UNIVERZITA PALACKÉHO V OLOMOUCI

Přírodovědecká fakulta

Společná Laboratoř Optiky UP a FZÚ AV ČR

Kvantové kopírování

Mgr. Antonín Černoch, Ph.D.

Habilitační práce

Olomouc 2023

Poděkování

Jako experimentátor musím poděkovat teoretikům za to, že dokáží upravit své výpočty tak, aby odpovídaly naměřeným hodnotám.

Tonik Černoch

Prohlášení o původu

Tímto prohlašuji, že jsem jediným autorem této práce, která dle mého nejlepšího vědomí a svědomí neobsahuje materiály někoho jiného bez uvedení náležité citace.

V Olomouci dne

Mgr. Antonín Černoch, Ph.D.

Autor uděluje povolení Univerzitě Palackého v Olomouci ukládat a prezentovat tuto práci a její elektronickou verzi v univerzitní knihovně a na oficiálních webových stránkách.

Obsah

Předmluva

Ačkoliv je nějaká teorie známa už delší dobu, experiment, potvrzující její pravdivost, musí většinou počkat, dokud se nevyvine potřebná technologie. Nejinak to bylo i v případě kvantové mechaniky resp. kvantové informatiky. V případě druhé jmenované bylo nejdřív potřeba sestrojit *LASER*, pomocí něj studovat nelineární procesy a pomocí jednoho z nich, spontánní parametrické sestupné konverze (*SPDC – Spontaneous Parametric Down-Conversion*), generovat ideální nosiče kvantové informace – fotony.

Jednotlivé fotony (kvanta elektromagnetického záření) jsou nejlepším možným nosičem kvantové informace na velké vzdálenosti. Pohybují se nejvyšší možnou rychlostí, mají akceptovatelné ztráty a málo interagují s prostředím, nemění tedy příliš svůj kvantový stav. Na druhou stranu, pokud se nějaký narušitel pokusí zjistit kvantový stav těchto fotonů, nepovede se mu to bez toho, aniž by kvantový stav fotonů pozměnil. To se dá využít při **kvantové kryptografii**, tj. bezpečném přenosu klasické informace pomocí kvantových stavů.

Druhým hlavním využitím kvantové informatiky je tzv. **kvantové počítání**. Zde se využívá paralelní interakce kvantových stavů, která vede k výraznému zkrácení výpočetního času oproti známým klasickým algoritmům. Efektivní zpracování kvantové informace může být realizováno pomocí různých fyzikálních platforem, například iontů a atomů v pasti, jaderné magnetické rezonance, kvantových teček a supravodivých obvodů. Přehled a porovnání různých metod lze najít například v přehledové práci Ladda a kol. [1]. Využití fotonů pro kvantové počítání není vhodné, protože spolu vzájemně neinteragují kromě dvou případů: interakce v nelineárním médiu nebo pomocí interference na děliči svazku. Obojí má ale omezenou účinnost.

Už teď je jasné, že složitějším kvantovým výpočtům budou vévodit supravodivé obvody a přenosu informace pro změnu jednotlivé fotony. Je ale otázkou dalšího technologického vývoje, zda pro jednoduché kvantové zpracování informace během přenosu bude efektivní převádět kvantovou informaci z fotonů na jinou platformu.

Spolu s kolegy se ve Společné laboratoři optiky zabýváme experimenty ověřující základní principy kvantové mechaniky popřípadě konstruujeme prototypy kvantově informačních hradel. Tato práce je věnovaná různým experimentálním realizacím kvantového klonování. Důvodů k výběru tohoto tématu je několik. Jednak se dá klonovaní zahrnout do obou výše jmenovaných kategorií. Publikovali jsme na toto téma od roku 2006 do současnosti téměř tucet článků [A1–A11]. Klonování coby optimální útok na kvantovou kryptografii je stále aktuální s ohledem na celosvětovou snahu postupně vybudovat nadnárodní komunikační sítě na bázi kvantové kryptografie. Nicméně hlavním důvodem je to, že na jednom tématu můžeme ukázat, jak se během let zdokonalovala konstrukce experimentu.

Kapitola 1

Kvantová informace s využitím optiky

Jak již bylo napsáno v předmluvě, kvantovou informatiku lze implementovat na různých platformách. V naší laboratoři jsme se zaměřili na optická zařízení z jednoho prostého důvodu – využili jsme stávající zařízení a *know-how*. Přeorientování na jinou platformu vhodnější například pro kvantové počítání by bylo nereálné s ohledem na naše stávající vybavení, zkušenosti a v neposlední řadě i finanční možnosti.

Stejně tak se může diskutovat o tom, jaké je nejvýhodnější kódovaní informace do fotonů. Jednou z možností je zapsat kvantovou informaci do x a p kvadratur, tedy do tzv. spojitých proměnných [2]. Další možností je využít diskrétní povahu jednotlivých fotonů (Fockova reprezentace [3]). V této kapitole shrnu základní vlastnosti kvantové informace, která jsou společné všem platformám. Zaměřím se nicméně na metody, které jsme používali my, tedy polarizační a dráhové kódování kvantové informace do jednotlivých fotonů. Tento způsob byl pro nás experimentálně nejvýhodnější. Navíc se ukazuje, že pro přenos kvantové informace na delší vzdálenosti budou potřeba tzv. opakovače (*repeatery*), ty jsou nyní většinou na principu polarizačně kvantově provázaných fotonových párů a jsou tedy kompatibilní s naším vybavením.

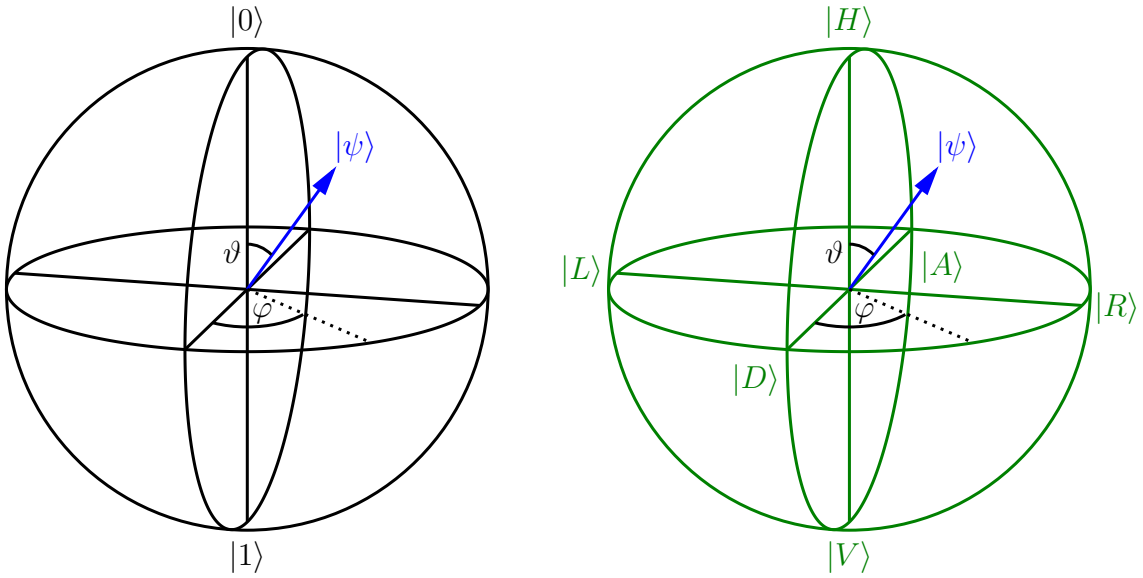
1.1 Qubit

Kvantový stav ve dvoudimenzionálním Hilbertově prostoru lze popsat pomocí kvantového bitu, zkráceně **qubitu** [4, 5]. Qubit je matematický objekt, který můžeme realizovat pomocí fyzikálních vlastností jednotlivých částic. Pro značení kvantového stavu používáme Diracovu braketovou symboliku, kde tzv. ket $|\cdot\rangle$ značí vektor v Hilbertově prostoru.

Obdobně jako u klasické binární informace, kde má bit hodnotu **0** nebo **1**, tak i kvantový bit může být ve stavu $|0\rangle$ resp. $|1\rangle$. Tyto dva stavy definují ortonormální bázi v Hilbertově prostoru. Na rozdíl od klasické informace může být qubit i v jakékoliv superpozici těchto bázových stavů,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1. \tag{1.1}$$

Komplexní koeficienty α a β určují pravděpodobnost, s jakou bychom při měření kvantového stavu získali výsledek $|0\rangle$ (s pravděpodobností $|\alpha|^2$) resp. $|1\rangle$ (s pravděpodobností $|\beta|^2$).



Obrázek 1.1: Vlevo grafické znázornění kvantového bitu pomocí Blochovy sféry, vpravo polarizačního stavu pomocí Poincarého sféry.

Do jednoho kvantového stavu lze teoreticky zakódovat nekonečné množství klasické informace. Koeficienty α a β jsou komplexní čísla s nekonečným počtem desetinných míst, přičemž každé z těchto míst může popisovat jeden klasický bit. Nicméně pokud chceme změřit komplexní koeficienty α a β, musíme provést projekční měření. Výsledkem tohoto měření je buď stav $|0\rangle$ a nebo stav $|1\rangle$. Stav původního qubitu se měřením změní, „vyprojektuje“ se do jednoho z bázových stavů. Pokud provedeme mnoho měření na stejně připravených qubitech, změřený qubit už použít nelze, můžeme určit pravděpodobnosti $|\alpha|^2$ a $|\beta|^2$ s dostatečnou přesností. Nakonec dojdeme k závěru, že jedním projekčním měřením určíme z kvantového stavu pouze jeden klasický bit informace.

Kvantový bit lze graficky vizualizovat pomocí Blochovy sféry (viz obr. 1.1a). Všechny možné čisté stavy leží na povrchu této sféry. Na pólech jsou bázové stavy. Komplexní koeficienty α a β lze zapsat pomocí Eulerových úhlů,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{\imath\varphi}\sin\frac{\vartheta}{2}|1\rangle, \qquad \vartheta \in [0,\pi], \varphi \in [0,2\pi]. \tag{1.2}$$

Obdobným způsobem, tedy pomocí Poincarého sféry, lze popsat úplně polarizované stavy světla, viz obr. 1.1b. Využití polarizačního stavu jednotlivých fotonů je tedy přímočarou volbou pro realizaci kvantových bitů.

Pro popis obecných kvantových stavů je potřeba zavést matici hustoty, ve 2D prostoru se jedná o 2×2 komplexní matici

$$\hat{\rho} \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{1.3}$$

Matice hustoty popisuje jak čisté stavy $|\psi\rangle$, kdy $\hat{\rho} = |\psi\rangle\langle\psi|$ a platí rovnost $\mathrm{Tr}(\hat{\rho}^2) = 1$, tak smíšené stavy, pro ně je $\mathrm{Tr}(\hat{\rho}^2) < 1$. Diagonální členy matice hustoty se rovnají pravděpodobnostem $|\alpha|^2$ resp. $|\beta|^2$, jelikož je součet pravděpodobností všech možných výsledků měření jednotkový, je $\mathrm{Tr}(\hat{\rho}) = 1$.

1.2 Generace jednotlivých fotonů

Je mnoho způsobů, jak generovat jednotlivé fotony. Pouze zeslabení laserového svazku není ve většině případů vhodné, protože si signál zachovává svou fotodistribuční statistiku. Pořád existuje nenulová pravděpodobnost vícefotonového pulzu, když se tuto pravděpodobnost budeme snažit minimalizovat, nevyhnutelně zvětšíme pravděpodobnost vakua (žádný foton). Dále můžeme použít zdroje na bázi kvantových teček [6], volných atomů [7] nebo atomů zachycených v rezonátoru [8]. Všechny tyto zdroje mají své výhody a nevýhody. Pokud ale budeme požadovat naprostou nerozlišitelnost dvou fotonů, která je potřebná pro dvoufotonovou Hongovu-Ouovu-Mandelovu (HOM) interferenci [9], zúží se nám spektrum použitelných zdrojů prakticky jen na nelineární proces spontánní sestupné parametrické frekvenční konverze (SPDC).

Při SPDC se v nelineárním médiu jeden čerpací foton s frekvencí ν_p rozpadá na dva fotony označované jako signální (s) a jalový (i). Tyto musí splňovat zákony zachování energie a hybnosti [10],

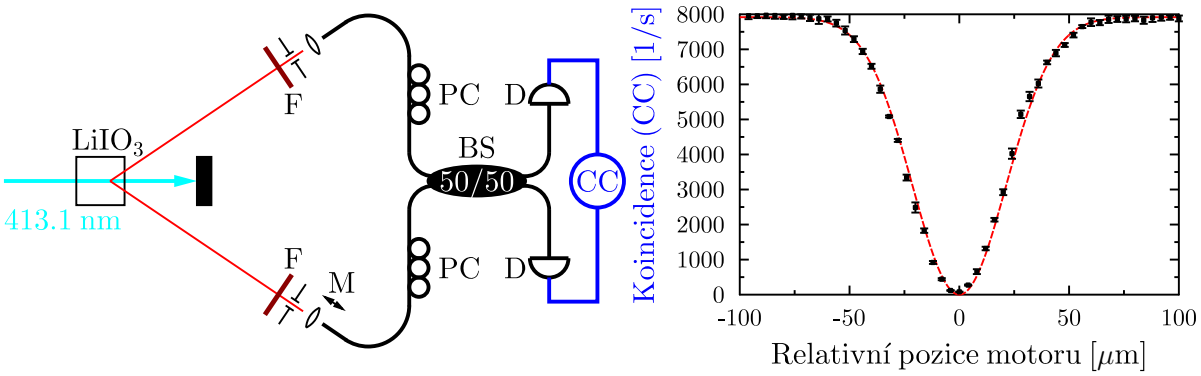
$$h\nu_p = h\nu_s + h\nu_i, \qquad \hbar\vec{k_p} = \hbar\vec{k_s} + \hbar\vec{k_i}. \tag{1.4}$$

Nejlépe jsou schopny interferovat fotony se stejnou frekvencí (resp. spektrálním profilem). Takto degenerované fotonové páry jsou vygenerovány pod úhlem, který odpovídá podmínce fázové synchronizace v daném nelineárním krystalu.

Při realizaci experimentu s jednotlivými fotony je potřeba optimalizovat několik hledisek a nalézt přijatelný kompromis. Předpokládejme, že potřebujeme vygenerovat fotonové páry v blízké infračervené oblasti spektra s vlnovou délkou okolo 800 nm. Tato oblast odpovídá prvnímu informačnímu oknu v optických vláknech (minimum ztrát) a navíc jsou pro tuto spektrální oblast k dostání jednofotonové křemíkové detektory s dostatečnou kvantovou účinností ($\geq 50\,\%$). Na poloviční vlnové délce (okolo 400 nm) tedy potřebujeme čerpat nelineární prostředí. Čerpací laserový svazek musí mít dobré prostorové a spektrální vlastnosti, protože se tyto vlastnosti přenáší i na generované fotony. Čerpání musí být silné (ve smyslu energie), protože nelineární procesy mají malou účinnost díky slabým nelinearitám zatím dostupných prostředí.

V našich experimentech jsme používali spektrální čáru 413 nm kryptonového laseru Innova 302 od firmy Coherent. Výstupní svazek laseru měl dobrý příčný profil, téměř dokonalý základní TEM_{00} mód, a kontinuální výkon typicky 250 mW. Svazek byl fokusován do nelineárního krystalu $LiIO_3$ o tloušťce 10 mm vyrobeného firmou EKSMA. Tento krystal byl vybroušen na Typ I s úhly řezu $\vartheta = 90°$ a $\varphi = 0°$. Při čerpání vertikální polarizací vznikají ve stejný okamžik dva horizontálně polarizované fotony. Fotony se stejnou frekvencí jsou generovány do kuželu s vrcholovým úhlem 34°. Z celého kuželu byly vybrány dvě pozice symetricky vůči směru čerpacího svazku, do kterých byly umístěny navazovače (viz obrázek 1.2 vlevo). Navazovač je mechanicky stavitelný teleskop, který navazuje volně se šířící optický signál do vlákna pomocí asférické čočky. Většinou je osazen hranovým popřípadě úzkopásmovým spektrálním filtrem a nastavitelnou clonou.

V našich experimentech jsme používali jednomodová vlákna. Touto prostorovou filtrací jsme přišli o značnou část signálu, ale zvýšili jsme nerozlišitelnost fotonů z páru s ohledem na prostorový mód, ty tak spolu mohly ideálně interferovat. Míra nerozlišitelnosti (interference) fotonů ze zdroje se ověřovala Hongovou-Ouovou-Mandelovou (HOM) interferencí [9] za pomocí vláknového děliče. Na děliči dochází ke shlukování fotonů, v případě



Obrázek 1.2: Vlevo schéma zdroje časově korelovaných fotonových párů. F – hranový nebo úzkopásmový filtr, M – motorizovaný posuv vláknového navazovače, PC – polarizační kontroler, BS – vláknový dělič, D – jednofotonový detektor. Vpravo naměřený dvoufotonový interferogram, tzv. HOM zářez (dip) v počtu současných detekcí (koincidencí) v závislosti na časovém zpoždění příchodu fotonů na dělič. Dráhové zpoždění je svázáno s časovým pouze rychlostí šíření světla ve volném prostoru.

současného příchodu dvou nerozlišitelných fotonů klesne pravděpodobnost současné detekce (koincidence) na dvou výstupech děliče k nule, protože oba fotony opustí dělič vždy jen jedním výstupem. Pokud je mezi fotony při detekci nějaká rozlišitelnost (například v polarizaci, spektru, prostorovém módu), tak bude pravděpodobnost koincidence vždy nenulová. Pro jednoduchou charakterizaci se používá vizibilita HOM interferogramu, $V = (MAX - min)/(MAX + min)$, kde MAX značí počet koincidencí mimo interferenční oblast (dostatečné dráhové rozposunutí) a min počet koincidencí v případě současného dopadu fotonů na dělič (nulový dráhový rozdíl, viz obr. 1.2 vpravo). Poloha a natočení navazovačů byly optimalizovány tak, aby bylo dosaženo co největší vizibility. Stejně tak se musela upravit polarizace fotonů šířících se vláknem. Ve válcových vláknech se polarizace světla (fotonů) mění s každou změnou geometrie vlákna (smyčky, kruty) nebo díky generovanému dvojlomu v ohybech. Tyto změny lze kompenzovat pomocí natočení tří smyček v polarizačním kontroleru (PC), které provádí stejnou transformaci polarizace jako trojice $\lambda/4$, $\lambda/2$ a $\lambda/4$ fázových destiček.

1.3 Kódování a přenos informace

Poté, co jsme vygenerovali časově korelované páry fotonů, můžeme do nich zapsat kvantovou informaci. Možností, jak to udělat, je několik [3]. Mimo zde zmíněné kódování do polarizace a dráhy lze například kódovat do času příchodu fotonu (*time bin*) a prostorového módu. Mezi jednotlivými způsoby kódování lze jednoduše a většinou deterministicky přecházet. Některé transformace qubitu jsou experimentálně snáze proveditelné s některým kódováním než s jiným.

1.3.1 Polarizační kódování

Jak je patrné z obrázku 1.1, polarizační stav světla (fotonů) přímo koresponduje s vyjádřením kvantového stavu. Jeden foton s horizontální polarizací ($|H\rangle$) představuje kvantový

bit ve stavu $|0\rangle$, foton s vertikální polarizací ($|V\rangle$) potom qubit $|1\rangle$. Qubit v libovolné superpozici je představován jedním fotonem s obecně eliptickou polarizací.

Problém pro toto kódování představuje pouze šíření ve vláknech nezachovávajících polarizační stav. Tento problém lze ale řešit, protože šíření ve vlákně způsobí jen určitou změnu polarizačního stavu, která může být kompenzována polarizačním kontrolerem. Pokud se ovšem změní geometrie vlákna (například se s vláknem pohne), změní se i jeho polarizační transformace a musí se provést korekce.

Proto je jednodušší využívat polarizační kódování při šíření ve volném prostoru, kde se polarizační stav nemění. Polarizaci fotonů a tedy i jejich kvantový stav lze připravit a měnit pomocí fázových destiček. Ty jsou vyrobeny z dvojlomného materiálu s vhodně volenou tloušťkou tak, že transformují polarizační stav požadovaným způsobem. Fázová $\lambda/2$ destička (HWP) s hlavní osou otočenou o úhel θ vůči horizontální polarizaci transformuje bázové stavy takto,

$$|H\rangle \to \cos 2\theta\,|H\rangle + \sin 2\theta\,|V\rangle, \qquad |V\rangle \to \sin 2\theta\,|H\rangle - \cos 2\theta\,|V\rangle. \tag{1.5}$$

Fázová $\lambda/4$ destička (QWP) otočená o stejný úhel provede tuto transformaci:

$$\begin{aligned} |H\rangle &\to (\cos^2\theta + \imath \sin^2\theta)\,|H\rangle + \sin\theta\cos\theta(1-\imath)\,|V\rangle, \\ |V\rangle &\to \sin\theta\cos\theta(1-\imath)\,|H\rangle + (\sin^2\theta + \imath\cos^2\theta)\,|V\rangle. \end{aligned} \tag{1.6}$$

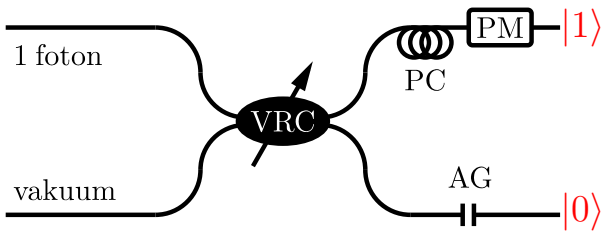
Pomocí kombinace fázových destiček lze připravit z fotonu ze zdroje s danou polarizací jakýkoliv polarizační qubit. Stejně tak lze vhodným natočením destiček provést jakoukoliv (unitární) jednoqubitovou operaci.

Pro měření polarizačních qubitů se používá projekce pomocí polarizátoru. Standardní polarizátor dělí světlo do dvou drah podle jeho polarizačního stavu. Fotony polarizované ve směru roviny dopadu, která je určena směrem šíření fotonu a kolmicí k dělícímu rozhraní, polarizátorem prochází, ortogonálně polarizované fotony se na rozhraní odrážejí. Fotony s obecnou polarizací $\alpha|H\rangle + \beta|V\rangle$ se rozhodují náhodně, s pravděpodobností $|\alpha|^2$ projdou, s pravděpodobností $|\beta|^2$ se odrazí. Zde je už aplikováno naše laboratorní pravidlo, kdy polarizátory v experimentu montujeme tak, aby horizontální složka prošla a vertikální se odrazila.

1.3.2 Dráhové kódování

V případě dráhového kódování je informace o kvantovém stavu zapsaná do dráhy, kterou se foton šíří. Na rozdíl od polarizačního kódování můžeme zvětšit dimenzi prostoru přidáním dalších drah. S pomocí tří drah můžeme zakódovat qutrit, s d drahami obecně qudit. Pro jednoduchost se omezíme 2D Hilbertův prostor. Bázové stavy $|0\rangle$ a $|1\rangle$ odpovídají dvěma rozdílným drahám, kterými se foton může šířit. Díky principu superpozice se může foton šířit i v obou drahách současně. Pro přípravu obecného qubitu je tedy potřeba nastavit dva parametry – pravděpodobnostní poměr detekce fotonu v jedné a druhé dráze a časové (fázové) zpoždění mezi těmito drahami.

