovu. Pro ex-

perimentální měření byly připraveny jak vzorky, u nichž byly naneseny kontakty ihned po lift-off procesu, tak i vzorky, u nichž ke zmenšení průměru disku touto metodou došlo. Pro přípravu disků s vyšší symetrií se z hlediska přípravy disků jeví jako výhodnější metoda, při které je výsledný rozměr disku získán odprášením hrany původně většího disku. Po provedení statistických testů vygenerovaných čísel bylo zjištěno, že se posloupnosti generátorů s disky upravenými i neupravenými od sebe nijak zásadně neliší. Podstatná je symetrie disku, nikoli postup, pomocí kterého se lze k takovému disku dobrat.

Měřicí metoda, jež byla použita v rámci navrženého konceptu generátoru, je založená na magnetorezistanci, tedy závislosti odporu materiálu na působícím magnetickém poli. V případě disku, jehož magnetizace se nachází ve stavu magnetického víru, lze změnu odporu interpretovat jako důsledek pohybu magnetického víru v závislosti na působícím magnetickém poli. Při vhodně navrženém experimentálním uspořádání je možné na základě změny odporu jednoznačně určit směr cirkulace magnetického víru. Konkrétní určování cirkulace magnetického víru je prováděno na základě sklonu křivky odporu poblíž nulové hodnoty magnetického pole. Odečtená cirkulace je následně transformována do hodnoty bitu. Vzhledem k tomu, že cirkulace magnetizace i binární čísla mohou nabývat pouze dvou hodnot, tato transformace nevyžaduje žádné složité postupy.

Připravené vzorky s generátory náhodných čísel, které byly připraveny na základě navrženého konceptu, byly proměřeny při několika různých stavech okolních podmínek, a na základě jejich výsledků bylo odhaleno několik důležitých zjištění.

Jako poměrně zásadní vliv na charakter produkovaných čísel se prokázala teplota okolí vzorku při generování vzorku. Měřeny byly vzorky jak při běžné pokojové teplotě, tak po zahřátí na teplotu $T = 80$ °C. Ze získaných měření bylo možné porovnat jak různé vzorky, které byly měřené za různých podmínek, tak i vzorek, u kterého došlo k proměření při obou možných teplotách. Na základě dosažených výsledků vybraných statistických testů vygenerovaných posloupností čísel je ukázáno, že pro dosažení jejich lepších vlastností je lepší generátor při generování čísel udržovat na vyšší teplotě.

V průběhu měření byla zpozorována i silná závislost natočení vzorku v externím magnetickém poli. Tohoto zjištění bylo dosaženo pouze kvalitativně, a to poměrně nečekaným způsobem. Došlo k němu v případě vzorku, u kterého byl naměřen dostatečně velký soubor dat, ale poté se vzorkem bylo manipulováno, a po jeho vrácení do oblasti působení magnetického pole již byly vlastnosti generovaných čísel dle statistických testů odlišné. Pro dosažení nejlepších vlastností generovaných čísel by poloha vzorku v magnetickém poli měla být taková, aby směr působícího pole odpovídal rovině disku a byl rovnoběžný s kontakty na disk nanesenými. Pozorované odlišné vlastnosti čísel při různých polohách vzorku byly způsobeny odchylkami způsobenými při přípravě vzorku při elektronové litografii, při umístění vzorku do keramického pouzdra či při upevnění pouzdra se vzorkem mezi pólové nástavce cívky indukující magnetické pole způsobující pohyb magnetického víru v rámci disku, případně součtem více či všech těchto faktorů.

Získané posloupnosti čísel byly podrobeny statistickým testům. V případě nijak neupravených posloupností jsou tyto výsledky pouze orientační, a bylo jich využito především pro porovnání generátorů za různých podmínek. Jediné, co lze na základě těchto testů pro vygenerovaná skutečně náhodná čísla konstatovat, je, že z hlediska statistiky je generátor nenáhodný. Pro jeho další využití v aplikaci, která požaduje statisticky kvalitnější čísla, je nutné generátor upravit vhodnou metodou, pomocí které dojde ke zlepšení statistických výsledků.

V případě navrženého generátoru v kombinaci s von Neumannovým extraktorem jsou testy již o něco více vypovídající. V tomto případě lze rovněž konstatovat, že nedošlo k zásadnímu zlepšení jejich vlastností oproti číslům nijak neupravovaným.

Zjištění zde uvedená naznačují, že magnetické nanostruktury mohou být využity jako zdroj náhodnosti pro generátor skutečně náhodných čísel. Je ale nutné vyřešit několik problémů, jejichž úspěšné řešení by mělo pomoci k dosažení lepších vlastností generátorů.