Experimentálně lze libovolný dráhový qubit připravit pomocí děliče s proměnným dělicím poměrem a fázovým posuvem. Nastavitelný dělič lze vytvořit pomocí fázové $\lambda/2$ destičky a polarizátoru. Nebo pro libovolnou polarizaci můžeme použít vláknový dělič s proměnným dělícím poměrem VRC (*Variable Ratio Coupler*). Fázový posuv prodlužuje



Obrázek 1.3: Příprava kvantového stavu v případě dráhového kódovaní. VRC – vláknový dělič s proměnným dělicím poměrem, PC – polarizační kontroler, PM – fázový modulátor, AG – vzduchová mezera.

jednu dráhu vůči druhé o zlomky vlnové délky použitých fotonů. V optických vláknech lze použít fázový modulátor (PM), v kterém se vlivem přiloženého napětí mění index lomu optického prostředí. Fázový modulátor pracuje správně jen pro jednu polarizaci, proto je jeho součástí polarizátor a pro minimalizaci ztrát musí být před ním polarizační kontroler (PC). Ve složitějších experimentech využívajících dráhové qubity tvoří zařízení interferometry, v kterých je potřeba vyvážit délky ramen na jednotky mikrometru (v závislosti na koherenční délce používaných fotonů). Jelikož s takovou přesností nelze upravit délky optických vláken, musíme různé délky ramen interferometru kompenzovat pomocí vzduchové mezery (AG). Zde se fotony vyváží z vlákna pomocí čočky do volného prostoru a pomocí další čočky se naváží do druhého vlákna. Délka vzduchové mezery může být kontrolována pomocí motorizovaného posuvu. Pokud je jeden z navazovačů navíc na piezoposuvu, který umožňuje posun s nanometrovou přesností, lze pomocí této modifikované vzduchové mezery ovládat i fázové zpoždění.

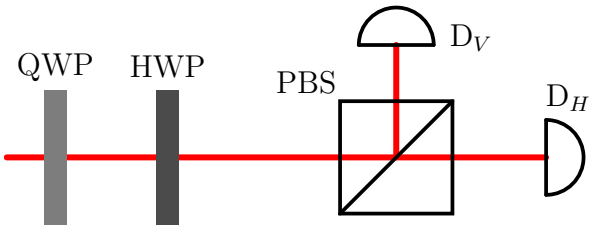
1.4 Měření kvantového stavu

Kvantový stav jednoho neznámého qubitu nelze změřit. Pro určení kvantového stavu musíme provést mnoho projekčních měření v různých bázích na stavech, které jsou připraveny stejným způsobem. V případě qubitu v podobě jednotlivých fotonů musíme mít k dispozici detektory schopné zaregistrovat energie v řádu 10^{-19} J. Pomocí těchto detektorů provádíme projekční měření v různých bázích. Z výsledků měření můžeme určit různé parametry včetně matice hustoty, která plně popisuje kvantový stav.

1.4.1 Jednofotonové detektory a elektronické zpracování

K zaznamenání přítomnosti fotonů můžeme použít jakýkoliv typ detektoru s jednofotonovou účinností, dostatečně velkou kvantovou účinností a opakovací frekvencí a malým počtem temných detekcí (šum). V našich experimentech se používají lavinové fotodetektory SPCM (*single-photon counting modules*) od firmy Excelitas (dříve Perkin Elmer) s typickou kvantovou účinností 55 %, maximální opakovací frekvencí nad 10 MHz a temnými pulzy okolo $100\,\mathrm{s}^{-1}$. Detektory mají vláknové konektory, proto se volně šířící svazek nejdřív naváže do vlákna, které vede signál přímo na střed čipu detektoru.

Tyto detektory nedokáží rozeznat počet fotonů v jednom časovém okamžiku, mají **binární odezvu**. Stejnou odezvu (napěťový TTL pulz) vyvolá jeden i více fotonů. Fotonové detekční události načítáme pomocí modulu *Counter&Timer* (Kortec) a počty za



Obrázek 1.4: Schéma polarizační analýzy. QWP – čtvrtvlnná destička, HWP – půlvlnná destička, PBS – polarizátor, D – detektor.

určitý čas se odesílají do počítače. Počty detekcí jsou zatíženy šumem. Jedná se o již zmíněné temné detekce způsobené termálními excitacemi. Dalším zdrojem je šum pozadí, tedy detekce fotonů z nesledovaných zdrojů (LED kontrolky přístrojů v laboratoři, displej monitoru atd.).

V případě měření stavu dvou fotonových qubitů se může provést **postselekce** na koincidence. Předpokládejme, že máme na vstupu zařízení dva časově korelované qubity. Potom můžeme položit podmínku, že proces v kvantovém zařízení proběhl úspěšně pouze tehdy, je-li na dvou výstupech zařízení současně po jednom fotonu. Tím odfiltrujeme všechny události, kdy se jeden foton z páru ztratil nebo kdy zařízení nezafungovalo správně. Filtraci na současné detekce můžeme provést pomocí speciální koincidenční elektroniky, která zaznamená pouze současné detekce, respektive detekce zaznamenané v malém časovém rozmezí, tzv. koincidenčním okně. Tímto se výsledky měření oprostí od šumových temných detekcí detektorů i nedokonalostí zdroje fotonů, který nedodá na vstup zařízení dva fotony současně a zařízení by tedy nefungovalo správně.

Používáme dva způsoby určení koincidenční události. Koincidenční modul (logika) dokáže zpracovat hned několik koincidenčních událostí z více detektorů. Současnou detekci rozpozná přímým součtem napětí z detektorů – za koincidenci označí případ, pokud součet napětí přesáhne napětí výstupního pulzu jen z jednoho detektoru. Problém nastává u pulzních dějů s velkou opakovací frekvencí. Samotné délky výstupních pulzů z detektoru jsou v řádově 9 až 35 ns (v závislosti na typu), to limituje minimální délku koincidenčního okna. Pokud toto koincidenční okno zahrnuje několik po sobě jdoucích pulzních dějů, nevyhnutelně vzroste počet chybně vyhodnocených koincidencí.

Druhou možností je využít kombinace modulů TAC (*Time to Amplitude Converter*) a SCA (*Single Channel Analyzer*) obojí od výrobce Kortec. Tyto dva moduly jsou schopny zpracovávat pouze signál ze dvou detektorů a hlásit pouze jednu současnou detekci. Nicméně k určení koincidence využívají pouze náběžné hrany pulzů z detektorů, koincidenční okno muže být tedy nastaveno na zlomek nanosekundy.

1.4.2 Polarizační analýza

Určení kvantového stavu si vysvětlíme na polarizaci fotonu. Tzv. detekční blok se skládá z fázových destiček (čtvrtvlnné a půlvlnné), polarizátoru a jednoho nebo dvou detektorů (obr. 1.4). Použité komponenty musí být samozřejmě optimalizované na vlnovou délku fotonů.

V závislosti na tom, co hodláme měřit, akumulujeme detekce pro několik projekcí. Různé projekce se nastavují pomocí fázových destiček. Například pro projekci na H a

V polarizaci nám stačí pouze polarizátor s dělícím rozhraním kolmo na horizontální rovinu. Fázové destičky jsou nastavené na nulu, to znamená, že jejich hlavní osy koincidují s natočením polarizátoru. V případě projekce na diagonální polarizaci musí být QWP otočená o 45° a HWP o 22.5°. Pro projekci na kruhovou polarizaci musí být HWP natočená o 22.5° a QWP zůstává na nule.

Pro jedno projekční nastavení se po určitou dobu akumulují detekční události. Doba měření se nastavuje podle průměrného počtu detekcí tak, aby se minimalizovala neurčitost měření a celkový čas měření nebyl zase neúměrně dlouhý. Směrodatná odchylka počtu detekcí je dána odmocninou tohoto počtu, tedy čím je počet detekcí větší, tím je relativní neurčitost měření menší.

V případě, že využijeme obou výstupů z polarizátoru, můžeme provést měření dvakrát rychleji, protože získáme hodnotu detekcí pro nastavenou projekci a z druhého detektoru počet detekcí pro kolmou projekci. Nevýhodou je, že musíme mít více detektorů a že musíme provést kompenzaci na rozdílné účinnosti jak samotných detektorů tak účinnosti navázání do optického vlákna. V prvních experimentech jsme tuto kompenzaci prováděli přivřením clon před vláknovými navazovači. Tato kompenzace se ale musela opravit po každé úpravě experimentální sestavy. Později jsme zvolili cestu jen jednoho detektoru na výstupu z polarizátoru i za cenu delšího měření. Tím jsme se vyhnuli dalšímu problému s polarizátorem, který mimo vertikální polarizace částečně odráží i horizontální složku (cca 5 %). Polarizační analýzu s takto nedokonalým polarizátorem již nelze považovat za projekční měření, museli by jsme přejít na obecnější popis pomocí měření hodnoty pozitivního operátoru (POVM).

1.4.3 Fidelita klonů F

Fidelita kvantového stavu je reálné číslo $F \in [0, 1]$, poměřuje věrnost (podobu) kvantových stavů. Ta je definována jako pravděpodobnost, se kterou se měřený stav $|\psi_c\rangle$ (klon) vyprojektuje do stavu původního qubitu (vstupní stav) $|\psi\rangle$. Pokud je jeden ze stavů nebo oba ve smíšeném stavu, musíme využít k výpočtu matice hustoty $\hat{\rho}_c$ a $\hat{\rho}$:

$$F = |\langle\psi|\psi_c\rangle|^2, \qquad F = \langle\psi|\hat{\rho}_c|\psi\rangle, \qquad F = \left(\mathrm{Tr}\sqrt{\sqrt{\hat{\rho}_c}\hat{\rho}\sqrt{\hat{\rho}_c}}\right)^2. \tag{1.7}$$

Pokud jsou stavy shodné, je fidelita rovna jedné, $F = |\langle\psi|\psi\rangle|^2 = 1$. V případě dvou ortogonálních stavů je jejich vzájemná fidelita nulová, $F = |\langle\psi|\psi^\perp\rangle|^2 = 0$. Pokud porovnáme stav $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ s maximálně smíšeným stavem $\mathbb{1} = (|H\rangle\langle H| + |V\rangle\langle V|)/2$, dostaneme fidelitu $F = (|\alpha|^2 + |\beta|^2)/2 = 1/2$.

V případě jednoho qubitu je měření fidelity přímočaré. Známe-li (čistý) vstupní stav $|\psi\rangle$, nastavíme fázové destičky tak, aby skrz polarizační dělič prošel jen tento polarizační stav. Samozřejmě, kvantová fyzika je pravděpodobnostní, jen pokud bude mít měřený stav kolmou polarizaci, tak se na děliči s jistotou odrazí. Jinak vždy bude určitá pravděpodobnost, že projde. A tato pravděpodobnost je naše hledaná fidelita. Je dána počtem případů, kdy zaregistrujeme foton na průchod, ku součtu počtů detekcí jak na průchod tak na odraz.

Jestliže měříme výstupní stavy dvou fotonů, musíme vzít v potaz všechny možné kombinace. Tedy počet událostí, kdy první i druhý foton projde přes polarizátor, značíme

C^{++}, první foton projde a druhý se odrazí (C^{+-}), první se odrazí a druhý projde (C^{-+}). A nakonec počet událostí (koincidencí), kdy se oba fotony odrazí, značíme C^{--}. Fidelity prvního a druhého qubitu spočteme z koincidenčních měření podle těchto vztahů:

$$F_1 = \frac{C^{++} + C^{+-}}{C^{++} + C^{+-} + C^{-+} + C^{--}}, \qquad F_2 = \frac{C^{++} + C^{-+}}{C^{++} + C^{+-} + C^{-+} + C^{--}}. \tag{1.8}$$

1.4.4 Matice hustoty $\hat{\rho}$

Matice hustoty dvouqubitového stavu je popsána komplexní maticí 4×4. Díky podmínkám na fyzikální stav je tato matice definována šestnácti reálnými čísly. Pro určení matice hustoty tohoto stavu musíme provést nejméně 15 různých měření, šestnáctou neznámou určíme z normalizační podmínky. Různé počty měření nejčastěji používaných způsobů určení matice hustoty s ohledem k robustnosti vůči experimentálním chybám jsou shrnuty v ref. [A12].

My jsme používali úplnou tomografii dvouqubitového stavu, tj. 36 měření ve všech kombinacích projekcí dvou fotonů do lineární horizontální, vertikální, diagonální, antidiagonální a levotočivě a pravotočivě kruhové polarizace. Tato sada dat přeurčuje matici hustoty ($36 > 16$ resp. 15). Pro nalezení matice hustoty, která nejvíce odpovídá naměřeným výsledkům, se použila metoda maximální věrohodnosti (*Maximum Likelihood*) [11]. Tento způsob určení matice hustoty sice není nejrychlejší, potřebuje víc než dvojnásobek nutných měření, nicméně měření jsou snadno proveditelná a výsledek je robustní vůči experimentálním chybám.

Matice hustoty plně popisuje kvantový stav, pomocí ní lze spočítat čistotu stavu i fidelitu s daným stavem. Oproti přímému měření fidelity máme tu výhodu, že můžeme analyzovat změřený stav a objevit případnou experimentální nedokonalost. Například fidelitu klonovaných stavů lze zvýšit lokální transformací jednotlivých qubitů.

1.4.5 Pravděpodobnost úspěchu P_{succ}

Kvantové operace dělíme na deterministické, podaří se vždy, a pravděpodobností, občas se nezadaří. Pravděpodobnost úspěchu P_{succ} udává podíl úspěšných realizací operace vůči všem pokusům.

Při experimentální realizaci nějaké pravděpodobnostní operace máme dvojí účinnost. Jednou je teoretická pravděpodobnost úspěchu, která limituje úspěšnost zařízení s dokonalými bezztrátovými komponentami. Druhou je propustnost zařízení, která klesá s nedokonalostí vybavení. Většina optických komponent vykazuje ztráty. Tyto ztráty lze minimalizovat povrstvením optických ploch antireflexními vrstvami. Markantní jsou ztráty při navázání volně se šířícího prostorového svazku fotonů do optického vlákna. A také omezená účinnost detektorů způsobuje pokles měřeného signálu. Většinou se při prezentaci výsledků oprostí naměřená pravděpodobnost úspěchu o tyto tzv. technologické ztráty.

1.5 Využití kvantové informace

Možnosti využití kvantové informace vyplývají z vlastností kvantových stavů. To, že se kvantový stav změní při každém měření, se využívá při bezpečném přenosu informace

v kvantové kryptografii. S tím je spojena problematika přenosu kvantové informace. Při kvantovém počítání se využívá paralelní interakce kvantových stavů. Podrobnější popis jednotlivých využití najdete v referencích [4, 5].

1.5.1 Kvantová kryptografie

Kvantová kryptografie zaručuje bezpečný přenos klasické informace. Pomocí kvantových stavů se přenese kryptografický klíč, který je náhodný, stejně dlouhý jako zpráva, kterou má zašifrovat. Pokud by se nějaký narušitel pokusil odposlouchávat přenos kvantového klíče, nevyhnutelně svou interakcí kvantové stavy změní. Tato změna bude při kontrole odhalena a klíč se ke kódování tajné zprávy nepoužije. Teoreticky je tento koncept tajného přenosu neprolomitelný. V praxi se ale musí použít reálná zařízení a přenosové linky, jejichž nedokonalostí lze využít k zakrytí přítomnosti narušitele.

V podstatě jsou možné dvě strategie útoku na kvantovou kryptografii. Buď můžeme využít technické nedokonalosti vysílací nebo přijímací stanice [12–14] a nebo na linku připojíme kvantově klonovací zařízení a nepřesnosti a šum, které do přeneseného klíče zanese klonování, budeme vydávat za nedokonalost přenosového kanálu. Různými klonovacími zařízeními a jejich experimentální realizací se zabývá tato práce. Účelem výzkumu nebylo přímo napadení důvěryhodnosti kvantové kryptografie. Snažili jsme se ukázat, že současné experimentální vybavení je opravdu schopné pracovat na hranici teoretických možností. Po ověření limitů klonovacích zařízení je potřeba určit limity tolerovatelné chybovosti při přenosu náhodného klíče. Pokud bude chybovost přenosu vyšší, tak se buď klíč zahodí nebo se přistoupí k nějaké formě zesílení zabezpečení (*Privacy Amplification*) [15].

Všechna komerčně dostupná kvantově kryptografická zařízení využívají fotony jako nosiče kvantové informace. Obecně by se dalo říci, že světlo se dá využít primárně na přenos. Má malé ztráty při šíření volným prostorem i ve vláknech, kvantový stav se šířením příliš nemění. Na druhou stranu světlo nepostojí, nedá se snadno využít pro kvantové paměti ani pro složitější kvantové počítání.

1.5.2 Kvantové zpracování informace

Aby bylo kvantové počítání efektivní, tj. aby kvantové algoritmy byly rychlejší než klasické, potřebujeme mnoho interagujících qubitů. Toho lze snadněji dosáhnout na jiných platformách než na světle. Jejich nevýhodou je složitá podpůrná aparatura, tedy potřeba vysokého vakua, kryogenních teplot, magnetického stínění. První komerční ale finančně velmi málo dostupný kvantový „optimizátor“ – D-Wave byl představen v roce 2016 [16]. Od té doby se vyvíjejí stále větší (ve smyslu počtu aktivních qubitů) univerzální kvantové počítače, v současnosti vévodí tomuto odvětví čínský 50 qubitový fotonický Jiuzhang [17], 53 qubitový supravodivý Sycamore od Googlu [18] a 127 qubitový supravodivý Eagle od IBM [19]. Od IBM je ostatně hezké, že nechává své starší vývojové verze procesorů nám vědcům na hraní v projektu IBM Q.

V případě využití fotonů, buď už na platformě „spojitých proměnných“, např. stlačených stavů (jako Jiuzhang) nebo „diskrétních proměnných“, qubitů zakódovaných do jednotlivých fotonů, se ale musíme vypořádat s problematickou foton-fotonovou interakcí. Té lze dosáhnout například pomocí nelineárního média [20]. Materiály s dostatečnou nelinea-

ritou jsou zatím nedostupné, i kdyby byly, problém s náhodnou fází [21] činí tuto metodu prakticky nepoužitelnou. Další možnost fotonové interakce je tzv. lineární optika, kde se využívá jednoqubitových operací, dvoufotonové interference na děliči svazků, pomocných fotonů a jejich projekce. Tato metoda tzv. podmíněné interakce má pravděpodobnost úspěchu menší jak jedna [22].

Zpracování kvantové informace na platformě jednotlivých fotonů je tedy omezené. Nicméně může být s výhodou využito jako testovací platforma pro zkoumání fundamentálních vlastností. Také lze lineární optiku využít pro jednoduché operace související s přenosem kvantové informace. Převod kvantové informace mezi fotonovou a pevnolátkovými platformami není bezchybný a stoprocentně účinný. Převést fotonový qubit na pevnolátkový, provést deterministicky jednoduchou úlohu a znovu přepsat kvantovou informaci na foton je méně účinné a bezchybné než provést jednoduchý kvantový výpočet přímo pomocí fotonů.

V naší laboratoři jsme se zabývali testováním některých jednoduchých optických hradel pro zpracování kvantových bitů, např. SWAP hradlo [A13], částečnou symetrizaci a antisymetrizaci dvoufotonového stavu [A14], přípravu tzv. KLM stavů [A15] a C-phase hradlo [A16]. Popis těchto zařízení není tématem této práce.

1.5.3 Kvantové strojové učení

Strojové učení zažívá v posledních letech nebývalý rozmach [23–25]. Nejspíš je to kvůli rostoucí složitosti řešených problémů, kdy už začíná být problémem vytvořit dostatečně přesný matematický model zkoumaného procesu. Pro strojové učení stačí jen velké množství výstupních stavů tohoto procesu, aby v nich našlo skryté spojitosti.

I toto strojové učení by mohlo být mnohem účinnější, pokud by mohlo využít tzv. kvantového zrychlení (*Quantum Boost*). V současnosti se zatím publikují jen články o kvantově-klasickém strojovém učení, kdy pouze jeden ze dvou základních předpokladů strojového učení je kvantový, buď algoritmus nebo data. Spolu s kolegy jsme v této oblasti přispěli v obou těchto oblastech, pomocí neuronových sítí (klasický algoritmus) jsme určovali míru entanglementu (kvantová data) [A17, A18]. V druhém případě jsme našli správné nastavení (klasická data) pro fázově kovariantní klonování (kvantové zařízení) [A3, 26].

V tom druhém případě jsme chtěli ukázat, že strojový optimalizační algoritmus dokáže najít takové nastavení univerzálního kvantového zařízení, aby jeho výstupem byly klony vstupního stavu s maximální fidelitou. Jako modelovou situaci jsme zvolili interferometrický dělič schopný měnit dělící poměr nezávisle pro horizontální a vertikální polarizaci. Na vstupu zařízení byly polarizačně zakódované qubity, pomocná ancila a klonovaný stav s určitou distribucí na Blochově sféře. Pro testovanou třídu stavů byly výsledky nastavení zařízení známy z analytických výpočtů a optimalizační algoritmus je jen potvrdil. Nicméně bychom mohli na vstup zařízení poslat jakoukoliv netriviální distribuci stavů, pro kterou je přesné analytické nalezení nastavení zařízení prakticky nemožné. A v tom je právě přidaná hodnota kvantového strojového učení.

Kapitola 2

Klonování - teorie

Klonováním kvantových stavů myslíme takovou operaci, při které se nám zvětší počet kvantových stavů. Obecně z N stejných vstupních kvantových stavů $|\psi\rangle$ chceme vytvořit M výstupních stavů $|\psi\rangle$. Základní proces klonování vytváří z jednoho originálu dvě stejné kopie, značíme jako $1 \to 2$ klonování.

2.1 Nemožnost dokonalého klonování

Možnost respektive nemožnost klonovat neznámý čistý kvantový stav se zkoumala už v osmdesátých letech dvacátého století. Pánové Wooters a Żurek ve svém článku [27] ukázali jednoduchý důkaz známý jako *no cloning theorem*, který zde zopakuji.