Jak bylo v této práci ukázáno, chování magnetického víru v nanostruktuře je podstatně ovlivněno tvarem nanostruktury, v tomto případě disku. Podaří-li se optimalizovat jednotlivé kroky přípravy vzorku do té míry, že bude dosaženo perfektně symetrického disku bez defektů, nečistot či zbytků elektronového rezistu, náhodnost výstupních dat generátoru se zlepší.

Pro možné využití generátoru je nutné zajistit, aby jím produkovaná čísla vykazovala dobré statistické vlastnosti, tedy aby generátor dokázal projít předepsanými statistickými testy. Tato úprava generátoru by spočívala v nalezení vhodného extraktoru.

Dalšími možnými přístupy, kterými by bylo možné zlepšit generátor náhodných čísel založený na magnetických nanostrukturách, mohou spočívat například ve zrychlení procesu generování čísel. To by bylo možné dosáhnout umístěním feromagnetického disku na vlnovod, ve kterém by bylo proudovými impulsy generováno magnetické pole, pomocí kterého by bylo možné určit směr cirkulace magnetického víru. Vzhledem k tomu, že magnetický vír je charakterizován dvěma na sobě nezávislými veličinami, tak se stále naskýtá možnost využití druhé veličiny, polarity jádra, která nebyla v této práci předmětem zájmu.

Tyto uvedené myšlenky mohou být využity pro vylepšení generátoru náhodných čísel založeného na magnetických nanostrukturách, který bude dále rozvíjet koncept generátoru představeného v této práci. Vzhledem k tomu, že v této práci je představena zcela nová idea pro generování náhodných čísel, je v této oblasti dostatečný prostor pro její další rozvíjení a různé modifikace.

Literatura

[1] WOLF, S. A., A. Y. CHTCHELKANOVA a D. M. TREGER. *Spintronics—A retrospective and perspective.* IBM Journal of Research and Development. 2006, vol. 50, issue 1, s. 101–110. DOI: 10.1147/rd.501.0101. Dostupné z http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5388780&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5388780.

[2] CHOU, S. Y., P. R. KRAUSS a L. KONG. *Nanolithographically defined magnetic structures and quantum magnetic disk (invited).* Journal of Applied Physics. 1996, vol. 79, issue 8, s. 6101–6106. DOI: 10.1063/1.362440. Dostupné z: http://www.researchgate.net/profile/Stephen_Chou2/publication/224486835_Nanolithographically_defined_magnetic_structures_and_quantum_magnetic_disk_(invited)/links/00b7d52175784c0a9d000000.pdf.

[3] ROSS, C. A. *Patterned magnetic recording media.* Annual Review of Materials Research. 2001, vol. 31, issue 1, s. 203–235. DOI: 10.1146/annurev.matsci.31.1.203. Dostupné z: http://www.annualreviews.org/doi/abs/10.1146/annurev.matsci.31.1.203.

[4] JUNG, H., *et al. Logic Operations Based on Magnetic-Vortex-State Networks.* ACS Nano. 2012, vol. 6, issue 5, s. 3712–3717. DOI: 10.1021/nn3000143. Dostupné z: http://pubs.acs.org/doi/abs/10.1021/nn3000143.

[5] KUMAR, D., S. BARMAN a A. BARMAN. *Magnetic Vortex Based Transistor Operations.* Scientific Reports. 2014, vol. 4, 8 s. DOI: 10.1038/srep04108. Dostupné z: http://www.nature.com/doifinder/10.1038/srep04108.

[6] JANČÁŘ, P. *Radioaktivní rozpad a náhodná čísla.* Elektrorevue - Internetový časopis. 2007, vydáno 21.4.2007, 10 s. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/file.php?id=200000122-597045a6a5.

[7] WALKER, J. *HotBits: Genuine random numbers, generated by radioactive decay.* [online]. 1996, 2006 [cit. 2015–01–13]. Dostupné z: https://www.fourmilab.ch/hotbits/.

[8] EPSTEIN, M., *et al. Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts.* In: Cryptographic Hardware and Embedded Systems – CHES 2003. Springer Berlin Heidelberg. 2003. s. 152–165. DOI: 10.1007/978-3-540-45238-6_13. ISBN: 978-3-540-45238-6. Dostupné z: http://link.springer.com/10.1007/978-3-540-45238-6_13.

[9] HAAHR, M. *RANDOM.ORG.* [online]. 1998 [cit. 2015–01–25]. Dostupné z: https://www.random.org/.

[10] XU, F., *et al. Ultrafast quantum random number generation based on quantum phase fluctuations.* Optics Express. 2012, vol. 20, issue 11, s. 12366–12377. DOI: 10.1364/OE.20.012366. Dostupné z: http://www.opticsinfobase.org/abstract.cfm?URI=oe-20-11-12366.