Předpokládejme, že existuje taková unitární transformace, která je schopná vytvořit kopii bázového stavu, např. horizontálně polarizovaného fotonu, $|Q\rangle|H\rangle \to |Q_H\rangle|HH\rangle$. Zde $|Q\rangle$ a $|Q_H\rangle$ značí stav klonovacího zařízení před a po transformaci. Obdobná transformace by měla být schopna klonovat i ortogonální stav, tedy $|Q\rangle|V\rangle \to |Q_V\rangle|VV\rangle$. Podle principu superpozice by měla tato transformace klonovat i jakoukoliv lineární kombinaci těchto bázových stavů,

$$|Q\rangle(\alpha|H\rangle + \beta|V\rangle) \to \alpha|Q_H\rangle|HH\rangle + \beta|Q_V\rangle|VV\rangle.$$

Tento výsledek je ale odlišný od stavu dvou fotonů (v reprezentaci kreačních operátorů), které jsou oba v superpozici H a V polarizace

$$\frac{1}{\sqrt{2}}\left(\alpha\hat{a}_H^\dagger + \beta\hat{a}_V^\dagger\right)^2|\text{vak}\rangle = \alpha^2|HH\rangle + \sqrt{2}\alpha\beta|HV\rangle + \beta^2|VV\rangle,$$

kde kreační operátor aplikovaný na vakuový stav $|\text{vak}\rangle$ dá vzniknout fotonu s danou polarizací: $\hat{a}_{H,V}^\dagger|\text{vak}\rangle = |H\rangle$ resp. $|V\rangle$. Klonovací operace funguje tedy jen pro bázové stavy. Pokud je klonovaný stav v superpozici bázových stavů, výsledek klonování není shodný se stavem dvou fotonů v této superpozici.

Následující důkaz je trochu názornější. Předpokládejme unitární transformaci U působící na čisté signální stavy $|\psi\rangle$ a $|\phi\rangle$ a pomocné stavy (ancily) $|a\rangle$ tak, že vytvoří dvě kopie signálních stavů:

$$U\ |\psi\rangle|a\rangle = |\psi\rangle|\psi\rangle, \qquad U\ |\phi\rangle|a\rangle = |\phi\rangle|\phi\rangle.$$

Když druhou rovnici komplexně sdružíme a vynásobíme první rovnicí, dojdeme k rovnosti

$$\underbrace{U^*U}_{=1}\underbrace{\langle\phi|\psi\rangle}_{=x}\underbrace{\langle a|a\rangle}_{=1} = \underbrace{\left(\langle\phi|\psi\rangle\right)^2}_{=x^2}. \tag{2.1}$$

Rovnice, kdy se nějaké reálné číslo rovná svému kvadrátu ($x = x^2$), vede na dvě řešení, buď je $x = \langle\phi|\psi\rangle = 0$ nebo je $x = 1$. Tedy, buď jsou stavy $|\psi\rangle$ a $|\phi\rangle$ ortogonální nebo shodné. Jen v těchto dvou případech lze unitární transformací vytvořit dvě bezchybné kopie.

Touto kapitolou bychom mohli skončit – dokonalé klonování obecného (neznámého) stavu je nemožné. Ono je ale nemožné pouze vytvoření přesných kopií původního stavu. Pokud si ale dovolíme nazvat kopiemi i stavy přibližně podobné originálu (fidelita mezi originálem a kopií je menší jak jedna), potom můžeme směle v klonování pokračovat. Tento krok vpřed provedli Bužek a Hillery v roce 1996 [28]. Od té doby vznikly desítky teoretických i experimentálních prací zabývající se touto tematikou, první vlna je podchycena v přehledové práci Scaraniho a kol. [29].

2.2 Rozdělení klonovacích zařízení

S ohledem na *no cloning theorem* musíme upravit definici klonování. Kvantovým klonováním myslíme takovou operaci, která rozdělí kvantovou informaci ze vstupních stavů $|\psi\rangle$ mezi stavy výstupní, které jsou popsány celkovou maticí hustoty $\hat{\rho}$. Množství informace o původním stavu, která se přenese na jednotlivé výstupní klony, lze charakterizovat fidelitou klonu $F = \langle\psi|\hat{\rho}_c|\psi\rangle$. Zde $\hat{\rho}_c$ značí matici hustoty jednoho klonu, která se získá z celkové matice hustoty částečnou stopou přes ostatní klony.

Obecné klonovací zařízení vytvoří M klonů z původního počtu N vstupních stavů, tedy $N \to M$ klonování. Výstupní klony ale nemusí být stejné, tj. jejich fidelita se vstupním stavem $|\psi\rangle$ může být různá. Pokud tomu tak je, označujeme zařízení za **nesymetrická**. Při větším počtu klonů mohou nastávat složitější případy, kdy mají dva klony stejnou fidelitu a jeden odlišnou, což lze graficky vyjádřit takto: $1 \to 2 + 1$. Na rozdíl od nesymetrických zařízení je fidelita všech výstupních stavů **symetrického** klonování stejná.

Podobně jako u diskriminace neortogonálních kvantových stavů [A19] můžeme i klonovací zařízení dělit na **deterministická a pravděpodobnostní**. Deterministické zařízení zafunguje pokaždé, nicméně fidelita klonů je nejednotková. Oproti tomu pravděpodobnostní zařízení produkuje dokonalé kopie, ale pouze v určitém procentu realizací [30]. Dalo by se říci, že nedokonalé kopie se postselekčně vyřazují. V našem případě je ale pravděpodobnostní i ta deterministická strategie, protože pracujeme na platformě lineární optiky.

Velká pozornost při návrhu všech kvantových zařízení je věnována **optimalitě**. Optimální zařízení je takové, které pracuje na hraně zákonů kvantové mechaniky. Například klonovací zařízení produkujících klony neznámého stavu s jednotkovou fidelitou je už za touto hranou. Ale kde tato hrana leží se musí zjistit výpočtem pro každou třídu klonovaných stavů.

Variant klonovacích zařízení je mnoho, v následujícím výčtu jsou zmíněny ty nejzákladnější včetně těch, které jsme realizovali experimentálně. Pro jednoduchost budeme uvažovat pouze symetrické $1 \to 2$ klonování ve dvou dimenzích (prostor qubitu).

2.2.1 Semiklasické klonování

Semiklasické klonování se skládá ze dvou operací – z projekčního měření a z přípravy kvantových stavů. Na vstupním stavu $|\psi\rangle$ provedeme měření v náhodné bázi, například v H/V bázi, tím získáme klasickou informaci o tomto stavu. Pokud je výsledek měření $|H\rangle$, potom vytvoříme dva (nebo více) fotonů s touto polarizací a pošleme je na výstup. Pokud budeme měřící bázi měnit náhodně pro každý jednotlivý vstupní stav, potom bude fidelita klonů nezávislá na vstupním stavu a bude mít hodnotu $F = 2/3$. Tato hodnota se nazývá **semiklasický limit**, tvoří mezní hranici pro kvantová zařízení. Pokud navrhneme experimentální realizaci, která bude dosahovat horších výsledků, nemá ji cenu vůbec prezentovat. Výhodou semiklasického klonování je to, že se fidelita výstupních klonů nemění s jejich počtem (je nezávislá na počtu kopií M).

2.2.2 Triviální klonování

Za triviální klonování označujeme metodu vytváření kopií, která sice není optimální, nicméně je extrémně jednoduchá. Tato metoda by se dala shrnout slovy „nesahat a přidat“. Spočívá v tom, že vstupní stav necháme beze změny, jen k němu přidáme další foton s náhodnou polarizací. Aby bylo takové zařízení symetrické, musí být zajištěno nějaké promíchání těchto klonů, aby nebylo zřejmé, který z nich je originál a který je ten přidaný. Při měření bude mít jeden klon fidelitu rovnu jedné a druhý 1/2. V průměru budou mít oba klony fidelitu $F = 3/4$. S rostoucím počtem přidaných fotonů bude ale fidelita klonů klesat až k hodnotě 1/2, viz obr. 2.3.

2.2.3 Optimální univerzální klonování

Předchozí metody klonování jsou univerzální, tj. fidelita výstupních klonů je nezávislá na vstupním stavu. Nicméně, jak už bylo řečeno, nejsou optimální co do velikosti hodnot fidelit klonů. Optimální univerzální klonovací zařízení bylo navrženo pány Bužkem a Hillerym v již zmiňovaném průlomovém článku [28].

Optimální univerzální klonovací transformace má tvar

$$|H\rangle|Q\rangle \to \sqrt{\frac{2}{3}}|HH\rangle|\uparrow\rangle + \sqrt{\frac{1}{3}}|\Psi^+\rangle|\downarrow\rangle, \qquad |V\rangle|Q\rangle \to \sqrt{\frac{2}{3}}|VV\rangle|\downarrow\rangle + \sqrt{\frac{1}{3}}|\Psi^+\rangle|\uparrow\rangle. \quad (2.2)$$

Zde $|Q\rangle$ značí původní stav klonovacího zařízení, který je lineární kombinací bázových stavů $|\uparrow\rangle$ a $|\downarrow\rangle$, a $|\Psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$ je maximálně entanglovaný Bellův stav. Pokud je na vstupu této transformace stav $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, potom budou mít klony ve výstupních módech A a B matici hustoty ve stejném tvaru

$$\hat{\rho}_A = \hat{\rho}_B = \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^\perp\rangle\langle\psi^\perp|, \quad (2.3)$$

kde $|\psi^\perp\rangle = \alpha^*|V\rangle - \beta^*|H\rangle$ je stav kolmý vůči vstupnímu stavu $|\psi\rangle$. Tuto matici hustoty lze interpretovat i tak, že se s pravděpodobností 5/6 vytvoří dokonalá kopie stavu $|\psi\rangle$ a s pravděpodobností 1/6 dokonalý antiklon $|\psi^\perp\rangle$. Jen nevíme, kdy vznikne který z nich.

V průměru dosáhneme fidelitu klonů $F = \frac{5}{6} \approx 0.833$. Tato hodnota je optimální, maximálně dosažitelná v případě, že o vstupních stavech nemáme žádnou informaci. Ohledně

stavu $|\psi^{\perp}\rangle$, tak jak kvantová mechanika zakazuje bezchybné klonování neznámého stavu, není možné provést bezchybně ani NOT operaci, tj. vytvořit stav ortogonální k původnímu neznámému stavu.

2.2.4 Stavově závislé klonování

Úplný protipól univerzálního klonovacího zařízení je zařízení, které by bylo optimalizováno jen na jeden známý vstupní stav. Takové zařízení je ale triviální a klonovací fidelita jednotková. Pokud rozšíříme repertoár klonovacího zařízení na dva známé stavy $|\psi_0\rangle$ a $|\psi_1\rangle$, bude pro změnu výpočet fidelit klonů kvůli nedostatku symetrie až příliš netriviální. Jak je odvozeno v ref. [31], výsledek je závislý na překryvu vstupních stavů $s = |\langle\psi_0|\psi_1\rangle|$:

$$F = \frac{1}{2} + \frac{\sqrt{2}}{32s}(1+s)\left(3 - 3s + \sqrt{1-2s+9s^2}\right)\sqrt{-1+2s+3s^2+(1-s)\sqrt{1-2s+9s^2}}. \tag{2.4}$$

Pokud do vzorce dosadíme hodnotu překryvu $s = 0$ nebo $s = 1$, tedy kolmé či shodné stavy, bude výsledná fidelita klonů jednotková. Což je v souladu s *no-cloning theoremem* a rovnicí (2.1). Zajímavé je ale minimum fidelity pro nezávislé stavy ($s = 0.5$), hodnota $F \approx 0.987$ znamená téměř dokonalé kopie (alespoň co se experimentálního hlediska týče). Z tohoto důvodu je nutné, aby pro přenos náhodného klíče při kvantové kryptografii bylo použito tří a více kvantových stavů.

2.2.5 Fázově kovariantní klonování

Fázově kovariantní klonování je optimální individuální útok na kryptografické protokoly, u kterých leží přenášené stavy na jedné rovnoběžce (obecně na jakémkoliv rovinném řezu) Blochovy sféry, například nejznámější BB84 [32] nebo R04 [33]. Pro kódování bitů klíče se u prvního jmenovaného protokolu využívá dvou dvojic vzájemně kolmých stavů, typicky $|H\rangle/|V\rangle$ a $|D\rangle/|A\rangle$. Nicméně se dá použít i jakákoliv jiná kombinace stavů splňující podmínku, že tyto stavy leží v jedné rovině a tato rovina prochází středem Blochovy sféry. Pro jednoduchost zarotujeme tuto rovinu unitární transformací do rovníku Blochovy sféry. Stavy z rovníku Blochovy sféry můžeme popsat takto

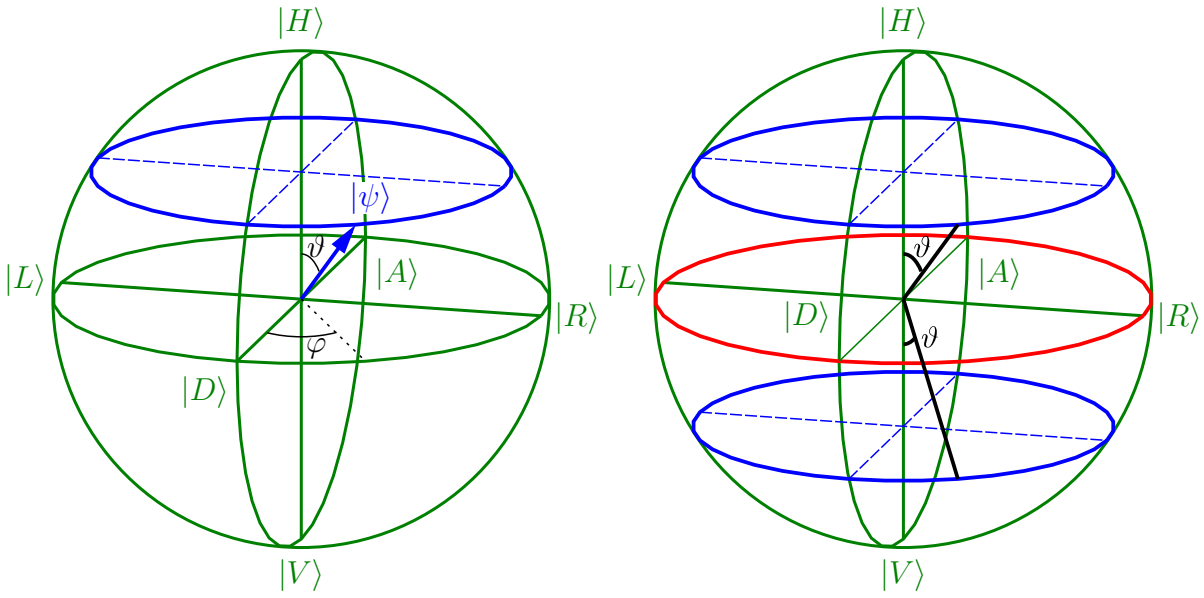
$$\left|\psi\left(\frac{\pi}{4},\varphi\right)\right\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{\imath\varphi}|V\rangle), \qquad \varphi \in [0, 2\pi]. \tag{2.5}$$

Fázově kovariantní klonovací zařízení může klonovat stavy nacházející se i mimo rovník, jen je vždy potřeba zvolit patřičnou polarizaci pomocného stavu. „Fázová kovariance“ znamená, že fidelita výstupních klonů nezávisí na fázi φ, ale jen na úhlové vzdálenosti stavu od rovníku (popsané parametrem ϑ). Třídu stavů klonovaných se stejnou fidelitou tvoří tedy rovnoběžky na Blochově sféře (viz obr. 2.1 vlevo),

$$|\psi(\vartheta,\varphi)\rangle = \cos\frac{\vartheta}{2}|H\rangle + e^{\imath\varphi}\sin\frac{\vartheta}{2}|V\rangle, \qquad \vartheta \in [0,\pi], \varphi \in [0,2\pi]. \tag{2.6}$$

Optimální klonovací transformace fázově kovariantních stavů z horní hemisféry má tvar [34]:

$$|H\rangle|H\rangle \to |H\rangle|H\rangle, \qquad |V\rangle|H\rangle \to \frac{1}{\sqrt{2}}(|V\rangle|H\rangle + |H\rangle|V\rangle). \tag{2.7}$$



Obrázek 2.1: Zobrazení kvantových stavů na Blochově sféře, vlevo fázově kovariantní stavy, vpravo stavy zrcadlově fázově kovariantní.

Druhý pomocný vstupní qubit má horizontální lineární polarizaci. Transformace pro dolní hemisféru je obdobná, jen se zamění stav $|H\rangle$ za $|V\rangle$ a naopak. Polarizace pomocného fotonu má potom logicky lineární vertikální polarizaci.

Minimální fidelity dosahuje fázově kovariantní kloner pro stavy z rovníku Blochovy sféry, $F = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.8535$, což je přibližně o dvě setiny více než u univerzálního klonování. Hodnota fidelit klonů roste s tím, jak se stavy blíží víc k pólům, viz obr. 2.2,

$$F(\vartheta) = \begin{cases} \frac{1}{2}\sin^2\frac{\vartheta}{2} + \cos^4\frac{\vartheta}{2} + \frac{\sqrt{2}}{4}\sin^2\vartheta, & 0 \le \vartheta \le \frac{\pi}{2} \\ \frac{1}{2}\cos^2\frac{\vartheta}{2} + \sin^4\frac{\vartheta}{2} + \frac{\sqrt{2}}{4}\sin^2\vartheta, & \frac{\pi}{2} \le \vartheta \le \pi \end{cases} . \tag{2.8}$$

Na pólech dochází ke klonování ortogonálních stavů, tedy s jednotkovou fidelitou.

2.2.6 Zrcadlově fázově kovariantní klonování

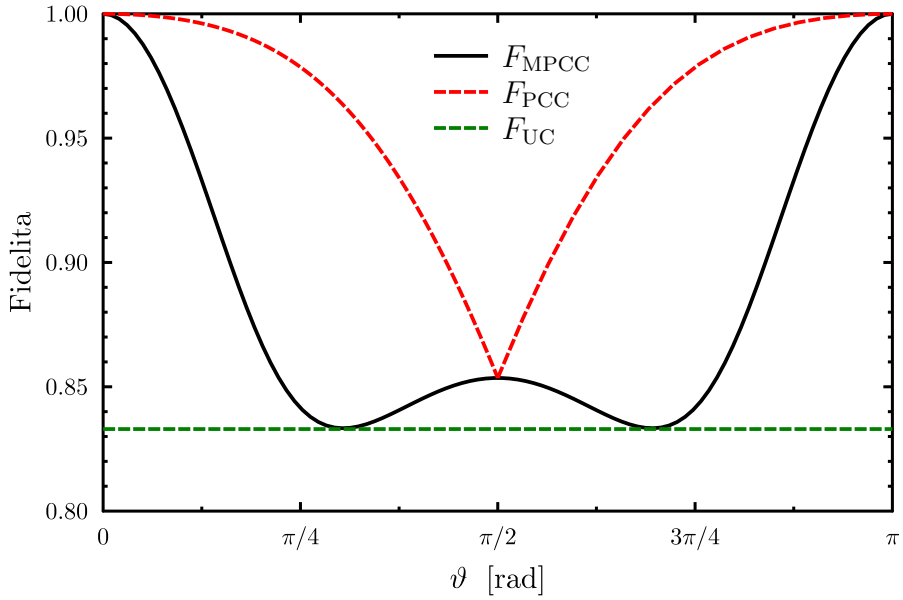
Zrcadlově fázově kovariantní stavy jsou, jak už název napovídá, rozšířením kovariantních stavů o stavy ležící ve stejné vzdálenosti od rovníku ale na druhé polokouli (viz obr. 2.1 vpravo). Klonovací transformace je odvozena v ref. [35]:

$$|H\rangle|0\rangle_a \to \Lambda|HH\rangle|0\rangle_a + \overline{\Lambda}|\Psi^+\rangle|1\rangle_a, \qquad |V\rangle|0\rangle_a \to \Lambda|VV\rangle|1\rangle_a + \overline{\Lambda}|\Psi^+\rangle|0\rangle_a, \tag{2.9}$$

kde $|\cdot\rangle_a$ značí pomocný stav, $|\Psi^+\rangle$ tripletní Bellův stav, $\overline{\Lambda} = \sqrt{1-\Lambda^2}$ a Λ má čtyři různá řešení

$$\Lambda_{i+2j} = (-1)^i \sqrt{\frac{1}{2} + (-1)^j \frac{\cos^2\vartheta}{2\sqrt{P(\vartheta)}}}, \qquad i,j = 0,1, \qquad P(\vartheta) = 2 - 4\cos^2\vartheta + 3\cos^4\vartheta. \tag{2.10}$$

Fidelita klonů zrcadlově kovariantních stavů je netriviální, viz obr. 2.2. Pro rovníkové stavy ($\vartheta = \pi/2$) provádí zařízení stejnou operaci jako fázově kovariantní klonování. Pro



Obrázek 2.2: Fidelita klonů optimálního symetrického zrcadlově fázově kovariantního klonování (MPPC) v závislosti na úhlu ϑ. Pro porovnání je znázorněn průběh i univerzálního (UC) a fázově kovariantního (PCC) klonování.

ortogonální stavy na pólech je dosaženo jednotkové fidelity jako u fázově kovariantního klonování. Ale pro stavy mezi těmito extrémy je výstupní fidelita horší, v jednom místě (prakticky ve dvou z důvodu zrcadlení) poklesne fidelita klonů na úroveň univerzálního klonování.

Optimální zrcadlově fázově kovariantní klonovací zařízení vytváří kopie, jejichž stav je podobný ke stavům prošlých Pauliho tlumícím kanálem [A8]. Qubity jsou částečně postiženy překlopením bitu (polarizace) nebo fáze. Klonovací zařízení se dá použít k simulaci takto chybové linky nebo k maskování útoku na kvantovou kryptografii za nedokonalou přenosovou linku.

2.2.7 Asymetrické klonování

U asymetrického klonování mohou být fidelity klonů různé. Při útoku na kvantovou kryptografii tím lze měnit poměr mezi množstvím zanesené chyby a získanou informací.

V případě optimálního univerzálního klonování fidelity klonů v módech 1 a 2 saturují *no-cloning* nerovnost:

$$\sqrt{(1-F_1)(1-F_2)} \geq \frac{1}{2} - (1-F_1) - (1-F_2). \tag{2.11}$$

Pokud si pomůžeme parametrizací, lze fidelity klonů vyjádřit takto:

$$F_1 = 1 - \frac{b^2}{2}, \qquad F_2 = 1 - \frac{a^2}{2}, \qquad a^2 + b^2 + ab = 1. \tag{2.12}$$

Symetrický případ nastane, je-li $a = b = \frac{1}{\sqrt{3}}$. Naopak, pro $a = 0$ resp. $b = 0$ dostaneme fidelitu jednoho klonu jednotkovou (klon shodný s originálem) a druhého klonu poloviční (klon nemající žádnou podobnost s originálem).

U fázově kovariantního klonování jsou fidelity klonů větší díky omezené třídě klonovaných stavů (viz obr. 2.2). Pro $\vartheta = \pi/2$ (rovníkové stavy) lze hodnoty fidelit klonů parametrizovat takto:

$$F_1 = (1 + \sqrt{q})/2, \qquad F_2 = \left(1 + \sqrt{1-q}\right)/2, \qquad q \in [0,1]. \tag{2.13}$$

V případě zrcadlově fázově kovariantního klonování závisí fidelita klonů též na parametru Λ,

$$F_1 = \left(1 + 2\sqrt{q}\Lambda\overline{\Lambda}\right)/2, \qquad F_2 = \left(1 + 2\sqrt{1-q}\Lambda\overline{\Lambda}\right)/2, \qquad q \in [0,1]. \tag{2.14}$$

2.2.8 $N \to M$ klonování

Případem, kdy máme k dispozici N stejných vstupních stavů a hodláme z nich vytvořit $M > N$ stejných výstupních klonů, se zabývalo více skupin [36–38]. Jejich výsledky ve dvou a více dimenzích shrnuje tabulka 2.1 a graf na obrázku (2.3).

režim klonování	dimenze 2	dimenze d
triviální	$\frac{N}{M} + \frac{M-N}{2M}$	$\frac{N}{M} + \frac{M-N}{dM}$
univerzální	$\frac{MN+M+N}{M(N+2)}$	$\frac{N}{M} + \frac{(M-N)(N+1)}{M(N+d)}$
fázově kovariantní ($N = 1$)	$\frac{3M+1}{4M}$	$\frac{1}{d} + \frac{(d-1)(M+d-1)}{Md^2}$

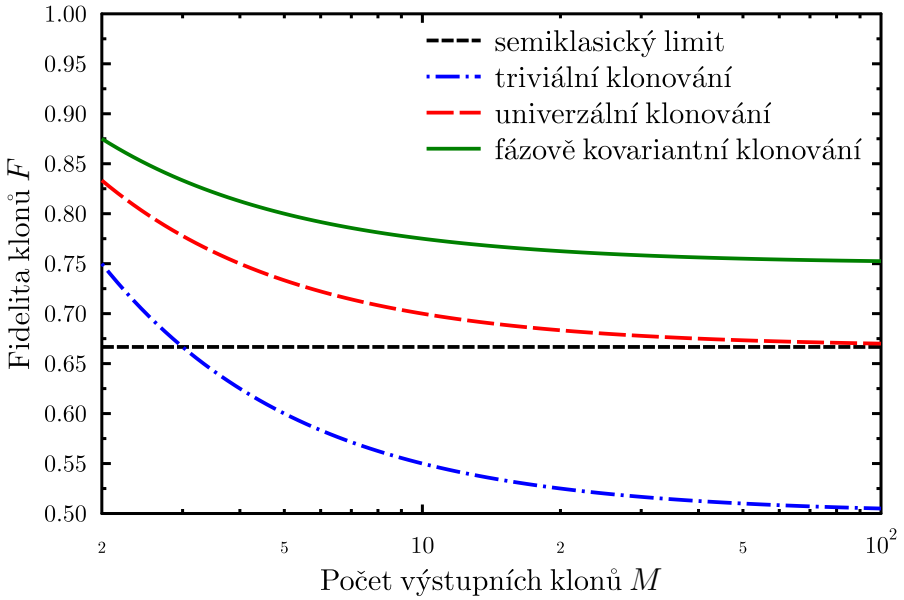
Tabulka 2.1: Fidelita klonů $N \to M$ klonování v různých režimech [29, 37, 38]. Pro fázově kovariantní klonování lze obecný předpis najít v ref. [39].

2.3 Využití klonování kvantových stavů

Kromě ověření platnosti základních principů kvantové mechaniky nabízí kvantová klonovací zařízení i jiné možnosti využití. Nejčastěji zmiňovaným využitím je útok na kryptografický přenos kvantových stavů. Nebo se může pomocí klonování zvýšit kapacita popřípadě maximální vzdálenost přenosu kvantových stavů ztrátovou linkou. Klonovací zařízení může také simulovat Pauliho ztrátovou linku [A8] nebo se pomocí něho mohou entanglovat mikroskopické (kvantové) a makroskopické objekty [40]. Pomocí klonování lze vytvořit speciální stavy umožňující získat lepší přesnost měření případně lepší rozlišení litografického zápisu [41–43]. Kromě popsaného klonování obstarává téma k zamyšlení desítkám vědců už pár desítek let.

2.3.1 Útok na kvantovou kryptografii

Koncept kvantové kryptografie, tedy protokolu pro bezpečný přenos kryptografického klíče mezi odesílatelem (Alicí) a příjemcem (Bobem), je v ideálních podmínkách nenapadnutelný. Při přenosu se využívá kódování do kvantových bitů, jakýkoliv pokus provést na



Obrázek 2.3: Závislost fidelity výstupních klonů na jejich počtu pro různé režimy klonování. Počet vstupních stavů je $N = 1$.

těchto qubitech měření narušitelem (Evou) tyto qubitů nevyhnutelně změní. Tato změna způsobí nenulový počet chyb zjištěných při následné kontrole Alicí a Bobem. Nicméně v reálných podmínkách s použitím standardních telekomunikačních přenosových linek (typické ztráty $0.2\,\mathrm{dB\,km^{-1}}$, tedy 20 km způsobí ztrátu 40 % fotonů) a detektorů s nejednotkovou kvantovou účinností a velkým počtem temných detekcí musí Alice s Bobem s určitou technologickou chybovostí počítat. Eva v principu může těchto nedokonalostí využít k maskování svého útoku. Ideálně pomocí kvantového klonování, buď fázově kovariantního nebo univerzálního, v závislosti na použitém přenosovém protokolu. Proto má každý protokol určenou mezní hodnotu chybovosti, se kterou se dá ještě považovat kryptografický přenos za bezpečný. Tato hodnota je různá, pokud uvažujeme, že je Eva schopna provést nekoherentní (individuální) nebo koherentní (kolektivní) útok.

Individuální útok je co do provedení jednodušší. Eva klonuje jednotlivé qubity z přenosové linky, jeden klon pošle Bobovi, na druhém provede měření. Pokud má Eva k dispozici nějaký druh kvantové paměti, může v ní uchovat své klony až do doby, kdy Bob Alici veřejně oznámí báze, ve kterých měřil. Eva s touto informací navíc může zoptimalizovat své měření tak, aby efektivně odhadla stavy klasických bitů sdílených Alicí a Bobem.

V případě **koherentního útoku** provádí Eva kolektivní měření na části nebo všech svých kopiích zároveň. Současný stav kvantových technologií tento útok zatím neumožňuje.

2.3.2 Zvýšení kapacity kvantového přenosu

Jednotlivé fotony jsou ideální pro přenos kvantové informace na velké vzdálenosti. Jak při šíření ve volném prostoru, tak v optických vláknech ale dochází ke ztrátám, jak bylo zmíněno výše. V případě klasické informace se dá signál zesílit v opakovacích stanicích dříve, než jeho intenzita poklesne pod měřitelnou úroveň. V případě kvantových stavů takto zesilovat nelze, maximální přenosovou vzdálenost určuje pokles počtu detekovaných

fotonů pod limitní hodnotu. Prodloužit tuto vzdálenost nebo zvýšit přenosovou rychlost (frekvenci detekcí signálních fotonů) jsou jedny z požadavků na větší rozšíření kvantové kryptografie.

Trojnásobné prodloužení maximální přenosové vzdálenosti umožňuje kvantový opakovač (*repeater, relay*) [44]. Toto zařízení potřebuje synchronizovaný zdroj entanglovaných fotonů, dvoufotonovou interferenci a měření Bellových stavů, což je experimentálně dosti náročné. Další možnost – zesilovače – tak, jak je zavedli N. Gisin, S. Pironio a N. Sangouard [45], ve skutečnosti kvantovou informaci nezesilují, pouze oznamují průchod signálního fotonu beze změny jeho kvantového stavu (nedemoliční měření přítomnosti).

První zmínku o tom, že lze pro zvýšení přenosové kapacity kvantové linky použít stavově závislé kvantové klonování, lze najít v referenci [46]. Tato myšlenka byla rozvedena a experimentálně ověřena v ref. [A10]. Princip tkví v tom, že místo jednoho fotonu pošleme do přenosové linky dva fotony vzniklé klonováním. Pokud k příjemci dorazí oba, lze z nich vyextrahovat původní kvantový stav. Pokud vlivem ztrát dorazí do cíle jen jeden foton, alespoň část informace bude přenesena. Tato metoda bude efektivní, pokud bude splněno

$$P_{succ} > \frac{1}{4F-2} \qquad \text{resp.} \qquad F > \frac{1}{4P_{succ}} + \frac{1}{2}, \tag{2.15}$$

kde F je fidelita klonů a P_{succ} pravděpodobnost úspěchu symetrického klonování. Pokud bude úspěšnost jednotková, stačí nám fidelita $F > 3/4$, tedy nad limitem triviálního klonování. S klesající pravděpodobností úspěchu klonování rostou nároky na fidelitu. Tu můžeme zvýšit například tehdy, známe-li nějakou apriorní informaci o přenášených stavech. Potom lze použít například fázově kovariantní klonování s vyšší fidelitou klonů a dosáhnout vyšší přenosové kapacity.

Kapitola 3

Univerzální klonování – experimenty

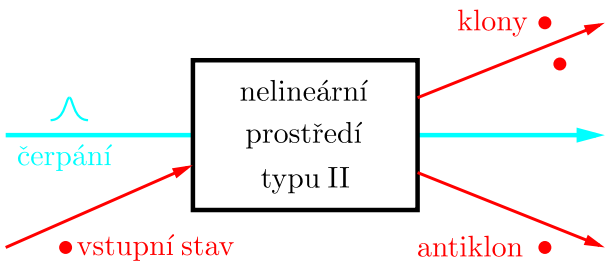
Pro univerzální klonování, kdy fidelita klonů nezávisí na stavu vstupního qubitu, lze použít několik metod. Historicky prvním byl nelineární proces stimulované sestupné konverze. Na tomto principu jsme v našich laboratořích žádné klonovací zařízení nesestrojili. Další možností je shlukování fotonů na vyváženém, polarizačně nezávislém děliči svazku, tzv. Hongovo-Ouovo-Mandelovo klonování. Třetí možností je univerzální klonování pomocí symetrizace dvoufotonového stavu.

3.1 Klonování na bázi stimulované emise

Klonování na bázi stimulované emise využívá nelineární jev stimulované sestupné parametrické konverze typu II [10], kdy signální foton nesoucí originální kvantovou informaci v podobě svého polarizačního stavu stimuluje vznik nového fotonu se stejnou polarizací. Typ II značí, že v nelineárním prostředí, které je čerpáno laserem na poloviční vlnové délce, může při spontánní emisi se stejnou pravděpodobností vzniknout dva kolmé polarizační stavy, tedy spontánně vzniklý fotonový pár je entanglovaný v polarizaci. A jelikož je pravděpodobnost pro stimulovanou i spontánní emisi stejná, nelze při klonování odlišit mezi stimulovanou emisí (dva klony s jednotkovou fidelitou) a spontánní emisí (původní qubit a qubit s náhodnou polarizací). Výsledná fidelita klonů bude mít hodnotu kvantového limitu univerzálního klonování $F = 5/6$.

Koncept klonování stimulovanou emisí lze jednoduše rozšířit na $N \to M$ klonování, v tom případě se na vstup zařízení pošle více vstupních fotonů. Antiklon, neboli stav s kolmou polarizací vůči vstupnímu stavu, vzniká na druhém výstupu nelineárního prostředí, je svázán s klonem a čerpacím fotonem zákony zachování hybnosti a energie (obr. 3.1). I jeho fidelita bude degradována neoddělitelnou spontánní emisí.

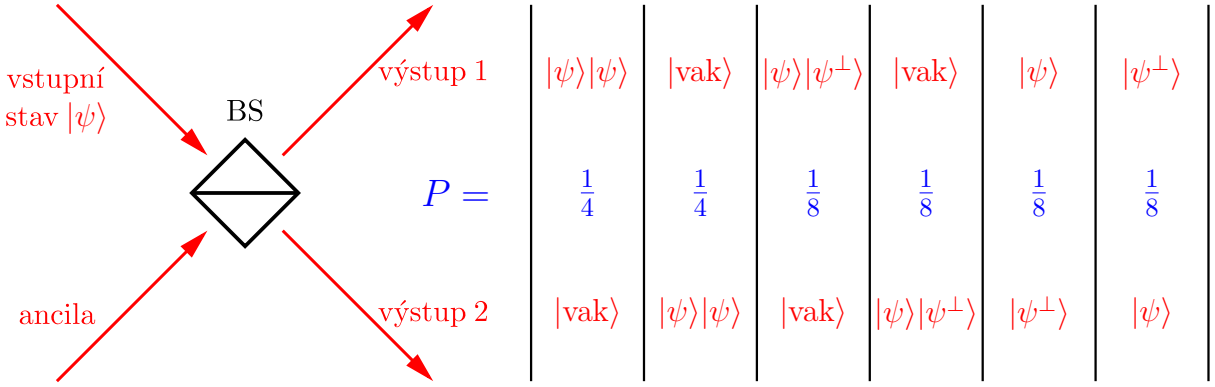
Experimentálně byla tato metoda ověřena několika skupinami [47–49]. Jednou z hlavních nevýhod tohoto způsobu klonování je zatím nedostatečná nelinearita současných prostředí. V současnosti používané krystaly BBO (β-baryum borát) s koeficientem nelineární susceptibility $\chi_{22} = 2.2\,\mathrm{pm\,V^{-1}}$ ale třeba i periodicky pólované KTP ($KTiOPO_4$) s efektivně větší nelinearitou nezaručují dostatečnou úspěšnost klonovací procedury. Další nevýhodou je složitá aparatura, kdy nelineární prostředí musí být čerpáno velmi krátkými ale vysoce energetickými pulzy, přičemž se musí signální foton časově překrýt s čerpacím pulzem.



Obrázek 3.1: Klonovaní na bázi stimulované emise.

3.2 Hongovo-Ouovo-Mandelovo klonování

Tzv. Hongovo-Ouovo-Mandelovo (HOM) klonování využívá jen aparátu „lineární optiky“ (děliče svazků a jednoqubitové operace). Toto klonování je založeno na efektu, který poprvé experimentálně demonstrovali pánové Hong, Ou a Mandel v roce 1987 [9]. Když na vyvážený dělič dopadají na dva vstupy dva nerozlišitelné fotony, potom se shluknou a opouštějí dělič jedním z výstupů pohromadě. Pro samotnou klonovací operaci stačí tedy jen polarizačně nezávislý vyvážený dělič a pomocný foton (*ancila*) s náhodnou polarizací. Tento pomocný foton se většinou připravuje ve stavu $|H\rangle$ a $|V\rangle$ polarizace, které se náhodně střídají. Vstupní qubit interaguje na děliči s pomocným fotonem. S pravděpodobností 1/2 se pomocný foton vyprojektuje do polarizace signálního fotonu, v tom případě se oba fotony shluknou a opouštějí dělič společně. V druhé polovině případů se pomocný foton vyprojektuje do kolmé polarizace, je vůči signálnímu fotonu rozlišitelný, oba fotony se rozhodují o výstupním portu náhodně, se stejnou pravděpodobností odchází pospolu nebo každý zvlášť. Všechny možné situace jsou znázorněny na obrázku 3.2. Pokud opouští oba fotony dělič jedním výstupem, je dvakrát větší pravděpodobnost stavu $|\psi\rangle|\psi\rangle$ než stavu $|\psi\rangle|\psi^\perp\rangle$. Pět ze šesti výstupních fotonů bude mít stav totožný s originálním stavem $|\psi\rangle$ a jeden foton bude mít stav ortogonální ($|\psi^\perp\rangle$), celková fidelita klonů bude opět 5/6. Je-li po jednom fotonu na každém výstupu, jedná se o původní vstupní qubit a jeho kolmý protějšek, jen nevíme, kterým výstupem vyšel který.



Obrázek 3.2: Hongovo-Ouovo-Mandelovo klonování se všemi výstupními kombinacemi a jejich pravděpodobností. Ancila je připravena ve stavu náhodné polarizace. $|\text{vak}\rangle$ značí vakuový stav, tedy na daném výstupu není žádný foton.

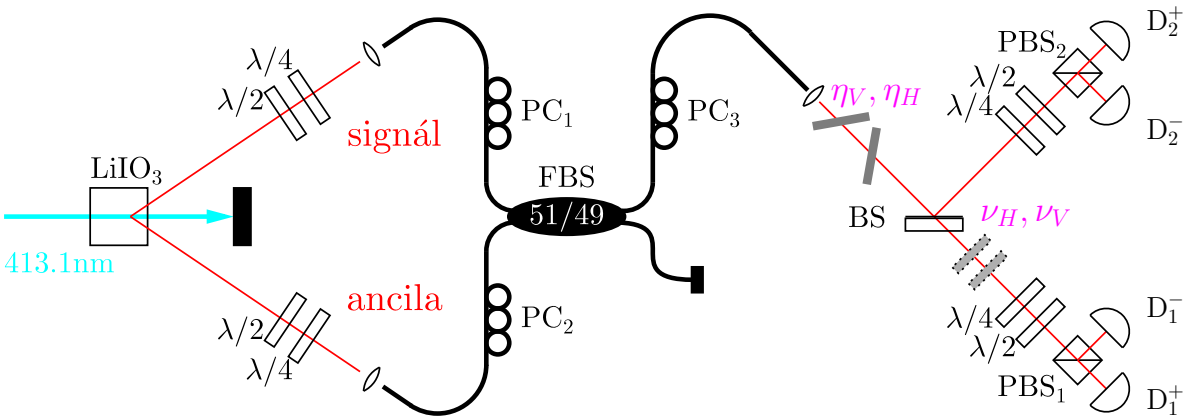
Experimentů, popisujících klonovací zařízení pracující na tomto principu, bylo několik [50–54]. Kritický problém této metody je v tom, že je naprosto náhodné, kterým výstupním portem fotony dělič opustí. Můžeme provést pouze postselekci, pokud na jednom výstupu nezaznamenáme detekci fotonu, tak to značí, že oba klony opustily dělič druhým výstupem. To nastane s pravděpodobností 3/8. Tento způsob klonování nelze rozšířit na více vstupních či výstupních stavů, při větším počtu fotonů nelze využít zhlukovacího efektu. Při experimentální realizaci je největším oříškem dosáhnutí dostatečné nerozlišitelnosti vstupního a pomocného fotonu za děličem, kdy musí být fotony nerozlišitelné ve všech stupních volnosti krom polarizace.

3.2.1 HOM klonování hybridním setupem

Test HOM klonování jsme provedli jen pomocí tzv. hybridní zařízení [A4, A6]. To získalo svůj název díky tomu, že je sestaveno jak z komponent vláknové optiky, tak z komponent pro volné šíření v prostoru, viz schéma na obrázku 3.3.

Prvotní motivací pro stavbu tohoto zařízení bylo dosažení lepšího prostorového překryvu interagujících fotonů díky vláknovému děliči. Přitom jsme ale chtěli zachovat polarizační kódování informace. Polarizaci jsme mohli efektivně ovládat jen ve volném prostoru. Zařízení by samozřejmě fungovalo stejně, i kdyby byl místo vláknového děliče použit objemový.

Pokud fázové destičky kontrolující stav signálního a pomocného fotonu neprovádí žádnou transformaci a polarizační rotátory PC_1 a PC_2 kompenzují polarizační změnu vláken před vláknovým děličem, potom se páry fotonů na tomto děliči shlukují (oba fotony ze zdroje mají stejnou horizontální lineární polarizaci). Se změnou délky jednoho ramene lze sledovat tzv. HOM zářez (dip). Jeho vizibilita byla přibližně 98 %, což bylo výrazně více, než se nám tehdy dařilo dosáhnout s objemovým děličem. Dokázali jsme tedy pomocí jednomodových vláken a pečlivého výběru správných prostorových a spektrálních módů ze zdroje dosáhnout téměř dokonalé nerozlišitelnosti fotonů z páru.

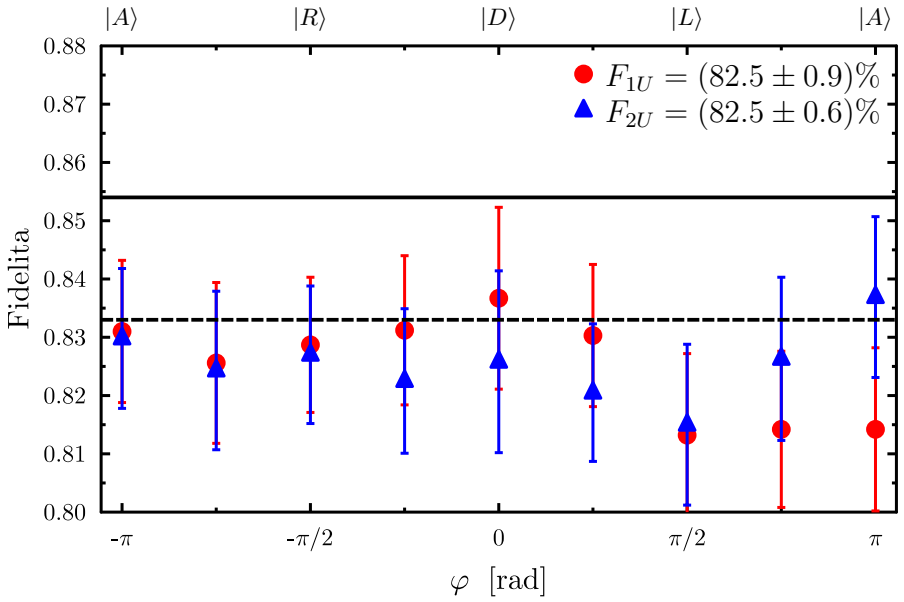


Obrázek 3.3: Hybridní klonovací zařízení, PC - polarizační rotátor, FBS - vláknový dělič, BS - polopropustné zrcátko (dělič), PBS - polarizátor, D - navázání do vlákna a detektor, $\lambda/2$ a $\lambda/4$ – půlvlnná a čtvrtvlnná fázová destička, η a ν - nakloněná sklíčka způsobující polarizačně závislé ztráty.

V této konfiguraci pracuje i HOM klonování. Polarizace pomocného fotonu (ancily) se mění náhodně mezi H a V polarizací. Fidelity klonů budou nezávislé na stavu vstupního qubitu. Nevýhodou je, že oba klony jsou v jednom prostorovém módu, buď na jednom nebo na druhém výstupu z vláknového děliče. V našem zařízení jsme jeden výstup nevyužili, ztratili jsme tedy polovinu výstupních klonů. Abychom od sebe jednotlivé klony před polarizační analýzou oddělili, museli jsme použít dalšího, tentokrát objemového, děliče (BS). Rozdělení se povede s pravděpodobností 1/2, v polovině případů pokračují fotony pospolu. Tyto případy nejsou započítány, nezpůsobí koincidenční událost. Další ztráty způsobily polarizační filtrace (viz sekce 4.1) před a za děličem BS, které kompenzovaly mírnou polarizační závislost děliče ($R_H = 52.7\,\%$, $R_V = 49.1\,\%$). Ve výsledku se dělič s filtrací choval jako polarizačně nezávislý do obou výstupů.

Vláknový dělič naproti tomu polarizační závislostí netrpěl. Nicméně vlákna k němu připojená měnila původní polarizační stav signálního a pomocného fotonu. Tato změna musela být vykompenzována pomocí polarizačních rotátorů pro každou vstupní polarizaci. V praxi to probíhalo tak, že se zaclonilo bud signální nebo pomocné vstupní rameno a nastavila se polarizační analýza na výstupech na požadovaný polarizační stav. Pak se pomocí polarizačního rotátoru PC_1 resp. PC_2 maximalizoval počet detekcí na detektorech D^+.