[11] WILLIAMS, C. R. S., *et al. Fast physical random number generator using amplified spontaneous emission.* Optics Express. 2010, vol. 18, issue 23, s. 23584–23597. DOI: 10.1364/oe.18.023584. Dostupné z: https://www.osapublishing.org/oe/fulltext.cfm?uri=oe-18-23-23584&id=206871.

[12] ARGYRIS, A., *et al. Sub-Tb/s Physical Random Bit Generators Based on Direct Detection of Amplified Spontaneous Emission Signals.* Journal of Lightwave Technology. 2012, vol. 30, issue 9, s. 1329–1334. DOI: 10.1007/springerreference_7989. Dostupné z: https://www.osapublishing.org/jlt/abstract.cfm?uri=jlt-30-9-1329.

[13] LI, X., *et al. Scalable parallel physical random number generator based on a superluminescent LED.* Optics Letters. 2011, vol. 36, issue 6, s. 1020–1022. DOI: 10.1364/OL.36.001020. Dostupné z: http://www.opticsinfobase.org/abstract.cfm?URI=ol-36-6-1020.

[14] STEFANOV, A., *et al. Optical quantum random number generator.* Journal of Modern Optics. 2000, vol. 47, issue 4, s. 595–598. DOI: 10.1080/09500340008233380. Dostupné z http://www.tandfonline.com/doi/abs/10.1080/09500340008233380#.VWduV8YqctQ.

[15] BLUM, L., M. BLUM a M. SHUB. *A Simple Unpredictable Pseudo-Random Number Generator.* SIAM Journal on Computing. 1986, vol. 15, issue 2, s. 364–383. DOI: 10.1137/0215025. Dostupné z: http://epubs.siam.org/doi/abs/10.1137/0215025.

[16] MATSUMOTO, M. a T. NISHIMURA. *Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator.* ACM Transactions on Modeling and Computer Simulation. 1998, vol. 8, issue 1, s. 3–30. DOI: 10.1145/272991.272995. Dostupné z: http://dl.acm.org/citation.cfm?id=272995.

[17] SACHOVÁ, R. *Generování náhodných dat z biometrických vzorků.* Praha: Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, 2011. 78 s. Vedoucí diplomové práce Ing. Mgr. Zdeněk Říha, Ph.D.

[18] HALLIDAY, D., R. RESNICK a J. WALKER. *Fyzika: vysokoškolská učebnice obecné fyziky.* 1. české vydání, 1. dotisk. Překlad Jan Obdržálek, Bohumila Lencová, Petr Dub. V Brně: VUTIUM, 2006, 1198 s. Překlady vysokoškolských učebnic. ISBN 80-214-1868-0.

[19] COEY, J. *Magnetism and magnetic materials.* 1. vydání. New York: Cambridge University Press, 2010, xii, 614 s. ISBN 978-0-521-81614-4.

[20] CHIEN, C. L., Frank Q. ZHU a J.-G. ZHU. *Patterned Nanomagnets.* Physics Today. 2007, vol. 60, issue 6, s. 40–45. DOI: 10.1063/1.2754602. Dostupné z: http://scitation.aip.org/content/aip/magazine/physicstoday/article/60/6/10.1063/1.2754602.

[21] OKUNO, T., *et al. MFM study of magnetic vortex cores in circular permalloy dots: behavior in external field.* Journal of Magnetism and Magnetic Materials. 2002, vol.

240, 1-3. DOI: 10.1016/S0304-8853(01)00708-9. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0304885301007089.

[22] LIU, J., *et al. Theoretical Methods of Domain Structures in Ultrathin Ferroelectric Films: A Review.* Materials. 2014, vol. 7, issue 9, s. 6502–6568. DOI: 10.3390/ma7096502. Dostupné z: http://www.mdpi.com/1996-1944/7/9/6502/.

[23] BOHLENS, S., *et al. Current controlled random-access memory based on magnetic vortex handedness.* Applied Physics Letters. 2008, vol. 93, issue 14. 3 s. DOI: 10.1063/1.2998584. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/93/14/10.1063/1.2998584.

[24] MIYATA, M., *et al. Control of vortex chirality in polygonal nanomagnets.* In: TENCON 2010 – 2010 IEEE Region 10 Conference. 2010, IEEE, s. 1878–1880. DOI: 10.1109/TENCON.2010.5686386. ISBN 978-1-4244-6889-8. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5686386.

[25] CHOE, S.-B., *et al. Vortex Core-Driven Magnetization Dynamics.* Science. 2004, vol. 304, issue 5669, s. 420–422. DOI: 10.1126/science.1095068. Dostupné z: http://www.sciencemag.org/content/304/5669/420.short.

[26] VAN WAEYENBERGE, B., *et al. Magnetic vortex core reversal by excitation with short bursts of an alternating field.* Nature. 2006-11-23, vol. 444, issue 7118, s. 461–464. DOI: 10.1038/nature05240. Dostupné z: http://www.nature.com/doifinder/10.1038/nature05240.

[27] ANTOŠ, R., M. URBÁNEK a Y. OTANI. *Controlling spin vortex states in magnetic nanodisks by magnetic field pulses.* Journal of Physics: Conference Series. 2010, vol. 200, issue 4. 4 s. DOI: 10.1088/1742-6596/200/4/042002. Dostupné z: http://stacks.iop.org/1742-6596/200/i=4/a=042002?key=crossref.fee1676098536936f262cd6b2f654163.

[28] UHLÍŘ, V., *et al. Dynamic switching of the spin circulation in tapered magnetic nanodisks.* Nature Nanotechnology. 2013, vol. 8, issue 5, s. 341–346. DOI: 10.1038/nnano.2013.66. Dostupné z: http://www.nature.com/doifinder/10.1038/nnano.2013.66.

[29] GLIGA, S., R. HERTEL a C.M. SCHNEIDER. *Flipping magnetic vortex cores on the picosecond time scale.* Physica B: Condensed Matter. 2008, vol. 403, 2–3, s. 334–337. DOI: 10.1016/j.physb.2007.08.043. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0921452607005832.

[30] HERTEL, R., *et al. Ultrafast Nanomagnetic Toggle Switching of Vortex Cores.* Physical Review Letters. 2007, vol. 98, issue 11. 4 s. DOI: 10.1103/PhysRevLett.98.117201. Dostupné z: http://link.aps.org/doi/10.1103/PhysRevLett.98.117201.

[31] YAKATA, S., *et al. Chirality control of magnetic vortex in a square Py dot using current-induced Oersted field.* Applied Physics Letters. 2011, vol. 99, issue 24. 4 s. DOI: 10.1063/1.3669410. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/99/24/10.1063/1.3669410.

[32] CHOU, K. W., *et al. Direct observation of the vortex core magnetization and its dynamics.* Applied Physics Letters. 2007, vol. 90, issue 20. 3 s. DOI: 10.1063/1.2738186. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/90/20/10.1063/1.2738186.

[33] TOSCANO, D., *et al. Magnetic vortex behavior and its dynamics in nanomagnets in the presence of impurities.* Physics Procedia. 2012, vol. 28, s. 99–104. DOI: 10.1016/j.phpro.2012.03.679. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1875389212011637.

[34] VAVASSORI, P., *et al. Magnetoresistance of single magnetic vortices.* Applied Physics Letters. 2005, vol. 86, issue 7. s. DOI: 10.1063/1.1866212. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/86/7/10.1063/1.1866212.

[35] CUI, X., S. HU a T. KIMURA. *Detection of a vortex nucleation position in a circular ferromagnet using asymmetrically configured electrodes.* Applied Physics Letters. 2014, vol. 105(8), 082403, 4 s. DOI: 10.1063/1.4894216. ISSN 0003-6951. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/105/8/10.1063/1.4894216.

[36] NAKANO, K., *et al. Real-time observation of electrical vortex core switching.* Applied Physics Letters. 2013, vol. 102, issue 7. 3 s. DOI: 10.1063/1.4793212. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/102/7/10.1063/1.4793212.

[37] BINNIG, G., C. F. QUATE, a Ch. GERBER. *Atomic Force Microscope.* Physical Review Letters. 1986, vol. 56, issue 9, s. 930–933. DOI: 10.1103/PhysRevLett.56.930. Dostupné z: http://link.aps.org/doi/10.1103/PhysRevLett.56.930.

[38] MARTIN, Y. a H. K. WICKRAMASINGHE. *Magnetic imaging by "force microscopy" with 1000 A resolution.* Applied Physics Letters. 1987, vol. 50(20), s. 1455–1457. DOI: 10.1063/1.97800. ISSN 00036951. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/50/20/10.1063/1.97800.

[39] SHINJO, T., *et al. Magnetic vortex core observation in circular dots of permalloy.* Science. 2000, vol. 289, issue 5481, s. 930–932. DOI: 10.1126/science.289.5481.930. Dostupné z: http://www.sciencemag.org/cgi/doi/10.1126/science.289.5481.930.

[40] SHIGETO, K., *et al. Magnetic force microscopy observation of antivortex core with perpendicular magnetization in patterned thin film of permalloy.* Applied Physics Letters. 2002, vol. 80, issue 22, s. 4190–4192. DOI: 10.1063/1.1483386. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/80/22/10.1063/1.1483386.