Výsledky měření v univerzálním klonovacím režimu jsou na obrázku 3.4. Polarizace signálního fotonu byla vybírána z rovníku Blochovy sféry. Pro takové stavy není potřeba náhodně měnit polarizaci pomocného fotonu, takže byl nastaven trvale na vertikální lineární polarizaci. Průměrné hodnoty fidelit klonů byly 82.5 %, což je blízko teoretickému limitu $83.\overline{3}$ %.



Obrázek 3.4: Závislost fidelit klonů na parametru φ pro rovníkové stavy ($\vartheta = \pi/2$) v případě symetrického univerzálního klonování. Pomocný foton měl vertikální lineární polarizaci. Černá plná a přerušovaná čára značí limity fázově kovariantního resp. univerzálního klonování. Hodnoty fidelit v legendě jsou průměry přes všechny měřené stavy.

3.3 Klonování symetrizací dvoufotonového stavu

V článku Wernera a kol. [55] je popsána myšlenka, že klonovat kvantový stav lze i pomocí symetrizace dvoufotonového stavu, který je složen ze stavu, který hodláme klonovat (signál), a z ancily s náhodnou polarizací. Proces symetrizace si můžeme jednoduše představit tak, že pomocí nějakého zařízení rozložíme vstupní dvoufotonový stav na symetrickou a antisymetrickou část (ve smyslu maximálně entanglovaných Bellových stavů $|\Phi^{\pm}\rangle$ a $|\Psi^{\pm}\rangle$). Tu antisymetrickou ($|\Psi^{-}\rangle$) definovaně utlumíme a obě části opět koherentně složíme. Míra zeslabení (symetrizace) je úměrná koeficientu asymetrie klonování. V limitním případě, pro úplné utlumení antisymetrické části budou mít klony stejnou fidelitu.

Operaci symetrizace můžeme matematicky popsat operátory

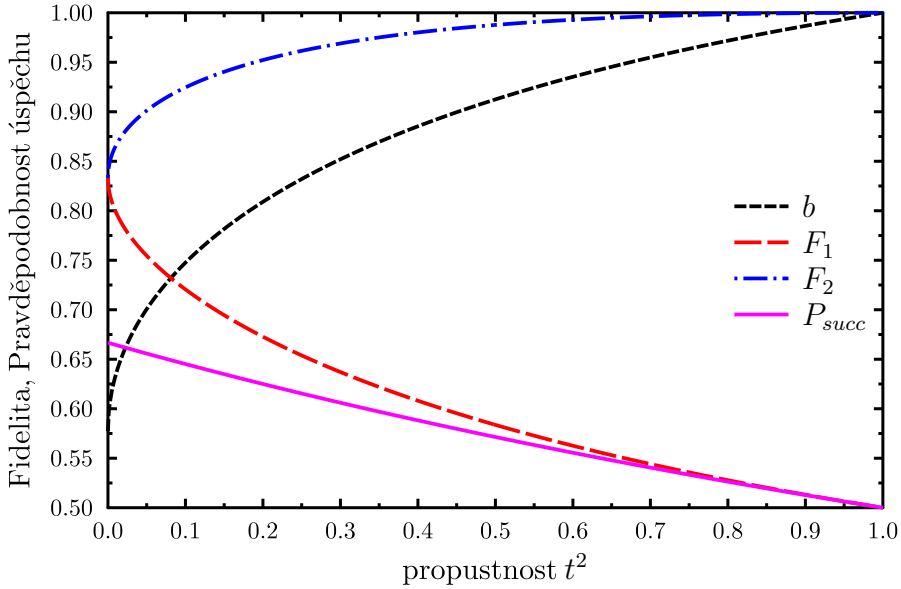
$$V_s = \Pi_+ + t\Pi_-, \qquad \text{kde} \qquad \Pi_- = |\Psi^-\rangle\langle\Psi^-| \qquad \text{a} \qquad \Pi_+ = \mathbb{1} - \Pi_-. \tag{3.1}$$

Čím víc zmenšujeme hodnotu koeficientu propustnosti t, tím víc bude transformace symetrizovat vstupní dvoufotonový stav složený ze signálního stavu $|\psi\rangle$ a pomocné ancily s náhodnou polarizací popsanou maticí hustoty $\hat{\rho}_a = (|H\rangle\langle H| + |V\rangle\langle V|)/2$. Fidelity výstupních klonů budou závislé jen na parametru propustnosti t,

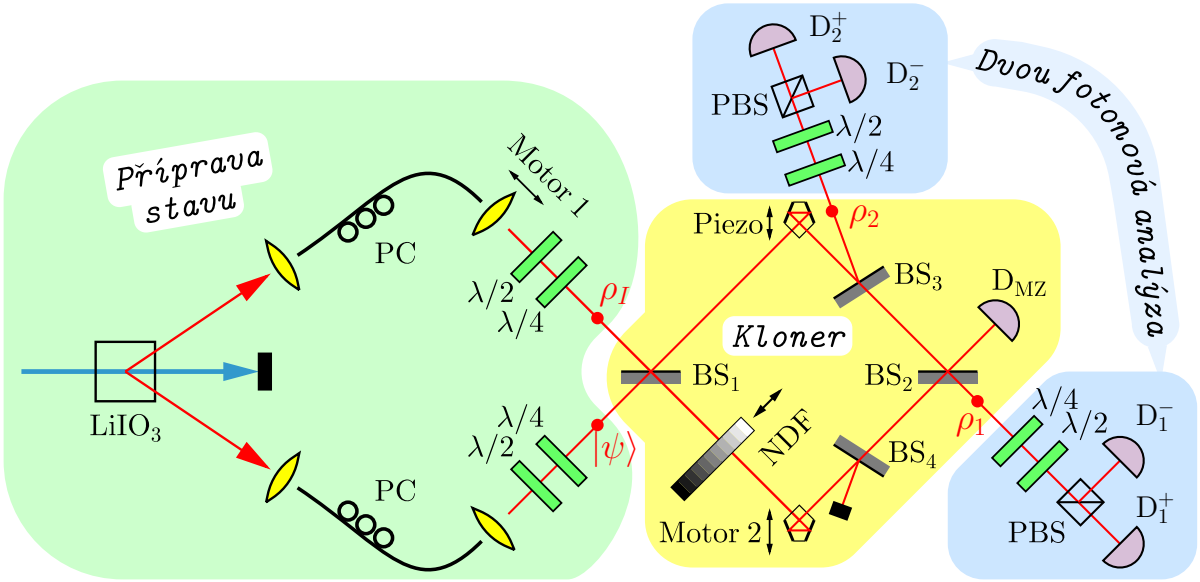
$$F_1 = \frac{t^2 - 2t + 5}{2t^2 + 6}, \qquad F_2 = \frac{t^2 + 2t + 5}{2t^2 + 6}. \tag{3.2}$$

Pokud tyto hodnoty dosadíme do vztahu 2.11, dojdeme k rovnosti, což značí, že takové zařízení je optimální, tj. dosažené fidelity jsou maximálně možné podle teorie.

Na obrázku 3.5 je znázorněna závislost pravděpodobnosti úspěchu klonování na míře symetrizace zařízení, které zastupuje propustnost t^2. Na propustnosti závisí i asymetrie



Obrázek 3.5: Závislost fidelit klonů a pravděpodobnosti úspěchu klonování pomocí symetrizace v závislosti na propustnosti t^2. Znázorněn je též průběh jednoho z koeficientů asymetrie b.



Obrázek 3.6: Univerzální klonovací zařízení na bázi částečné symetrizace, PC - polarizační rotátor, BS - vyvážený nepolarizační dělič, PBS - polarizátor, D - navázání do jednomodového vlákna a detektor, $\lambda/2$ a $\lambda/4$ – půlvlnná a čtvrtvlnná fázová destička, NDF – šedý filtr s proměnnou propustností.

fidelit klonů, které můžeme popsat pomocí koeficientů a a b (viz rovnici 2.13),

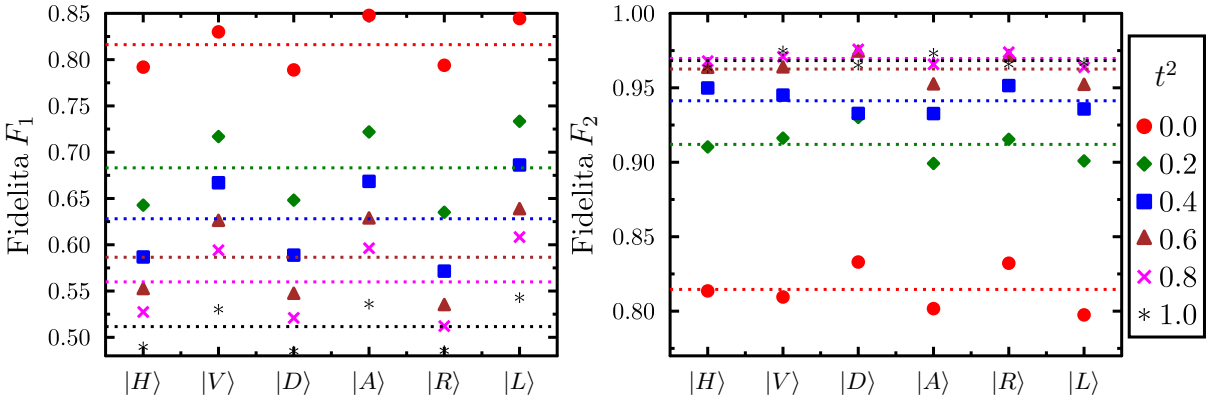
$$P_{succ} = \frac{2}{3+t^2}, \qquad a = \frac{1-t}{\sqrt{t^2+3}}, \qquad b = \frac{1+t}{\sqrt{t^2+3}}. \tag{3.3}$$

K experimentálnímu ověření tohoto principu klonování jsme použili zařízení pro částečnou symetrizaci a asymetrizaci [A14]. Pro symetrické i asymetrické klonování jsme samozřejmě použili jen částečnou symetrizaci dvoufotonového stavu, výsledky jsou shrnuty v článku [A7]. Schéma zařízení (již adaptovaného na klonování) je na obrázku 3.6.

Klonovací zařízení se skládá z Machova-Zehnderova interferometru s šedým filtrem ve spodním rameni. Druhý výstup zařízení je odkloněn děličem BS_3 z horního ramene interferometru, dělič BS_4 kompenzoval ztráty v ramenech. Druhý výstup interferometru vedoucí na detektor D_{MZ} byl použit pro stabilizaci fáze.

Zařízení opět funguje pravděpodobnostně, úspěšné je jen tehdy, zadetekujeme-li po jednom fotonu na každém výstupu. Výsledek klonování se odvíjí od chování signálního a pomocného fotonu na prvním děliči BS_1. Lze předpokládat, že pokud spolu tvoří symetrický dvoufotonový stav, na tomto děliči se shluknou. Pokud půjdou spolu oba spodním výstupem, neexistuje možnost, aby dorazily na oba výstupy zařízení. V tomto případě je klonování neúspěšné. Pokud půjdou oba horním ramenem (s pravděpodobností 1/2), potom se s pravděpodobností 1/4 na následujících děličích rozdělí tak, že budeme mít po jednom fotonu na obou výstupech, zařízení zafunguje s celkovou účinností 1/8. V horním rameni nejsou žádné další ztráty, symetrický stav nebude zeslaben.

V případě vstupního antisymetrického dvoufotonového stavu dojde na prvním děliči k antishluknutí, tj. vždy jde jeden foton do jednoho výstupu. Spodní foton projde šedým filtrem s propustností t a s pravděpodobností 1/4 dojde na první výstup zařízení. Foton



Obrázek 3.7: Fidelity klonů pro různé stavy z Blochovy sféry. Hodnoty fidelit nejsou korigovány na různé účinnosti detektorů. Parametr asymetrie je úměrný propustnosti šedého filtru t^2.

na horním výstupu necítí žádné další ztráty a s pravděpodobností 1/2 vyjde na druhý výstup. Se změnou propustnosti šedého filtru můžeme tento stav definovaně utlumit.

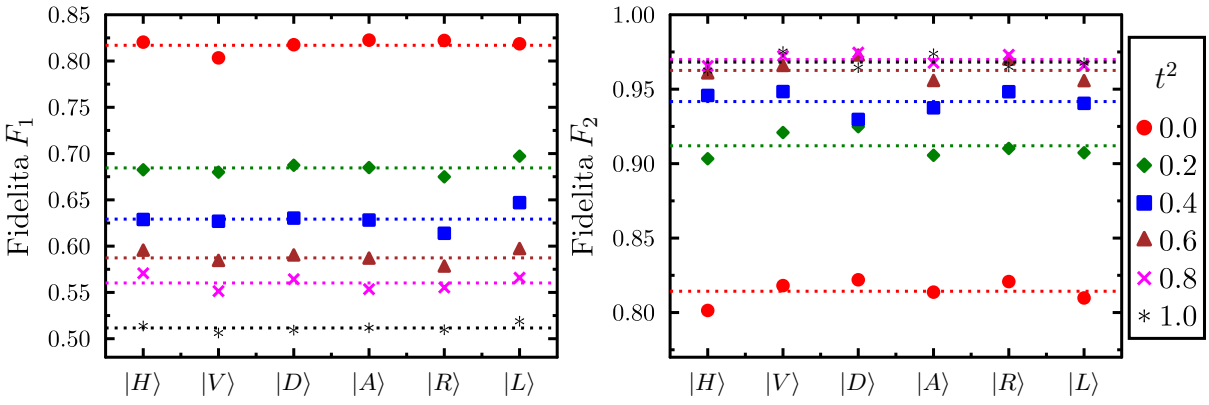
Pro $t = 1$ dojde k opětovnému obnovení vstupního dvoufotonového stavu. Signální foton skončí na druhém výstupu ($F_2 = 1$), pomocný foton na prvním výstupu ($F_1 = 0.5$) [1]. Je-li $t = 0$, potom je spodní rameno interferometru prakticky zablokováno, antisymetrický stav je úplně utlumen. Ze zařízení se stane symetrické HOM klonovací zařízení jako to na obr. 3.3 (jen bez ztrátových sklíček).

Zařízení jsme testovali pro šest různých stavů z Blochovy sféry, $|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, $|R\rangle$ a $|L\rangle$. Pomocný foton měl náhodně buď horizontální nebo vertikální lineární polarizaci. Na výstupu se prováděla projekce na vstupní stav a na stav kolmý. Toto měření bylo ovlivněno rozdílnou účinností detektorů, což se projevilo v oscilacích naměřených fidelit pro různé vstupní stavy (viz grafy na obr. 3.7).

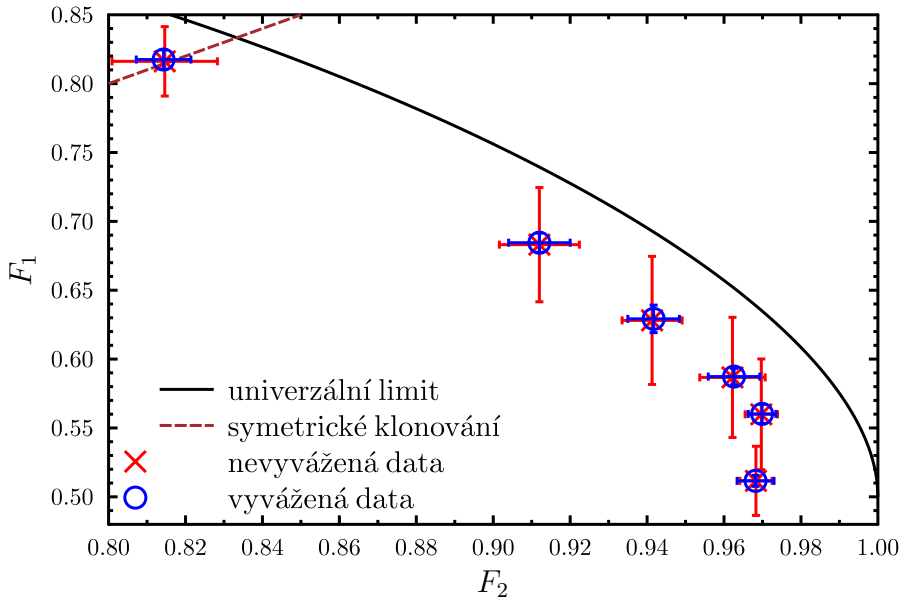
Oscilaci fidelit jsme opravili tak, že se na vstupu změnil stav signálního fotonu na ortogonální protějšek a provedlo se měření tentokrát se zaměněnou funkcí detektorů D^+ a D^-. Naměřené hodnoty pro oba ortogonální vstupy se sečetly. Naměřené fidelity vyvážené tak, aby nebyly ovlivněné účinností detektorů jsou na grafech na obr. 3.8.

Průměrné hodnoty fidelit přes 6 stavů z Blochovy sféry v závislosti na míře asymetrie jsou vykreslené v grafu 3.9 a vypsané v tabulce 3.1. Nižší hodnotu fidelit vzhledem k teoretickému předpokladu lze přičíst nedokonalé interferenci v MZ interferometru. Pravděpodobnost úspěchu zařízení nebyla určena. Samotné symetrizační zařízení má účinnost 1/8, úspěšnost klonování potom závisí ještě na propustnosti šedého filtru, celková závislost teoretické pravděpodobnosti úspěchu má tvar $P_{succ} = \frac{1}{8}\frac{2}{t^2+3}$. Pohybuje se tedy mezi hodnotami 1/12 pro $t = 0$ a 1/16 pro $t = 1$.

[1] To, na kterém výstupu který foton skončí, závisí na fázovém rozdílu mezi rameny MZ interferometru. Pro fázi π se výstupní ramena signálního a pomocného fotonu prohodí, toto zařízení funguje též jako SWAP hradlo [A13].



Obrázek 3.8: Fidelity klonů pro různé stavy s Blochovy sféry. Hodnoty fidelit jsou korigovány na různé účinnosti detektorů. Parametr asymetrie je úměrný propustnosti šedého filtru t^2.



Obrázek 3.9: Závislost fidelit asymetrického univerzálního klonování na principu symetrizace stavů. Asymetrie klonování se mění propustností šedého filtru, pro $t^2 = 0$ dochází ke symetrickému HOM klonování. Hodnoty jsou určeny zprůměrováním fidelit přes 6 různých vstupních stavů.

t^2	a	b	$F_{1T}[\%]$	$F_{2T}[\%]$	$F_1[\%]$	$F_2[\%]$
0.0	$1/\sqrt{3}$	$1/\sqrt{3}$	$83.\overline{3}$	$83.\overline{3}$	81.8±0.7	81.4±0.7
0.2	0.31	0.81	67.3	95.2	68.5±0.7	91.2±0.8
0.4	0.20	0.89	60.8	98.0	62.9±1.0	94.2±0.7
0.6	0.12	0.94	56.3	99.3	58.7±0.6	96.3±0.7
0.8	0.05	0.97	52.8	99.9	56.0±0.7	97.0±0.4
1.0	0.00	1.00	50.0	100.0	51.2±0.6	96.8±0.5

Tabulka 3.1: Tabulka průměrných hodnot fidelit klonování naměřených pomocí symetrizace pro různé hodnoty propustnosti t^2. Koeficienty a a b jsou parametry asymetrie, F_{1T} a F_{2T} značí teoretický hodnoty fidelit. Experimentální hodnoty fidelit jsou vyváženy na účinnost detektorů, jsou průměrem ze šesti měření pro různé vstupní stavy.

Kapitola 4

Fázově kovariantní klonování – experimenty

K prvním optickým realizacím fázově kovariantního klonování došlo v roce 2005. Zhao a kol. vytvořili zařízení pro útok na kvantovou kryptografii pomocí tzv. teleklonování [53]. Druhým experimentem Sciarrina a De Martiniho [40, 56] bylo fázově kovariantní $1 \rightarrow 3$ klonování. Oba experimenty použily dvojitý průchod čerpacího pulzu skrz nelineární krystal typu II k vygenerování čtyř fotonů, přičemž dva z nich poté spolu interferovaly na děliči svazků. Stejnou konfiguraci pro fázově kovariantní $1 \rightarrow 3$ klonování použil i Xu a kol. ve svém článku z roku 2008 [57]. V roce 2017 vytvořila argentinská skupina zařízení simulující fázově kovariantní klonovací zařízení, kdy polarizační stav fotonu byl klonován do dráhového stavu toho stejného fotonu [58]. Všechny ostatní mě známé realizace $1 \rightarrow 2$ fázově kovariantního klonování byly provedeny v Olomouci a budou popsány v tomto textu.

Jak metoda stimulované emise, tak HOM klonování mají jednu velkou nevýhodu. Vzniklé klony jsou ve stejném prostorovém módu (ve stejném čase na stejném místě). Neexistuje metoda, jak tyto fotony od sebe deterministicky oddělit. Můžeme použít vyvážený dělič svazků (stejně jako v případě hybridního zařízení), nicméně úspěšnost oddělení bude pouze 1/2, přičemž ve čtvrtině případů půjdou do jednoho výstupu oba klony a ve čtvrtině případů žádný.

Oproti tomu, fázově kovariantní klonování pomocí speciálního děliče svazků je úspěšné jen v případě, kdy je po jednom fotonu na každém výstupu. Pro různé režimy klonování musí mít tento dělič jiné vlastnosti. Obecně je potřeba dosáhnout libovolného dělicího poměru nezávisle pro dvě ortogonální báze. V případě dráhového kódování lze použít vláknový dělič s proměnným dělícím poměrem v obou prostorových módech.

Pro polarizační kódování nám stačí jeden dělič, ten ale musí mít nevyvážený dělicí poměr různý pro H a V polarizaci. Takové děliče se dají vyrobit na zakázku, různého dělicího poměru je dosaženo speciální kombinací tenkých vrstev. Ne vždy se ale podaří vyrobit dělič s požadovaným dělicím poměrem. Navíc, pokud chceme v experimentu dělicí poměr měnit, například pro testování různých asymetrií klonování, můžeme využít dělič s pevným dělicím poměrem a doplnit ho o polarizačně závislé ztráty. Takto můžeme dosáhnout téměř libovolného dělicího poměru pro obě bázové polarizace, cenu ovšem zaplatíme v podobě menší propustnosti děliče a tedy i celkově menší pravděpodobnosti úspěchu. Při ověřovacích testech klonovacích prototypů nás to ale nemusí trápit, ztráty

způsobené polarizační filtrací zahrneme do teoretického modelu. Metody zavedení polarizačně závislých ztrát jsou popsány v následující sekci.

4.1 Polarizačně závislé ztráty

Polarizačně závislé ztráty lze jednoduše vyvolat jen pomocí vhodně nakloněné skleněné planparalelní destičky. Další možností, kterou používáme, je složitější zařízení – polarizační interferometr.

Skleněná destička

Skleněnou destičkou, nebo obecněji jakoukoliv planparalelní průhlednou deskou s indexem lomu n, můžeme pozměnit jak dráhu svazku tak jeho polarizační stav. Podle Snellova zákona lomu,

$$\sin\vartheta = n\sin\vartheta', \tag{4.1}$$

můžeme vypočítat změnu dráhy svazku uvnitř skla. Výstupní svazek bude rovnoběžný se svazkem vstupujícím, jen bude posunut o vzdálenost $\delta = d(\sin\vartheta - \tan\vartheta'\cos\vartheta)$ ve směru otočení destičky (viz obrázek 4.1 vlevo).