[41] MIRONOV, V.L.,*et al. MFM probe control of magnetic vortex chirality in elliptical Co nanoparticles.* Journal of Magnetism and Magnetic Materials. 2007, vol. 312, issue 1, s. 153–157. DOI: 10.1016/j.jmmm.2006.09.032. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0304885306011048.

[42] WACHOWIAK, A., *et al. Direct Observation of Internal Spin Structure of Magnetic Vortex Cores.* Science. 2002, vol. 298, issue 5593, s. 577–580. DOI: 10.1126/science.1075302. Dostupné z: http://www.sciencemag.org/content/298/5593/577.

[43] NOVOSAD, V., *et al. Shape effect on magnetization reversal in chains of interacting ferromagnetic elements.* Applied Physics Letters. 2003, 82(21), s. 3716-3718. DOI: 10.1063/1.1577808. ISSN 00036951. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/82/21/10.1063/1.1577808.

[44] KIRK, K. J., J. N. CHAPMAN a C. D. W. WILKINSON. *Switching fields and magnetostatic interactions of thin film magnetic nanoelements.* Applied Physics Letters. 1997, vol. 71, issue 4, s. 539–541. DOI: 10.1063/1.119602. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/71/4/10.1063/1.119602.

[45] RAABE, J., *et al. Magnetization pattern of ferromagnetic nanodisks.* Journal of Applied Physics. 2000, vol. 88, issue 7, s. 4437–4439. DOI: 10.1063/1.1289216. Dostupné z: http://scitation.aip.org/content/aip/journal/jap/88/7/10.1063/1.1289216.

[46] CHUNG, S.-H., D.T. PIERCE a J. UNGURIS. *Simultaneous measurement of magnetic vortex polarity and chirality using scanning electron microscopy with polarization analysis (SEMPA).* Ultramicroscopy. 2010, vol. 110, issue 3, s. 177–181. DOI: 10.1016/j.ultramic.2009.11.002. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0304399109002459.

[47] FISCHER, P. *Exploring nanoscale magnetism in advanced materials with polarized X-rays.* Materials Science and Engineering: R: Reports. 2011, vol. 72, issue 5, s. 81–95. DOI: 10.1016/j.mser.2011.03.002. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0927796X11000143.

[48] PIGEAU, B., *et al. A frequency-controlled magnetic vortex memory.* Applied Physics Letters. 2010, vol. 96, issue 13. 3 s. DOI: 10.1063/1.3373833. Dostupné z: http://scitation.aip.org/content/aip/journal/apl/96/13/10.1063/1.3373833.

[49] BALAJKA, J. *Přepínání chirality vortexů v magnetostaticky svázaných permalloyových nanodiscích.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2013. 53 s. Vedoucí diplomové práce Ing. Michal Urbánek, Ph.D.

[50] CAMBEL, V., *et al. The influence of shape anisotropy on vortex nucleation in Pac-man-like nanomagnets.* Journal of Magnetism and Magnetic Materials. 2013, vol. 336, s. 29–36. DOI: 10.1016/j.jmmm.2013.01.042. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0304885313000693.

[51] COWBURN, R. P. *Spintronics: Change of direction.* Nature Materials. 2007, vol. 6, issue 4, s. 255–256. DOI: 10.1038/nmat1877. Dostupné z: http://www.nature.com/doifinder/10.1038/nmat1877.

[52] FLORESCU, I. a C. TUDOR. Handbook of probability. Wiley. 1. vydání. 2013, 449 s. ISBN 978-0-470-64727-1.

[53] HELLEKALEK, P. *Good random number generators are (not so) easy to find.* Mathematics and Computers in Simulation. 1998, vol. 46, 5–6, s. 485–505. DOI: 10.1016/s0378-4754(98)00078-0. Dostupné z: http://dl.acm.org/citation.cfm?id=284161.

[54] FAIRHEAD, Harry. *ERNIE - A Random Number Generator.* I programmer [online]. 2013 [cit. 2015–02–18]. Dostupné z: http://www.i-programmer.info/history/machines/6317-ernie-a-random-number-generator.html.

[55] METROPOLIS, N. a S. ULAM. *The Monte Carlo Method.* Journal of the American Statistical Association. 1949, vol. 44, issue 247, s. 335–341. DOI: 10.1080/01621459.1949.10483310. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/01621459.1949.10483310.

[56] VIRIUS, M. *Metoda Monte Carlo.* 1. vydání. Praha: České vysoké učení technické, 2010, 233 s. ISBN 978-800-1045-954.