Podle Fresnellových vztahů pro amplitudové koeficienty propustnosti rovnoběžné (p) a kolmé (s) složky polarizace na prvním (1) a druhém (2) optickém rozhraní skleněné destičky,

$$t_{p1} = \frac{2\cos\vartheta}{n\cos\vartheta + \cos\vartheta'} = \frac{2n\cos\vartheta}{n^2\cos\vartheta + \sqrt{n^2 - \sin^2\vartheta}}, \tag{4.2}$$

$$t_{p2} = \frac{2n\cos\vartheta'}{n\cos\vartheta + \cos\vartheta'} = \frac{2n\sqrt{n^2 - \sin^2\vartheta}}{n^2\cos\vartheta + \sqrt{n^2 - \sin^2\vartheta}}, \tag{4.3}$$

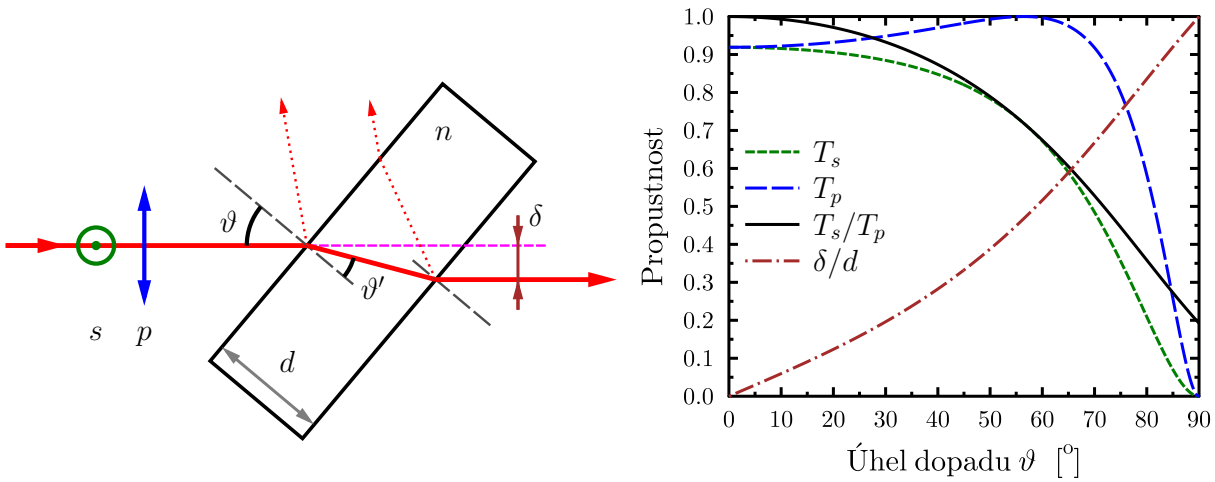
$$t_{s1} = \frac{2\cos\vartheta}{\cos\vartheta + n\cos\vartheta'} = \frac{2\cos\vartheta}{\cos\vartheta + \sqrt{n^2 - \sin^2\vartheta}}, \tag{4.4}$$

$$t_{s2} = \frac{2n\cos\vartheta'}{\cos\vartheta + n\cos\vartheta'} = \frac{2\sqrt{n^2 - \sin^2\vartheta}}{\cos\vartheta + \sqrt{n^2 - \sin^2\vartheta}}, \tag{4.5}$$

můžeme dopočítat celkové intenzitní propustnosti dvou ortogonálních složek polarizace $T_p = |t_{p1}t_{p2}|^2$ a $T_s = |t_{s1}t_{s2}|^2$:

$$T_p = \frac{16n^4\cos^2\vartheta(n^2 - \sin^2\vartheta)}{\left(n^2\cos\vartheta + \sqrt{n^2 - \sin^2\vartheta}\right)^4}, \qquad T_s = \frac{16\cos^2\vartheta(n^2 - \sin^2\vartheta)}{\left(\cos\vartheta + \sqrt{n^2 - \sin^2\vartheta}\right)^4}. \tag{4.6}$$

Grafické znázornění hodnot propustností je na obr. 4.1 vpravo. V závislosti na podílu propustností pro dvě kolmé polarizace dochází k polarizačně závislým ztrátám, tj. ztrátám různým pro různé dopadající polarizace. Z grafu je vidět, že nejvýhodnější je používat skleněnou destičku natočenou pod úhlem blízko Brewsterova úhlu $\vartheta_B = \arctan n$. Pro tento úhel jsou ztráty paralelní složky polarizace minimální, při klonování by se nezvyšovaly technologické ztráty. S malými celkovými ztrátami můžeme nastavit podíl propustností T_s/T_p až do hodnoty 0.65.



Obrázek 4.1: Vlevo průchod svazku skleněnou destičkou skloněnou pod úhlem ϑ podle vertikální osy, δ značí dráhové rozposunutí, d tloušťku, n index lomu, p a s paralelní a kolmou polarizaci vhledem k rozhraní. Vpravo grafické znázornění celkových propustností skleněné destičky s indexem lomu $n = 1.5103$ (sklo BK7) pro dvě kolmé polarizace, jejich podíl a relativní dráhové rozposunutí v závislosti na úhlu dopadu.

Nevýhodou tlustší skleněné destičky je rozposunutí svazku. Na druhou stranu, v případě tenké destičky mohou problémy působit zpětné odrazy z druhého rozhraní, které po dalším vnitřním odrazu opouští destičku rovnoběžně s původním svazkem, jen jejich intenzita je výrazně menší. Také musíme dbát na to, že se destička chová jako částečně odrazné zrcátko a do dráhy signálního svazku může odrazit nežádoucí světlo.

Pár skleněných destiček

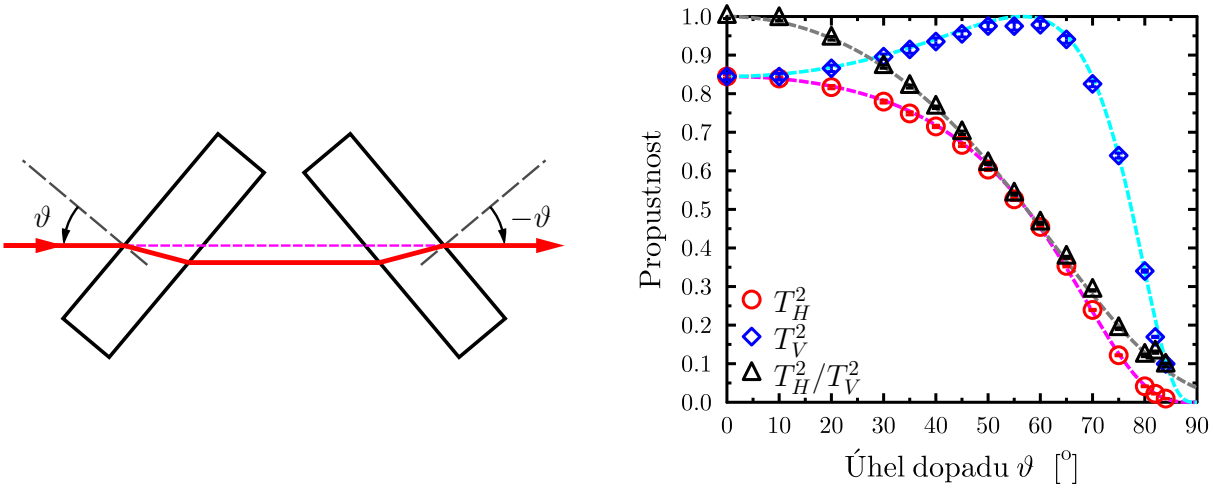
Nevýhodu rozposunutí svazku lze eliminovat použitím páru skleněných destiček otočených o opačný úhel, viz obr. 4.2 vlevo. Zdvojením ztrát dosáhneme také menší hodnoty podílu T_s/T_p při menších celkových ztrátách. V ideální oblasti blízko Brewsterova úhlu dosahuje podíl propustností hodnoty 0.4, viz graf na obr. 4.2 vpravo.

Nevýhodou tohoto uspořádání je větší počet souběžných zpětných odrazů a větší nebezpečí navázání nechtěného světla do svazku signálu.

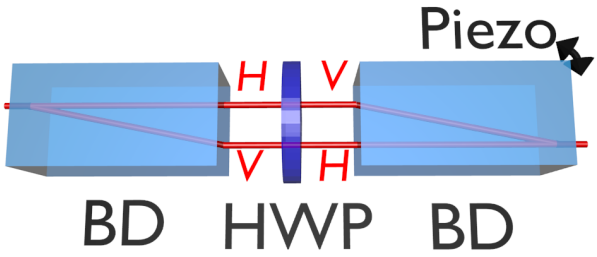
Polarizační interferometr – BDA

Polarizační interferometr je zařízení umožňující měnit propustnosti složek polarizace nezávisle v celém rozsahu od 1 až po 0. Signální svazek se na polarizátoru rozdělí na dvě ortogonální polarizační složky, nejčastěji na horizontální a vertikální složku polarizace. Na obou výstupech polarizátoru se mohou polarizační složky utlumit šedým filtrem. Následně se polarizační složky opět spojí na polarizátoru. Délky ramen interferometru musí být stejně dlouhé, jinak dochází k depolarizaci signálního svazku. Malou změnou rozdílu délek dochází k fázovému posuvu mezi H a V složkou, můžeme rotovat polarizační stav kolem vertikální osy Blochovy sféry.

Kritickou vlastností polarizačního interferometru při použití v experimentu je stabilita nastavené fáze. V tomto ohledu je výhodné použít kompaktní interferometr, v němž



Obrázek 4.2: Vlevo kompenzace dráhového rozposunutí při použití dvou sklíček otočených o opačný úhel podle horizontální osy (boční pohled). V tomto případě je kolmá k rovině dopadu (s) horizontální polarizace. Vpravo závislost propustností pro horizontální a vertikální složku polarizace a jejich podíl v závislosti na úhlu dopadu na dvojici sklíček, body značí naměřená data, čáry teoretické hodnoty.



Obrázek 4.3: Schéma polarizačního interferometru tvořeného dvojlomnými krystaly kalcitu (BD), HWP značí $\lambda/2$ destičku otočenou o 45°, Piezo potom piezoelektrický náklon, H a V horizontální a vertikální složku polarizace.

roli polarizátorů hrají dvojlomné rozposouvače svazků (BD – *beam displacer*) z kalcitu, viz obr. 4.3. V krystalu kalcitu dojde ke dvojlomu, jedna složka polarizace se šíří v nezměněném směru, kdežto druhá složka se odklání (tzv. *walk-off*). Směr odklonu závisí na směru hlavní osy dvojlomného krystalu, správným natočením krystalu můžeme docílit toho, že se vertikálně polarizovaný svazek odkloní dolů, tak jak na obrázku 4.3. Na výstupu z kalcitu jsou oba svazky paralelní, vzdáleny od sebe o 4 mm (při použití vhodně dlouhého krystalu kalcitu, například BD40 od ThorLabsu). Každý svazek zvlášť můžeme utlumit pomocí šedého filtru. Pomocí půlvlnné fázové destičky otočíme polarizace obou svazků o 90° ($H \leftrightarrow V$) a pomocí druhého totožného krystalu kalcitu spojíme svazky zpět do jedné výstupní dráhy. Výstupní polarizace je oproti vstupní otočená v planární projekci o 90°, což lze kompenzovat další půlvlnnou destičkou. Pomocí jemného piezonáklonu jednoho krystalu můžeme měnit dráhový rozdíl mezi svazky a nastavit fázi mezi H a V složku polarizace.

Nevýhodou tohoto interferometru je potřeba složité počáteční justáže, kdy se musí

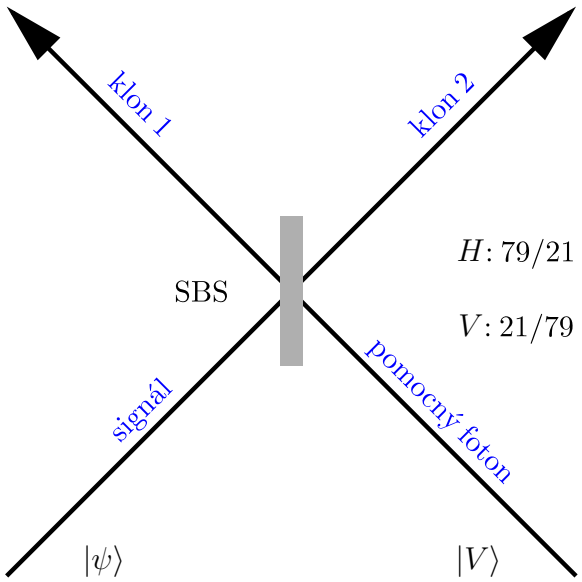
nastavit přesně rotace a náklony obou krystalů kalcitu. Pokud je celé zařízení fixní v jedné montáži, je interferometr velmi stabilní, fáze v něm se nemění v řádu dní. Další nevýhodou je potřeba zajistit dostatečnou nerozlišitelnost drah v interferometru. Aby toho bylo docíleno, musí být svazek za BDA prostorově filtrován, což děláme navázáním do jednomodového vlákna. Na druhou stranu nevadí, když místo šedého filtru použijeme částečné zaclonění H nebo V svazku hranou, narušení tvaru svazku se navázáním do jednomodového vlákna neprojeví, obnoví se původní základní prostorový mód TEM_{00}. Výraznou nevýhodou jsou technologické ztráty signálu způsobené odrazy na vstupních a výstupních plochách krystalů, které nemají antireflexní vrstvy.

Ze zmiňovaných tří metod polarizačních ztrát není žádná ideální. Pro hodnoty podílu propustností do 0.4 lze použít páru skleněných destiček pod přibližně Brewsterovým úhlem. Pro menší hodnoty podílu, popř. pro úplné utlumení jedné polarizační složky, musíme použít polarizační interferometr.

4.2 Speciální dělič

Výše zmíněné polarizační ztráty mají za úkol upravit dělící poměr děliče na požadovanou hodnotu různou pro horizontální a vertikální složku polarizace. Takový speciální dělič může být potom použit pro fázově kovariantní klonování, jak prvně navrhl J. Fiurášek [34]. Předpokládejme bezztrátový dělič, tedy koeficienty odrazivosti a propustnosti splňují podmínku $|r_{H,V}|^2 + |t_{H,V}|^2 = 1$. Symetrického klonování lze dosáhnout, je-li $r_H = t_V$ a $t_H = -r_V$. Omezíme-li se pouze na případy, kdy bude na obou výstupech děliče po jednom fotonu (obr. 4.4), bude mít transformace děliče tvar

$$|V_S\rangle|V_A\rangle \to (r_V^2 - t_V^2)|VV\rangle, \qquad |H_S\rangle|V_A\rangle \to r_V t_V \left(|HV\rangle + |VH\rangle\right).$$



Obrázek 4.4: Fázově kovariantní klonování na speciálním děliči. Situace, kdy je na každém výstupu po jednom fotonu, nastane s pravděpodobností 1/3.

zde symbol S náleží vstupnímu klonovanému qubitu (signál) a $|V_A\rangle$ značí vertikálně polarizovaný pomocný foton (ancila)ˇ. Tato transformace je až na záměnu H a V stavů podobná s transformací fázově kovariantního kloneru (2.7). Pro úplnou shodu už stačí jen zajistit, aby $\sqrt{2}r_V t_V = r_V^2 - t_V^2$, tedy aby $r_V^2 = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right) \approx 0.79$ a $r_H^2 \approx 0.21$. Tato transformace nastane podmíněně jen v případě, kdy bude po jednom fotonu na každém výstupu. To se stane s pravděpodobností úspěchu $P_{succ} = 2r_V^2 t_V^2 = 1/3$.

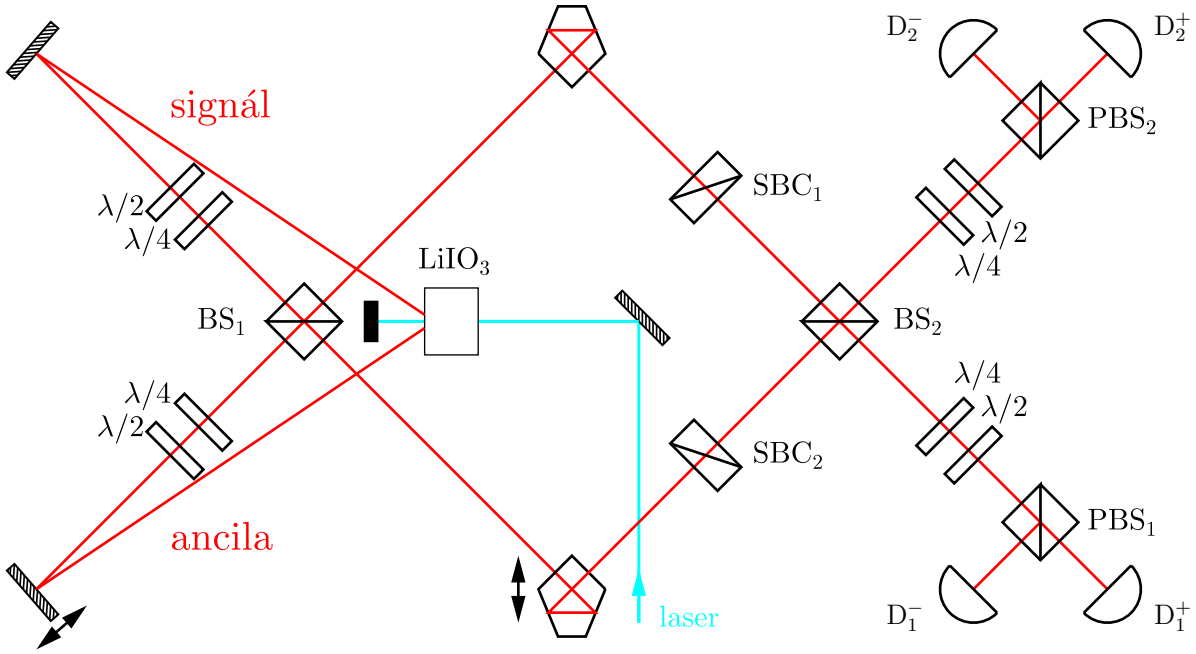
Dělič s tímto speciálním dělicím poměrem nebylo snadné ze začátku vyrobit. Proto se naše první experimentální realizace snažila speciální dělič nahradit interferometrem. V druhém případě jsme použili nastavitelné vláknové děliče, to ale znamenalo přejít k dráhovému kódování. Mezitím nám dorazil speciální dělič vyrobený na zakázku, neměl ale požadovaný dělicí poměr. Ten jsme tedy upravili pomocí polarizačně závislých ztrát – pomocí natočených sklíček nebo pomocí polarizačních interferometrů. V posledním realizovaném experimentu jsme se opět vrátili k interferometru, jen jsme tentokrát zvolili jinou konstrukci a snažili jsme se vyvarovat předchozích chyb.

4.2.1 Nevyvážený dělič pomocí Machova-Zehnderova interferometru

Tímto experimentem jsem končil v rámci svého doktorského studia, je popsaný v dizertaci [A20]. Až následně byl tento publikován v přehledovém článku [A4]. V tomto textu stručně popíšu experimentální sestavu a shrnu její nedostatky a důsledky, které jsme z toho vyvodili.

V této realizaci zařízení pro fázově kovariantní klonování jsme se pokusili nahradit nevyvážený dělič pomocí Machova-Zehnderova interferometru. Změnou fáze v jednom rameni se dá lehce měnit intenzitní propustnost a odrazivost interferometru. Samotný interferometr by byl ale nezávislý na polarizaci, tj. dělící poměr by byl stejný pro všechny polarizace. Polarizační závislost lze zavést pomocí polarizačně závislé fázové změny v ramenech interferometru. Potom bude interferometr jako celek se změnou fáze jinak dělit různé složky polarizace. Tuto polarizačně závislou fázovou změnu lze implementovat pomocí Soleilova-Babinetova kompenzátoru (SBC). Aby byl interferometr jako dělič symetrický, musí být kompenzátory v obou ramenech a na nich nastavené rozdíly fází musí být opačné. Podle velikosti fázového rozposuvu, které kompenzátory zavedou, a pomocí celkové změny fáze lze nastavit interferometr tak, aby se choval jako dělič s libovolným dělícím poměrem různým pro H a V polarizaci.

Schéma klonovacího zařízení využívající interferometr jako dělič je vyobrazen na obr. 4.5. Fotony, použité jako *signál* ke klonování a pomocná *ancila* s vertikální polarizací, vznikají v nelineárním procesu SPDC v krystalu lithium iodátu, který byl čerpán kontinuálním laserovým svazkem na vlnové délce 413 nm. Průřez čerpacího svazku byl téměř dokonale TEM_{00}. Při nelineární interakci by měly vznikající fotony v ideálním případě převzít jeho prostorové vlastnosti. V reálné situaci jsou ale fotonové páry na výstupu z krystalu v mnoha prostorových a spektrálních módech. V tomto experimentu nebyla provedena žádná filtrace na tyto prostorové a spektrální módy krom spektrálního hranového filtru, který na detektory nepustil rozptýlené laserové záření, a kruhových clonek před navázáním do mnohamodového optického vlákna vedoucího na jednofotonový detektor. Při nastavování experimentu se hledal ideální prostorový i spektrální překryv fotonů na děliči jen pomocí náklonů zrcátka za krystalem a děliče. Jediným ukazatelem kvality ne-



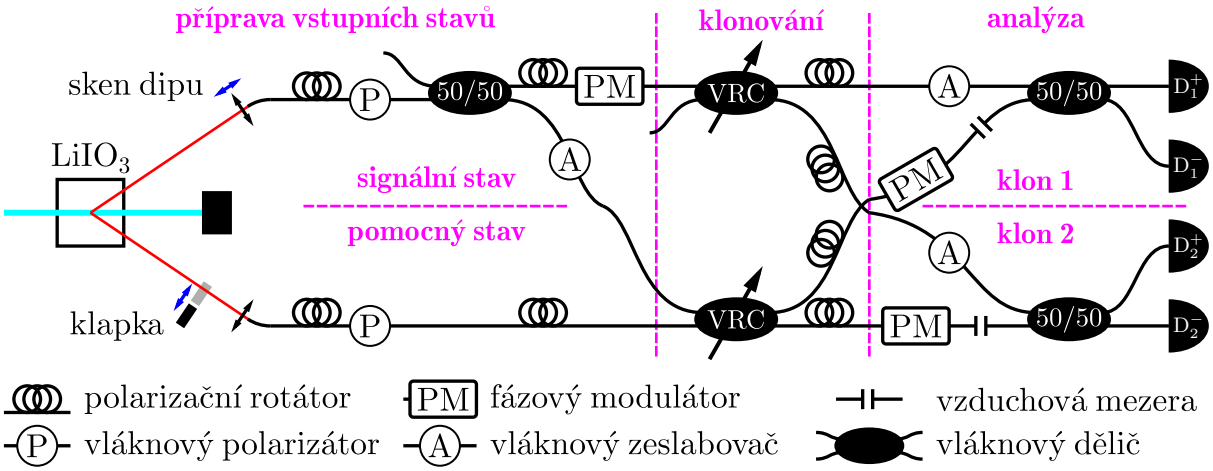
Obrázek 4.5: Klonovací zařízení s Machovým-Zehnderovým interferometrem namísto speciálního děliče. $LiIO_3$ - nelineární krystal pro generaci fotonových párů, BS - polarizačně nezávislý dělič svazků, PBS - polarizátor, $\lambda/2$, $\lambda/4$ - fázové destičky, SBC - Soleilův-Babinetův kompenzátor, D - detektor.

rozlišitelnosti fotonů za děličem byla vizibilita HOM zářezu [9]. Za těchto podmínek mohla jakákoliv změna geometrie vést ke zlepšení prostorového překryvu fotonů, ale zároveň je mohla od sebe spektrálně vzdalovat. V dalších experimentech jsme důsledně oddělovali část zdrojovou (SPDC a navázání fotonů do jednomodových vláken) a část interferenční. Tím jsme mohli nezávisle optimalizovat spektrální vlastnosti fotonů ze zdroje a překryv fotonů na děliči.