[57] BAUM, G., *et al. Monte Carlo studies of the COMPASS RICH 1 optical properties.* Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment. 1999, vol. 433, 1–2, s. 401–405. DOI: 10.1016/s0168-9002(99)00299-5. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0168900299002995.

[58] KAHN, D. *The codebreakers.* Sphere Books edition, reprinted. London: Sphere Books, 1977, 476 s. ISBN 07-221-5149-7.

[59] SINGH, S. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* Praha: Dokořán, 2003, 382 s. ISBN 80-865-6918-7.

[60] DIFFIE, W. a M. HELLMAN. *New directions in cryptography.* IEEE Transactions on Information Theory. 1976, vol. 22, issue 6, s. 644–654. DOI: 10.1109/TIT.1976.1055638. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1055638.

[61] RIVEST, R. L., A. SHAMIR a L. ADLEMAN. *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM. 1983, vol. 21, issue 2, s. 120–126. DOI: 10.1145/357980.358017. Dostupné z: http://portal.acm.org/citation.cfm?doid=357980.358017.

[62] ELGAMAL, T. *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory. 1985, vol. 31, issue 4, s. 469–472. DOI: 10.1109/TIT.1985.1057074. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1057074.

[63] BENNETT, C. H., *et al. Experimental quantum cryptography.* Journal of Cryptology. 1992, 5(1). 26 s. DOI: 10.1007/BF00191318. ISSN 0933-2790. Dostupné z: http://link.springer.com/10.1007/BF00191318.

[64] BURDA, K. *Aplikovaná kryptografie.* 1. vydání. Brno: VUTIUM, 2013, 255 s. ISBN 978-80-241-4612-0.

[65] KALÁNEK, J. *Praktická realizace generátoru šumu.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 38 s. Vedoucí diplomové práce Ing. Radek Kubásek, Ph.D.

[66] CHEN, I-T. *Random Numbers Generated from Audio and Video Sources.* Mathematical Problems in Engineering [online]. 2013, vol. 2013, s. 1–7. [cit. 2015–01–29]. DOI: 10.1155/2013/285373. Dostupné z: http://www.hindawi.com/journals/mpe/2013/285373/.

[67] ID Quantique. [online]. [cit. 2015–01–28]. Dostupné z: http://www.idquantique.com/.

[68] Lavarand. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001– [cit. 2015–01–28]. Dostupné z: http://en.wikipedia.org/wiki/Lavarand.

[69] BOUDA, J., *et al. Towards True Random Number Generation in Mobile Environments.* In: LNCS 5838, Identity and Privacy in the Internet Age. 5838/2009. Berlin: Springer, 2009. s. 179–189, 12 s. ISBN 978-3-642-04765-7. doi:10.1007/978-3-642-04766-4_13. Dostupné z: http://link.springer.com/10.1007/978-3-642-04766-4_13.

[70] KOZÁK, Š. *True Random Number Generator Output Postprocessing.* Brno: Masarykova univerzita, Fakulta informatiky, 2010. 37 s. Vedoucí bakalářské práce RNDr. Jan Bouda, Ph.D.

[71] WETZEL, C. *Can You Behave Randomly?.* [online]. 1998 [cit. 2015–01–28]. Dostupné z: http://faculty.rhodes.edu/wetzel/random/intro.html.

[72] KAKA, S., *et al. Spin transfer switching of spin valve nanopillars using nanosecond pulsed currents.* Journal of Magnetism and Magnetic Materials. 2005, vol. 286, s. 375–380. DOI: 10.1016/j.jmmm.2004.09.095. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S030488530401011X.

[73] KNUTH, D. E. *Umění programování. 2. díl – Seminumerické algoritmy.* 1. vydání. Brno: Computer Press, 2010, xi, 763 s. ISBN 978-80-251-2898-5.

[74] MACLAREN, M. D. a G. MARSAGLIA. *Uniform Random Number Generators.* Journal of the ACM. 1965, 12(1), s. 83–89. DOI: 10.1145/321250.321257. ISSN 00045411. Dostupné z: http://portal.acm.org/citation.cfm?doid=321250.321257.

[75] MARSAGLIA, G. a A. ZAMAN. *A New Class of Random Number Generators.* The Annals of Applied Probability. 1991, vol. 1, issue 3, s. 462–480. DOI: 10.1214/aoap/1177005878. Dostupné z: http://projecteuclid.org/euclid.aoap/1177005878.

[76] TREVISAN, L. *Extractors and pseudorandom generators.* Journal of the ACM. 2001, vol. 48, issue 4, s. 860–879. DOI: 10.1145/502090.502099. Dostupné z: http://portal.acm.org/citation.cfm?doid=502090.502099.