Hlavně díky značné rozlišitelnosti fotonů se pomocí tohoto zařízení nedalo klonovat s fidelitou lepší, než je semiklasický limit $F = 0.75$. Nicméně se ověřila nezávislost fidelit klonů na fázi vstupního stavu (stavy z rovníku Blochovy sféry) a průběh fidelit pro stavy z poledníku Blochovy sféry. Pravděpodobnost úspěchu zařízení odpovídala teoretickému předpokladu [A4, A20]. Bez ohledu na dosaženou kvalitu výsledků lze nicméně říct, že interferometr simulující dělič s nastavitelným dělicím poměrem nezávisle pro dvě bázové polarizace je ideální součást lineárně optických zařízení, je univerzální a bez dodatečných ztrát. Jeho nevýhodou je ale časová stabilita délek ramen interferometru a ztráty v obou ramenech. SBC tvoří dva klíny a jeden kompenzační krystal, celkem šest rozhraní, která neměla antireflexní povrstvení. Stejně tak bez antireflexe byla i rozhraní pentagonů. A na každém z těchto rozhraní docházelo k téměř desetiprocentním ztrátám.

4.2.2 Celovláknové klonovací zařízení

Celovláknové klonovacího zařízení [A4, A5] je prvním krokem k sestrojení zařízení na bázi vlnovodné integrované optiky. Z experimentálního hlediska nás lákal jak ideální překryv prostorových módů interagujících fotonů, tak i možnost spojitě a beze ztrát měnit dělicí



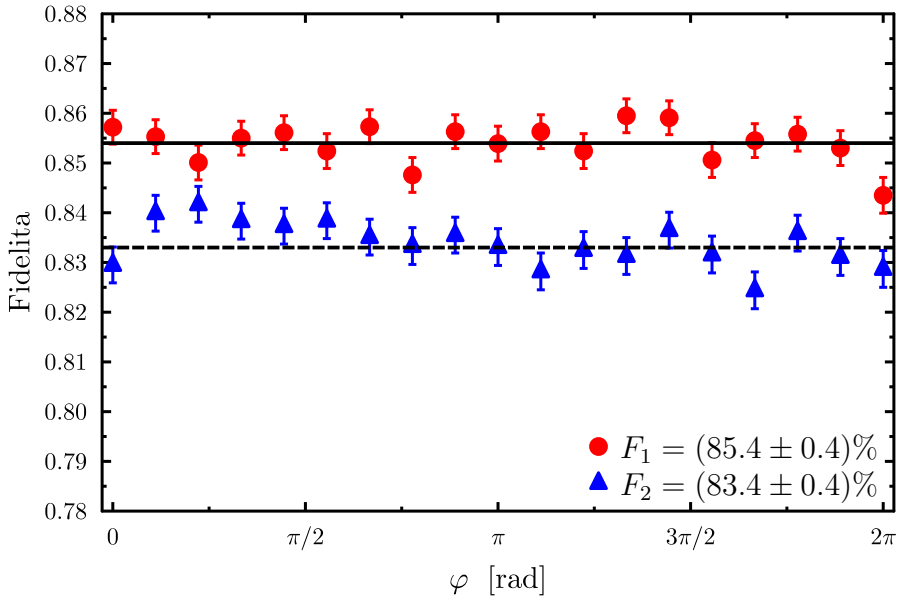
Obrázek 4.6: Celovláknové klonovací zařízení, zde bylo využito dráhového kódování qubitů – foton v horním vláknu značí stav $|0\rangle$, v dolním stav $|1\rangle$. Použité vláknové děliče měly buď pevný dělící poměr 50/50 nebo se dělící poměr mohl nastavit (VRC). D značí detektor, projektovalo se buď na stav signálního fotonu (D^+) nebo na stav k němu ortogonální (D^-).

poměr nevyváženého děliče. Jelikož bylo použito optických vláken nezachovávajících polarizační stav, muselo se použít dráhové kódování qubitu.

Schéma zařízení je na obrázku 4.6. Zdroj fotonových párů je totožný s předchozím experimentem. Jen byl navíc použit vláknový polarizátor (P) pro zvýšení čistoty separabilních vstupních stavů. Do dráhy zakódovaný kvantový stav signálního fotonu je připraven pomocí vyváženého vláknového děliče (50/50), přesnější vyvážení poměru mezi stavem $|0\rangle$ a $|1\rangle$ šlo ztrátově nastavit pomocí vláknového zeslabovače (A). Při měření jsme se omezili jen na vstupní stavy z rovníku Blochovy sféry, tedy vyvážený poměr bázových stavů. Fáze mezi nimi byla nastavena pomocí fázového modulátoru (PM). Ve schématu je dodržována konvence, kdy detekce fotonu v horním vláknu značí stav $|0\rangle$ a detekce ve spodním vláknu stav $|1\rangle$. Kvantový stav pomocného fotonu byl nastaven pevně na stav $|1\rangle$, tedy foton ve spodním vláknu.

K procesu klonování dochází na dvou vláknových děličích s proměnným dělícím poměrem (*Variable ratio coupler* - VRC). Tyto zastávají funkci speciálního děliče s dělícím poměrem různým pro dva bázové stavy. Horní dělič měl nastaveny parametry r_1 a t_1, spodní r_2 a t_2. Po klonování následuje stavová analýza obou klonů. K té byl opět potřeba vyvážený dělič a fázový modulátor. Projektovalo se opět na stav signálního fotonu a na stav k němu ortogonální. Při zpracování výsledků se použily dvě metody. První opravovala změřené fidelity podle rozdílných kvantových účinností detektorů, které se předtím určily pomocí definovaně zeslabeného klasického signálu změřeného kalibrovaným detektorem. Druhá metoda byla sekvenční, fidelita se určila jen z detekcí na jednom páru detektorů, na který se projektovaly různé kombinace signálního stavu a stavu k němu ortogonálnímu. Obě metody dávaly stejné výsledky.

Celé zařízení se skládá ze tří interferometrů. Prvním je dvoufotonový Hongův-Ouův-Mandelův interferometr, k interferenci dochází na spodním děliči VRC. Délka ramen se vyvažovala pomocí posuvu vláknového navazovače ve zdroji (sken dipu). Signální vyvážený dělič a dva děliče v analýze tvoří dva propojené Machovy-Zehnderovy interfero-



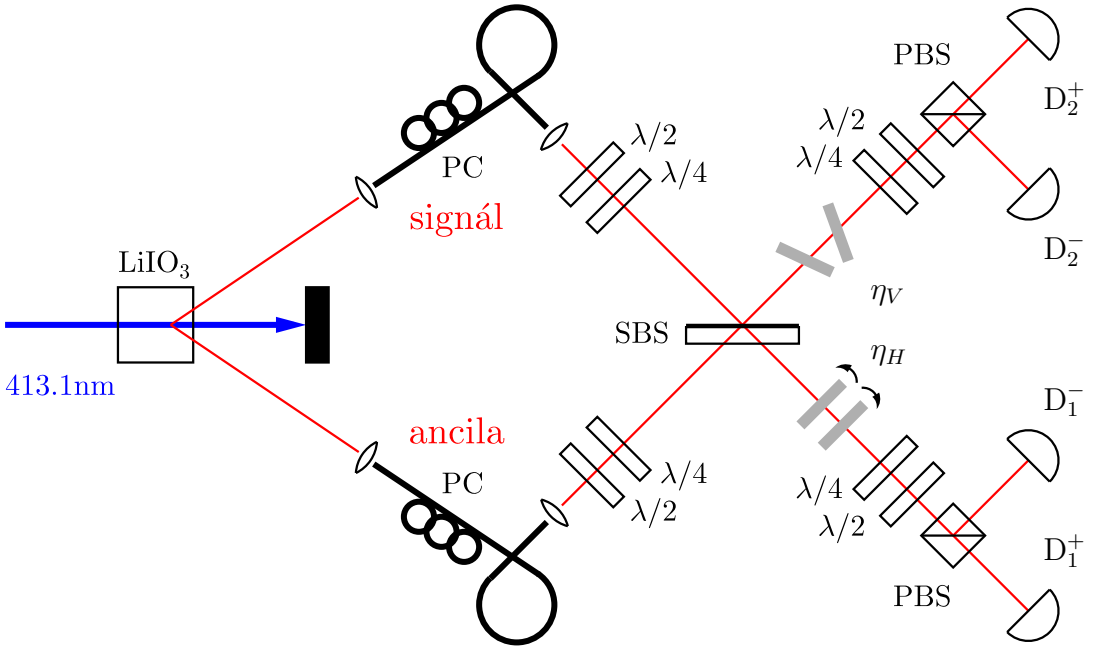
Obrázek 4.7: Závislost fidelit klonů na parametru φ pro rovníkové stavy ($\vartheta = \pi/2$) celovláknového zařízení. Čísla vypsaná v legendě jsou průměrem přes všechny měřené hodnoty.

metry. Délky ramen byly vyváženy pomocí vzduchových mezer. Změny fáze φ signálního stavu a nastavení správné projekce se provádělo pomocí fázových modulátorů. Ty pracují na bázi lineárního elektrooptického jevu, kdy se se změnou napětí na krystalu změní jeho index lomu. Proces funguje dobře jen pro jednu polarizaci, součástí každého fázového modulátoru je polarizátor. Kvůli minimalizaci ztrát je tedy před každým fázovým modulátorem (i vláknovým polarizátorem) polarizační rotátor. Další polarizační rotátory byly potřeba pro dosažení polarizačního překryvu na vyvážených děličích v analýze výstupních stavů.

Komplexnost celovláknového zařízení byla důvodem složitosti prvotního nastavení. V první fázi byly vláknové děliče s proměnnými dělícími poměry nastaveny na vyvážený dělící poměr. Zkontrolovala se nerozlišitelnost fotonů pomocí HOM dipu (typické vizibility 98 %). Vyrovnáním délek ramen, ztrát a polarizací v ramenech se maximalizovala interference obou MZ interferometrů na jednofotonovém signálu, pomocný foton byl zablokován klapkou ve zdroji, maximální dosažené vizibility byly 97 %. Správné nastavení dělícího poměru a vyvážení ztrát pro přípravu signálního qubitu se provedlo pomocí laserové diody.

Naměřené hodnoty fidelit pro rovníkové stavy jsou na grafu v obr. 4.7, průměrné hodnoty $F_1 = 0.854 \pm 0.004$ a $F_2 = 0.834 \pm 0.004$ jsou nad limitem univerzálního klonování (0.833). U tohoto zařízení jsme neměřili fidelity pro poledníkové stavy ($\varphi = 0$, $\vartheta \in [0; \pi]$).

Celovláknové klonovací zařízení těží z výhody vláknových děličů VRC. Ty mohou měnit dělicí poměr libovolně mezi výstupními módy. Tím můžeme přesně nastavit dělicí poměr pro fázově kovariantní klonování. Není potřeba vyrovnávat dělící poměr pomocí ztrát. Také lze bezztrátově měnit asymetrii zařízení a pravděpodobnost úspěchu bude optimální, tj. maximálně dosažitelná v rámci lineární optiky. Cena, kterou jsme museli za



Obrázek 4.8: Klonovací zařízení se speciálním děličem, PC - polarizační rotátor, SBS - speciální dělič, PBS - polarizátor, D - navázání do mnohamodového vlákna a detektor, $\lambda/2$ a $\lambda/4$ – půlvlnná a čtvrtvlnná fázová destička, ν_V a ν_H - nakloněná sklíčka způsobující polarizačně závislé ztráty.

tyto výhody zaplatit, byla ale vysoká. Dráhové kódování si vyžádalo sestavu se dvěma propojenými MZ interferometry. Během měření musela být zachována fázová stabilita těchto interferometrů. Stabilizace byla jak pasivní, teplotní polystyrenový kryt, tak aktivní. Po třech sekundách se muselo měření přerušit a aktivně opravit změnu fáze v obou interferometrech. Hodnoty pravděpodobnosti úspěchu jsou oproštěny od tzv. technologických ztrát. Mezi tyto ztráty zahrnujeme účinnost vyvázání a navázání do optických vláken ve vzduchových mezerách a ztráty všech vláknových komponent. Především ztráty fázového modulátoru, kde se fotony navazují do vlnovodné struktury krystalu, nejsou nezanedbatelné. Z původních několika set fotonových párů za sekundu na vstupu projde zařízením typicky 60 párů (při symetrickém klonování).

4.2.3 Speciální dělič se skleněnými destičkami

Díky pokroku v technologiích mohla být vytvořena struktura tenkých vrstev, která téměř splňovala požadované vlastnosti pro fázově kovariantní klonování. Firma EKSMA nám v roce 2005 na zakázku vyrobila dělič s odrazivostmi $R_V = 75.1\,\%$ a $R_H = 18.0\,\%$. V tomto případě jsme dělicí poměr upravili pomocí dvou párů skleněných destiček. Výsledky měření pomocí této experimentální sestavy (viz obr. 4.8) byly publikovány v článcích [A1, A4, A6].

Páry fotonů z nelineárního krystalu byly prostorově filtrovány jednomodovými optickými vlákny. Změnu polarizačního stavu, kterou způsobily, kompenzovaly polarizační rotátory (PC). Kvantový stav klonovaného (signál) a pomocného (ancila) fotonu byl nastaven pomocí fázových destiček. Poté oba fotony interferovaly na speciálním děliči. Za ním byla situována nakloněná skleněná sklíčka, jejichž propustnosti η_H a η_V byly po-

larizačně závislé. Tato sklíčka v prvé řadě korigovala neideální dělící poměr, v druhé řadě měnila efektivní dělící poměr celé soustavy tak, aby zařízení klonovalo asymetricky. Pak následovala polarizační analýza dvoufotonového výstupního stavu. Fázové destičky byly v motorizovaných rotacích, což umožnilo strojové ovládání měření. Za polarizačním děličem následoval spektrální hranový filtr, clonka, s níž se vyrovnávala detekční účinnost, a mnohamodové vlákno vedoucí na detektor.

Měření bylo automatizováno, což umožnilo získat více hodnot bez rizika chyby při manuálním nastavování rotací u fázových destiček. Provedla se úplná tomografie procesu, kdy se pro reprezentativní vstupní signální stavy provedlo úplné tomografické měření polarizace výstupních dvoufotonových stavů. Z těchto dat byla vybrána měření potřebná k přímému určení fidelit klonů, tedy když se projektovalo na stavy vstupního signálu a na stav ortogonální. Navíc se pomocí metody maximální věrohodnosti (*Maximum likelihood*) rekonstruovala Choiova-Jamilkowskeho matice procesu [59, 60], z ní se pak určila fidelita klonovacího procesu.

Pravděpodobnost úspěchu se spočetla jako podíl všech koincidenčních událostí v dipu, tj. signál a ancila se na děliči časově překrývali, a mimo dip, kdy se fotony na děliči nepotkaly ve stejném čase a o výstupním portu se rozhodovaly náhodně. Tento podíl byl korigován faktorem $Q = (T_V^2 + R_V^2 + T_H T_V + R_H R_V)/2 = 0.484$, který zohledňuje asymetrii speciálního děliče. Takto určená hodnota pravděpodobnosti úspěchu je oproštěna od všech technologických ztrát, jako jsou ztráty při odrazech na optických komponentách, nedokonalé navázání do vláken a jiné.

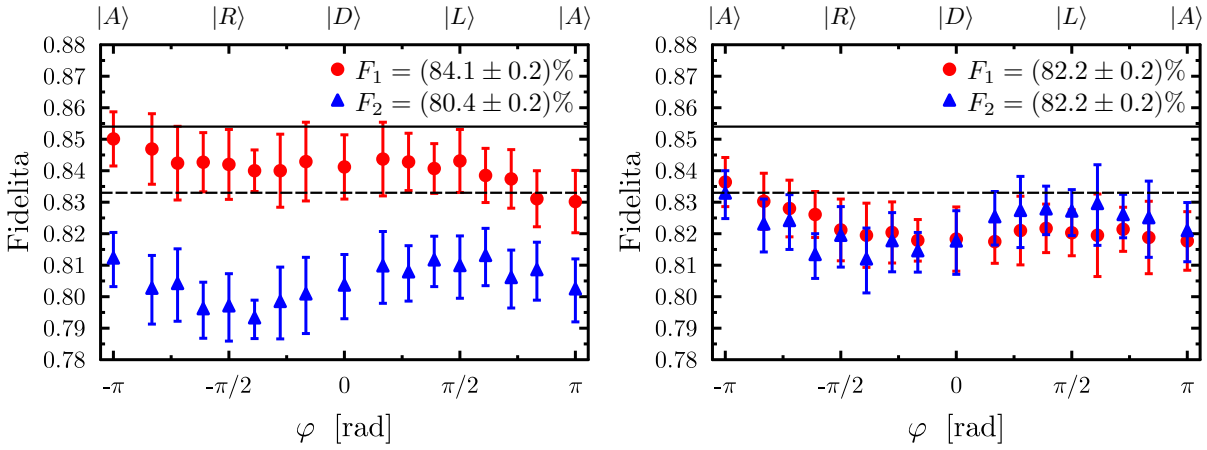
S touto experimentální sestavou se provedlo několik sad měření zvlášť v případě bez použití skleněných destiček (GP), kdy neideální speciální dělič klonoval asymetricky, a se skleněnými destičkami. V prvním případě jsou výsledné fidelity klonů pro rovníkové qubity ($\vartheta = \pi/2$) znázorněny v grafu na obr. 4.9 vlevo. Hodnoty $F_1 = (84.1 \pm 0.2)\%$ a $F_2 = (80.4 \pm 0.2)\%$ jsou určeny zprůměrováním hodnot přes všechna měřená φ. Pravděpodobnost úspěchu klonování bez ztrátových destiček byla $P_{succ} = (31.2 \pm 0.8)\%$.

V druhém případě ztrátová sklíčka srovnala hodnoty fidelit obou klonů za cenu menší pravděpodobnosti úspěchu. Náklon skleněných destiček byl nastaven tak, aby byla splněna podmínka $\frac{\eta_V}{\eta_H} = \frac{|r_H r_V|}{|t_H t_V|}$. Naměřené hodnoty jsou vyneseny v grafu na obr. 4.9 vpravo, průměrné hodnoty jsou stejné, $F_1 = F_2 = (82.2 \pm 0.2)\%$. Pravděpodobnost úspěchu klonování poklesla z důvodu polarizačně závislých ztrát na hodnotu $P_{succ} = (28.8 \pm 0.1)\%$.

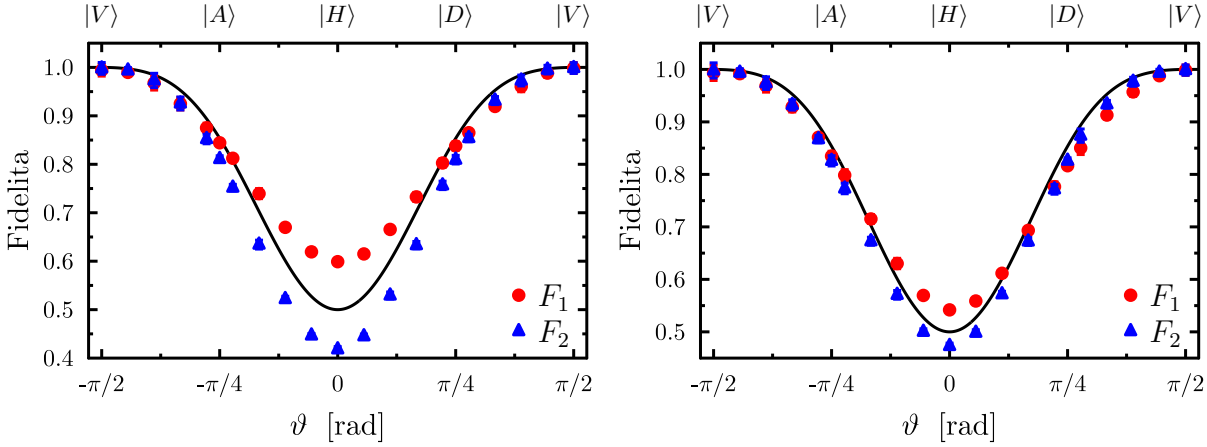
V grafech na obr. 4.10 je znázorněn průběh naměřených hodnot pro různé hodnoty ϑ (poledníkové qubity). Ancila měla po celou dobu vertikální lineární polarizaci, proto fidelita klonů klesá až na jednu polovinu. V případě bez kompenzace sklíčky je patrná výrazná asymetrie zařízení.

Je zřejmé, že se průměrná fidelita pohybuje na hranici univerzálního klonování, spíše pod ní. To můžeme přičítat nedokonalému prostorovému překryvu, prostorový mód fotonů vyfiltrovaný jednomodovými vlákny před děličem byl optickými komponentami narušen. Tím se staly fotony částečně rozlišitelné a neinterferovaly dokonale. Další problém tkvěl v koincidenční elektronice. Při tomto experimentu se k filtraci současných detekcí využil modul s minimálním rozsahem koincidenčního okna 20 ns. Měření byla tedy ovlivněna nezanedbatelným počtem náhodných koincidenčních událostí.

Z tomografických dat naměřených v případě bez filtrace skleněnými destičkami byla estimována tomografie procesu s fidelitou 93 %, tedy zařízení fungovalo jako ideální fázově



Obrázek 4.9: Závislost fidelit klonů na parametru φ pro rovníkové stavy ($\vartheta = \pi/2$) v případě fázově kovariantního klonování bez kompenzace (vlevo) a s kompenzací sklíčky (vpravo). V obou případech měl pomocný foton vertikální polarizaci. Čísla v legendě jsou průměry přes všechny hodnoty φ. Plná čára představuje fázově kovariantní a přerušovaná univerzální klonovací limit.