[77] VAZIRANI, U.V. a V.V. VAZIRANI. *Efficient And Secure Pseudo-Random Number Generation.* In: 25th Annual Symposium onFoundations of Computer Science, 1984. IEEE, 1984, s. 458–463. ISBN 0-8186-0591-x. DOI: 10.1109/SFCS.1984.715948. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=715948.

[78] MARSAGLIA, G. *The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness.* [online]. 1995 [cit. 2015–01–25]. Dostupné z: http://www.stat.fsu.edu/pub/diehard/.

[79] MASCAGNI, M. a A. SRINIVASAN. *Algorithm 806: SPRNG: a scalable library for pseudorandom number generation.* ACM Transactions on Mathematical Software. 2000, vol. 26, issue 3, s. 436–461. DOI: 10.1145/358407.358427. Dostupné z: http://portal.acm.org/citation.cfm?doid=358407.358427.

[80] L'ECUYER, P. a R. SIMARD. *TestU01: A C Library for Empirical Testing of Random Number Generators.* ACM Transactions on Mathematical Software. 2007, vol. 33, issue 4, 40 s. DOI: 10.1145/1268776.1268777. Dostupné z: http://ftp.genotec.ch/pub/FreeBSD/distfiles/testu01.pdf.

[81] Standards. National Institute of Standards and Technology. [online]. 1996, aktualizováno 2014 [cit. 2015–05–19]. Dostupné z: http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[82] WALKER, J. *ENT. A Pseudorandom Number Sequence Test Program.* [online]. 2008 [cit. 2015–05–18]. Dostupné z: http://www.fourmilab.ch/random/.

[83] SNOUFFER, R., LEE, A. a OLDEHOEFT, A. *NIST special publicaton 800-29: A comparison of the security requirements for cryptographic modules in FIPS 140-1 and FIPS 140-2.* National Institute of Standards and Technology. [online]. 2001 [cit. 2015–05–19]. Dostupné z http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf.

[84] Public-Key Cryptography Standards (PKCS). RSA Laboratories [online]. 2015 [cit. 2015–05–19]. Dostupné z: http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm.

[85] Laboratoře odboru povrchů a pevných látek. [online]. [cit. 2014–03–25]. Dostupné z: http://physics.fme.vutbr.cz/ufi.php?Action=0&Id=1422.

[86] Laboratoř přípravy a charakterizace nanostruktur. Středoevropský technologický institut. [online]. 2013 [cit. 2015–05–13]. Dostupné z: http://www.ceitec.cz/ceitec-vut/laborator-pripravy-a-charakterizace-nanostruktur/z1.

[87] HELLSTROM, S. L. *Basic Models of Spin Coating: Submitted as coursework for Physics 210, Stanford University, Autumn 2007.* [online]. 2007 [cit. 2015–01–19]. Dostupné z: http://large.stanford.edu/courses/2007/ph210/hellstrom1/.

[88] PAVERA, M. *Automatizace a řízení depozice multivrstev metodou IBS/IBAD.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011. 89 s. Vedoucí diplomové práce Ing. Michal Urbánek, Ph.D.

Seznam použitých zkratek a symbolů

a	násobitel
A	plocha
B	magnetická indukce
$\vec{B}_{\mathrm{pulz}}$	střídavé magnetické pole
c	cirkulace magnetizace
C	koeficient sériové korelace
c_{LCG}	inkrement lineárního kongruenčního generátoru
d	průměr
e	náboj elektronu
$F()$	distribuční funkce
$f(i)$	výskyt různých kombinací při pokerovém testu
$F_{\mathrm{n}}()$	empirická distribuční funkce
$\hbar$	redukovaná Planckova konstanta
$\vec{H}_{\mathrm{A}}$	anihilační intenzita magnetického pole
$\vec{H}_{\mathrm{EXT}}$	intenzita vnějšího magnetického pole
$\vec{H}_{\mathrm{N}}$	nukleační intenzita vnějšího magnetického pole
I	elektrický proud
$\vec{I}_{\mathrm{pulz}}$	střídavý elektrický proud
$\vec{j}$	proudová hustota
$\vec{J}$	celkový elektronový moment hybnosti
l	orbitální kvantové číslo
L	velikost orbitálního momentu hybnosti
$\vec{L}$	orbitální moment hybnosti
$\vec{M}$	magnetizace
m_{e}	hmotnost elektronu
m_{l}	magnetické orbitální číslo

m_s	magnetické spinové číslo
M_s	magnetizace v saturovaném stavu
n	přirozené číslo
n_q	hlavní kvantové číslo
p	polarita jádra
r_1	odpor části feromagnetického disku
r_2	odpor části feromagnetického disku
R_MTJ	odpor magnetického tunelového přechodu
s	spinové kvantové číslo
S	velikost spinového momentu hybnosti
$\vec{S}$	spinový moment hybnosti
t	tloušťka vrstvy
T	teplota
V	objem
X	náhodné číslo, veličina
Y	rozhodující parametr pro vybrané statistické testy
$\overline{x}$	aritmetický průměr hodnoty bytu
Z	atomové číslo
γ	gyromagnetický poměr
$\vec{\mu}$	magnetický moment
μ_B	Bohrův magneton
μ_e	magnetický moment elektronu
$\vec{\mu}_\mathrm{orb}$	orbitální magnetický moment
$\mu_\mathrm{orb,z}$	z-složka orbitálního magnetického momentu
μ_p	magnetický moment protonu
$\vec{\mu}_\mathrm{s}$	spinový magnetický moment
$\mu_\mathrm{s,z}$	z-složka spinového magnetického momentu
ρ	anizotropní magnetorezistivita

$\rho_{\parallel}$	rezistivita při paralelních směrech $\vec{M}$ a $\vec{j}$
$\rho_{\perp}$	rezistivita při kolmých směrech $\vec{M}$ a $\vec{j}$
φ	úhel svíraný $\vec{M}$ a $\vec{j}$
χ	magnetická susceptibilita
AFM	mikroskopie atomových sil (atomic force microscopy)
AMR	anizotropní magnetorezistivita (anisotropic magnetoresistivity)
AWC	součet s přenosem (add with carry)
CEITEC	Středoevropský technologický institut (Central European institue of technology)
CERN	Evorpská rada pro jaderný výzkum (Conseil Européen pour la Recherche Nucléaire)
COMPASS	Společné mionové a protonové zařízení pro zkoumání struktury a spektroskopii (Common muon and proton apparatus for structure and spectroscopy)
CW	po směru hodinových ručiček (clockwise)
CCW	proti směru hodinových ručiček (counter clockwise)
EBL	elektronová litografie (electron beam litography)
ERNIE	elektronické zařízení pro oznamování náhodných čísel (Electronic random number indicator equipment)
FIB	fokusovaný iontový svazek (focused ion beam)
FIPS	standard federálního zpracování informací (Federal information processing standard)
GPS	globální polohovací systém (Global positioning system)
GSFR	obecný registr se zpětnou vazbou (generalized feedback shift register)
IBAD	depozice s asistencí iontového svazku (ion beam assisted deposition)
IBS	depozice iontovým svazkem (ion beam sputtering)
IPA	isopropylalkohol
KS	Kolmogorovův-Smirnovův (test)
LCG	lineární kongruenční generátor (linear congruent generator)
LFG	zpožděný Fibonacciho generátor (lagged Fibonacci generator)

LSFR	lineární posuvný registr se zpětnou vazbou (linear feedback shift register
MFM	mikroskopie magnetických sil (magnetic force microscopy)
MIBK	methylisobutylketon
MOKE	magnetooptický Kerrův jev (magneto-optical Kerr effect)
MTJ	magnetický tunelový přechod
MTXM	magnetická transmisní rentgenová mikroskopie (magnetic transmission X-ray microscopy)
NIST	Národní institut standardů a technologie (National institute of standards and technology)
PBRT	testy náhodnosti založené na fyzikálních jevech (physically based randomness tests)
PKCS	Standardy pro kryptografii s veřejným klíčem (Public-key cryptography standards)
PMMA	polymethylmethakrylát
PRNG	generátor pseudonáhodných čísel (pseudorandom number generator)
SEMPA	rastrovací elektronová mikroskopie se spinově polarizovanou detekcí sekundárních elektronů (scanning electron microscopy with polarization analysis)
SPM	mikroskopie rastrovací sondou (scanning probe microscopy)
SP	spinově polarizovaný (spin-polarized)
SPS	Super proton synchrotron
SR	prostorově rozlišený (space resolved)
STEM	rastrovací transmisní elektronová mikroskopie (scanning transmission electron microscopy)
STM	rastrovací tunelová mikroskopie (scanning tunnelling microscopy)
STXM	rastrovací transmisní rentgenová mikroskopie (scanning transmission X-ray microscopy)
SWB	rozdíl s výpůčkou (substract with borrow)
TR	časově rozlišený (time resolved)
TRNG	generátor skutečně náhodných čísel (true random number generator)
USB	univerzální sériová sběrnice (universal serial bus)

X-MCD	rentgenový magnetický cirkulární dichroismus (X-ray magnetic circular dichroism)
X-MLD	rentgenový magnetický lineární dichroismus (X-ray magnetic linear dichroism)
X-PEEM	rentgenová fotoelektronová emisní mikroskopie (X-ray photo-electron emission microscopy)