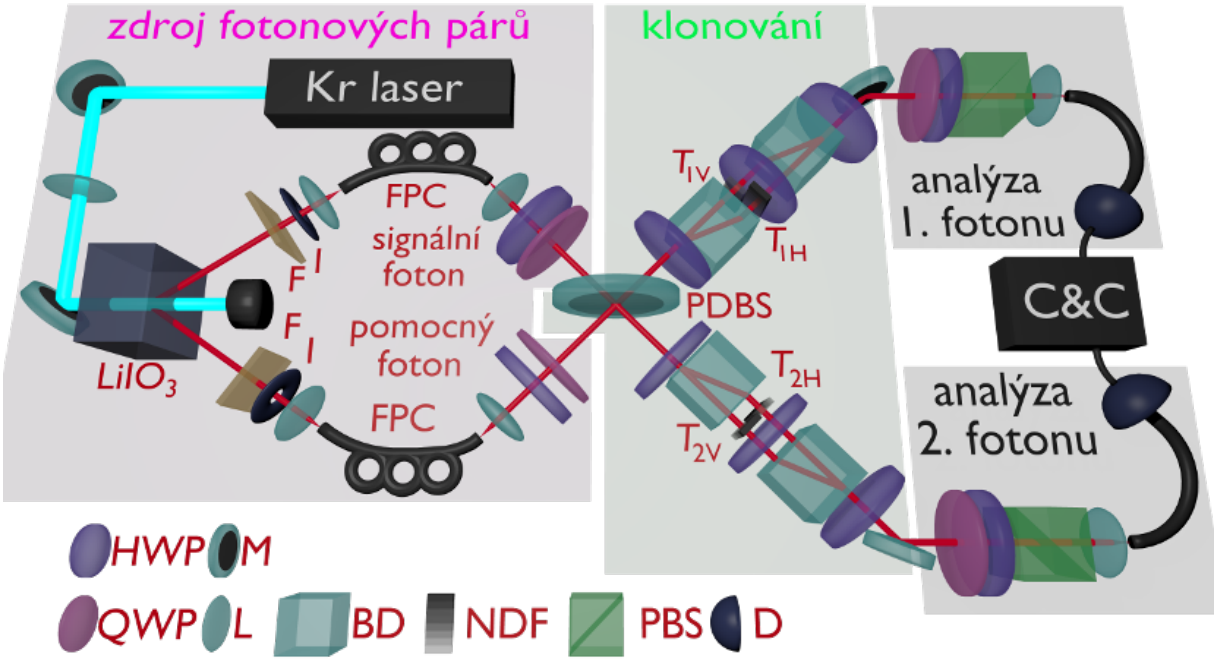


Obrázek 4.10: Závislost fidelit klonů na úhlu ϑ pro $\varphi = 0$ (stavy z poledníku Blochovy sféry) pro fázově kovariantní klonování bez kompenzace (vlevo) a s kompenzací sklíčky (vpravo). Pomocný foton byl stále ve stavu lineární vertikální polarizace. Plná čára představuje teoretickou předpověď symetrického klonování.

kovariantní kloner jen na 93 %. Když byl neideální dělič kompenzován sklíčky, vzrostla fidelita procesu na 94 %. Tomografické měření též odhalilo, že je jeden výstup zařízení fázově posunut, což snižovalo fidelitu procesu. Tomuto snížení by se dalo zabránit fázovou kompenzací na daném výstupu.

4.2.4 Polarizačně závislé ztráty pomocí interferometru

Použití skleněných destiček pro zavádění polarizačně závislých ztrát je efektivní jen pro omezený rozsah poměru propustností. Jakmile je úhel dopadu na destičky větší než je Brewsterův úhel, dochází k výrazným celkovým ztrátám. Klonovací zařízení s polarizačními interferometry pro kontrolu polarizačně závislých ztrát má oproti předchozí



Obrázek 4.11: Klonovací zařízení se speciálním děličem a polarizačně závislými ztrátami pomocí polarizačního interferometru BDA, $LiIO_3$ - nelineární krystal, F - spektrální filtr, I - clona, FPC - polarizační rotátor, PDBS - speciální dělič, HWP a QWP – půlvlnná a čtvrtvlnná fázová destička, M - zrcadlo, L - čočka, BD - rozposouvač svazků (krystal kalcitu), NDF - šedý filtr s proměnnou propustností, PBS - polarizátor, D - navázání do jednomodového vlákna a detektor, C&C - koincidenční elektronika.

implementaci se sklíčky jednu velkou výhodu, je schopno kontrolovat propustnost pro H nebo V složku polarizace v celém rozsahu od 1 po 0 bez toho, aniž bychom zeslabovali složku druhou. Tím jsme mohli ztrátově upravovat dělící poměr speciálního děliče tak, aby se s ním daly klonovat různé sady vstupních stavů. Výsledky měření pomocí tohoto zařízení byly publikovány v článcích [A8–A11].

Nevýhodou této implementace je složitější aparatura, kdy na obou výstupech speciálního děliče byl kompaktní polarizační interferometr. Vylepšením bylo pro změnu použití prostorové filtrace jednomodovými vlákny před detektory, tím jsme zvýšili nerozlišitelnost fotonů na detektoru. Pro výběr současných detekcí se použily elektronické moduly TAC a SCA s koincidenčním oknem 2 ns, tím se omezily náhodné koincidence. Užitím pouze dvou detektorů na průchod za polarizátory jsme eliminovali vliv rozdílných účinností detektorů, tomografické měření ale trvalo čtyřikrát déle.

Schéma experimentu je vykresleno na obr. 4.11. V polarizační interferometru (BDA – *Beam Divider Assembly*) se filtrovala vždy jen jedna polarizace, pomocí půlvlnných fázových destiček před a za BDA se otáčela polarizace tak, aby byla zeslabena ta správná složka a aby na výstupu z BDA byl kompenzována vnitřní fázová destička.

Nastavením různého efektivního dělícího poměru děliče pro dvě polarizační složky jsme schopni přepínat klonovací zařízení do odlišných režimů tak, abychom optimálně klonovali různé třídy vstupních stavů. Pokud nemáme žádnou apriorní informaci o vstupním stavu, musíme použít univerzální klonování. Pokud víme, že jsou klonované stavy rozloženy na jedné polokouli Blochovi sféry, můžeme použít fázově kovariantní klonování. Pokud jsou

	ideální komponenty	reálný případ
propustnost pro H pol.	$\mu = \frac{1}{2}\left(1+\frac{1}{\sqrt{3}}\right) \approx 0.789$	0.76
propustnost pro V pol.	$\nu = \frac{1}{2}\left(1-\frac{1}{\sqrt{3}}\right) \approx 0.211$	0.18
kompenzace na reálný dělič	$\omega = \frac{\mu\nu}{(1-\mu)(1-\nu)} = 1$	0.70
filtrování v závislosti na ancile	$\kappa = \frac{2\mu-1}{1-2\nu} = 1$	0.81

Tabulka 4.1: Hodnoty propustností μ a ν ideálního a reálného děliče, míra kompenzace ω na reálný neideální dělič a velikost filtrování κ v důsledku použití ancily s různou polarizací.

	$\|H\rangle$ ancila		$\|V\rangle$ ancila	
	ideál	realita	ideál	realita
$T_{1\mathrm{H}}$	1	1	τ	τ
$T_{1\mathrm{V}}$	τ	$\kappa\tau$	1	κ
$T_{2\mathrm{H}}$	1	1	τ	$\omega\tau$
$T_{2\mathrm{V}}$	τ	$\kappa\omega\tau$	1	κ

Tabulka 4.2: Hodnoty polarizačně závislých ztrát nastavených na výstupech speciálního děliče.

vstupní stavy rozloženy podél rovnoběžek symetrických vůči rovníku, použijeme zrcadlově fázově kovariantní klonování. S použitím objemového děliče, který by byl schopen měnit odrazivost a propustnost nezávisle pro H a V složku polarizace, bychom dokázali měnit klonovací režim s maximální možnou pravděpodobností úspěchu. V tomto případě jsme dělící poměr speciálního děliče měnili opět pomocí přidaných polarizačně závislých ztrát.

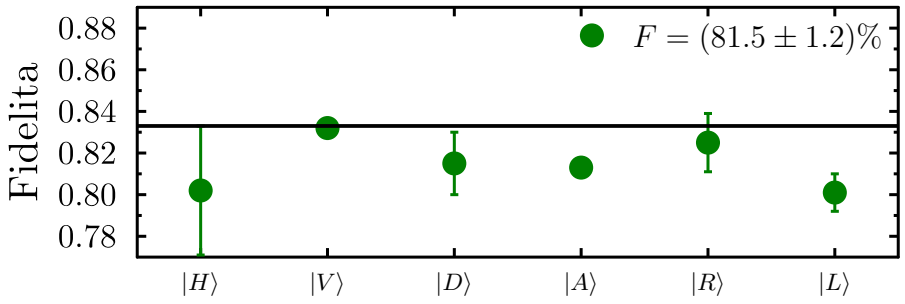
Pro fázově kovariantní klonování jsou ideální hodnoty propustnosti děliče $\mu \approx 0.789$ pro horizontální polarizaci a $\nu \approx 0.211$ pro vertikální polarizaci. Vyrobený dělič měl ale dělící poměr trochu odlišný, musel se tedy poupravit polarizačními ztrátami, viz tabulka 4.1.

V případě zrcadlově fázově kovariantního klonování se zaváděly další ztráty v závislosti na vzdálenosti klonovaného stavu $|\psi\rangle = \cos\vartheta/2|H\rangle + e^{\imath\varphi}\sin\vartheta/2|V\rangle$ od rovníku,

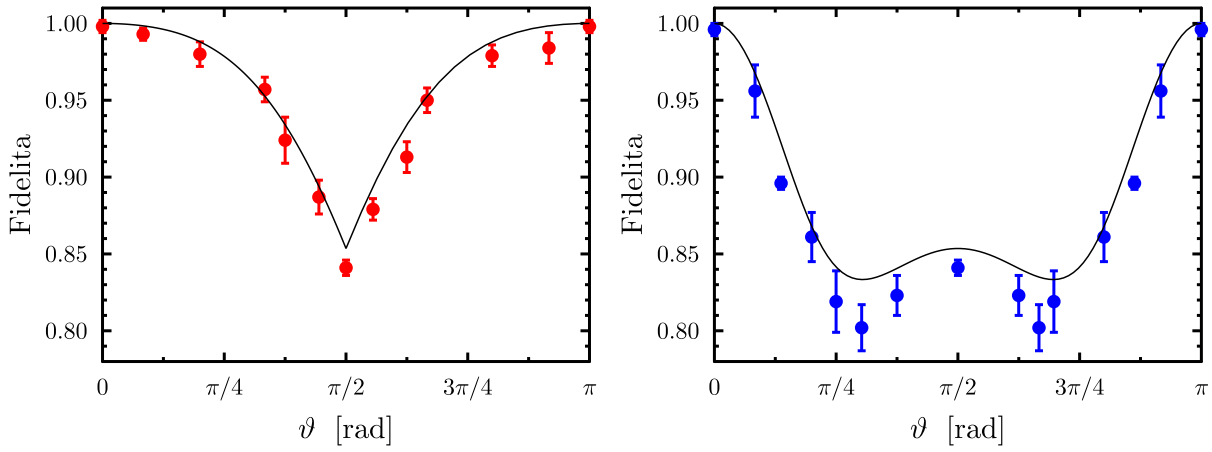
$$\tau = 1 - \frac{2\cos^2\vartheta}{\sqrt{S}+\cos^2\vartheta}, \quad S \ = 2 - 4\cos^2\vartheta + 3\cos^4\vartheta. \tag{4.7}$$

Aplikované ztráty na obou výstupech speciálního děliče v závislosti na polarizaci pomocného fotonu (ancily) jsou v tabulce 4.2.

Klonovací zařízení mohlo provádět i univerzální klonování, nicméně pravděpodobnost úspěchu tohoto režimu klonování nebylo optimální. Na druhou stranu, oproti HOM klonování jsme měli klony rozděleny do dvou výstupů a nemuseli je rozdělovat pomocí děliče (s úspěšností 1/2). Nastavené ztráty pro tento typ klonování byly $\tau = 0.5$, polarizace pomocného fotonu se měnila náhodně mezi H a V polarizací, v případě vertikální ancily se musela přidat fáze π mezi H a V polarizační složky klonů. V této experimentální sestavě jsme se snažili pouze o symetrické klonování, tj. fidelity obou klonů byly přibližně stejné. Průměrná hodnota obou fidelit je vykreslena v grafu na obr. 4.12 pro



Obrázek 4.12: Závislost průměru fidelit obou klonů pro univerzálního klonování na speciálním děliči s BDA. Plná čára značí teoretickou mez 0.833. Číslo v legendě je průměrem přes všechny měřené vstupní stavy.



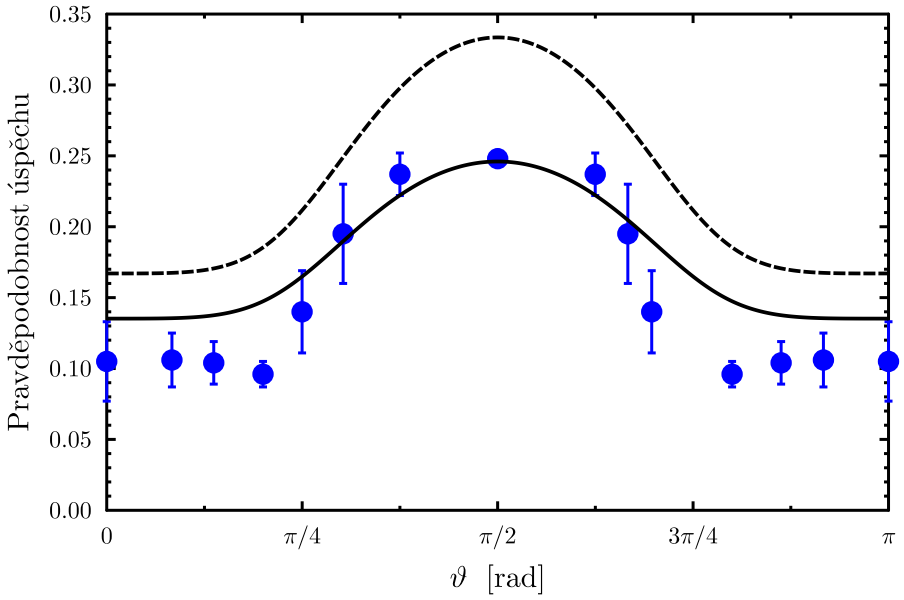
Obrázek 4.13: Hodnoty fidelity zprůměrované přes všechny měřené hodnoty φ obou klonů v závislosti na úhlu ϑ pro fázově kovariantní klonování (vlevo) a pro zrcadlově fázově kovariantní klonování (vpravo) pomocí speciálního děliče s BDA. Plná čára značí teoretickou předpověď.

šest různých vstupních polarizací signálního fotonu. Celkový průměr přes všechny vstupní stavy, $F = 0.815 \pm 0.012$, je velmi blízko teoretickému limitu (0.833).

V režimu fázově kovariantního klonování se nemusely aplikovat přidané ztráty ($\tau = 1$), pouze se korigoval neideální dělící poměr děliče. V grafu na obrázku 4.13 vlevo je znázorněna závislost průměrné fidelity klonů na úhlu ϑ. V tomto případě se průměrovaly rádoby konstantní fidelity klonů vstupních stavů s různým parametrem φ. Jako pomocný foton byl použit horizontálně lineárně polarizovaný foton pro stavy z horní polokoule Blochovy sféry a vertikálně polarizovaný foton pro stavy ze spodní polokoule.

Pro zrcadlově fázově kovariantní klonování se nastavují ztráty τ v polarizačním interferometru BDA podle rovnice (4.7). Polarizace pomocného fotonu se měnila náhodně mezi H a V. Závislost fidelity (viz obr. 4.13 vpravo) na parametru ϑ je také netriviální. Pro vstupní stavy z pólů je fidelita jednotková, klonují se ortogonální stavy. Pro stav z rovníku dostaneme fidelitu shodnou s fázově kovariantním klonováním. Stavy mezi těmito hodnotami prochází oblastí s fidelitou univerzálního klonování 0.833.

Pravděpodobnost úspěchu v zrcadlově fázově kovariantním režimu je nejvyšší pro rovníkové stavy. V případě ideálního speciálního děliče dosahuje teoretická mez hodnoty



Obrázek 4.14: Závislost pravděpodobnosti úspěchu zrcadlově fázově kovariantního klonování pomocí speciálního děliče s BDA. Černé čáry představují teoretickou předpověď, přerušovaná čára pro ideální dělič, plná čára pro náš neideální dělič.

1/3. Naměřená data odpovídají teoretické křivce upravené pro reálný dělič, viz obr. 4.14,

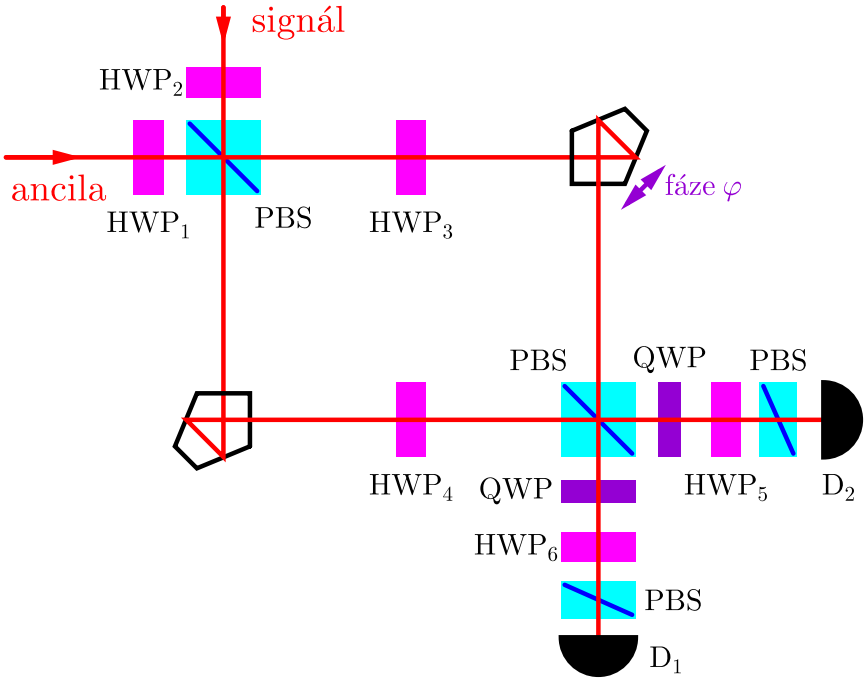
$$P_{succ} = \frac{(1-2\mu)^2}{2} + \mu\nu\tau\frac{2\mu-1}{1-2\nu}. \tag{4.8}$$

Naše realizace zrcadlově fázově kovariantního klonování byla prvním experimentálním ověřením tohoto specifického druhu klonování (a zatím jediným). Kromě článku [A8], který byl zaměřen na popis tohoto zařízení, se zrcadlově fázově kovariantní klonování použilo i pro zesilování kvantových stavů [A10], pro útok na kvantově kryptografické protokoly [A9] a ke kopírování kvantových bankovek [A11]. Tato využití klonovacího zařízení jsou podrobněji popsána v šesté kapitole.

4.2.5 Nevyvážený dělič pomocí Machova-Zehnderova interferometru – verze 2.0 pro kvantové strojové učení

Dělič s proměnným dělícím poměrem stále lákal pro svoji variabilitu v nastavení, kdy je pomocí jednoho zařízení možnost provést více operací, např. změnit asymetrii klonování. Nicméně celovláknové zařízení trpělo velmi nízkou stabilitou a speciální dělič doprovázený polarizačně závislými ztrátami byl neefektivní. Machův-Zehnderův interferometr se Soleilovými-Babinetovými kompenzátory v ramenech byl nedokonalost sama. Pro experiment ukazující výhody strojového učení [A3] jsme ale sestrojili takový interferometr, který se všem těmto nedokonalostem vyhnul.

Funkční schéma interferometru je na obrázku 4.15. Vstupní a výstupní polarizační dělič Machova-Zahnderova interferometru prakticky převádí polarizační kódování do dráhového. Horizontálně polarizovaná složka signálního fotonu prochází do spodního ramene, vertikální se odráží do horního ramene. Polarizace ancily je pootočena o 90° pomocí HWP_1



Obrázek 4.15: Funkční schéma Machova-Zehnderova interferometru pro strojově naučené klonování. HWP a QWP značí půl a čtvrtvlnné fázové destičky, PBS polarizátory a D detektory. Fáze v interferometru byla nastavována pomocí piezoposuvu jednoho z pentagonů.

(natočené o 45°), takže původně horizontální složka se odrazí a pokračuje do spodního ramene, kdežto vertikální složka projde do horního ramene. Natočení půlvlnných fázových destiček v ramenech potom mění efektivní dělící poměr nezávisle pro obě horizontální složky (HWP_4) a obě vertikální složky (HWP_3). Na výstupním polarizátoru se všechny složky opět koherentně transformují na polarizační qubity, přičemž na jednom výstupu musíme přehodit zpátky H a V složky pomocí HWP_6 otočené o 45°.

Abychom dosáhli maximální nerozlišitelnosti fotonů před i za interferometrem, byla na vstupech i výstupech z interferometru použita jednomodová vlákna pro prostorovou filtraci. Vizibilita dvoufotonové interference pro horizontálně polarizované fotony (HWP_4 na 22.5°) byla 0.92 ± 0.04. V případě jednofotonové interference jsme dosahovali 0.941 ± 0.006 vizibility. Pro co největší stabilitu byly klíčové komponenty interferometru (děliče a pentagony) spolu propojeny klecovou konstrukcí (*Cage system*, ThorLabs). Díky tomu se dráhový rozdíl ramen v interferometru změnil za deset sekund o méně než setinu vlnové délky. I v případě rušivého vlivu vibrací od rotací fázových destiček se dráhový rozdíl ramen po dobu 30 sekund změnil jen o $\lambda/76.1$ [26].

Účelem experimentu bylo, aby strojový algoritmus nalezl dělící poměr interferometru pro obě polarizační složky tak, aby na výstupu zařízení byly dva co nejdokonalejší klony signálního qubitu. Polarizace signálního fotonu se vybírala náhodně z třídy fázově kovariantních stavů $(|H\rangle + e^{i\varphi}|V\rangle)/\sqrt{2}$. Půlvlnná destička HWP_2 byla tedy nastavena na 22.5° a náhodná fáze $\varphi \in [0, 2\pi)$ se nastavovala pomocí piezoposuvu jednoho z pentagonů. Pomocný qubit (ancila) měl horizontální polarizaci. Pro každou nastavenou fázi se na výstupu změřily fidelity klonů, kdy se projektovalo na polarizaci signálního qubitu a na

polarizaci ortogonální. Čtvrtvlnné destičky byly fixně nastavené na 45°, půlvlnné se nastavily podle dané projekce, přičemž u HWP_6 se připočítalo otočení o 45°. Z naměřených fidelit klonů se spočítala hodnotová funkce (*cost function*)

$$C = (1 - F_1)^2 + (1 - F_2)^2 + (F_1 - F_2)^2.$$

Ta byla navržena tak, aby byla co nejmenší v případě co největších a hlavně stejných fidelit. Optimalizační Nelderův-Mieldův algoritmus potom hledal takové natočení destiček uvnitř interferometru, aby minimalizoval hodnotu C. Tento algoritmus je vhodný pro hledání minima N-dimenzionální funkce bez nutnosti znát její gradient. V našem případě se nejdřív provedlo měření pro tři různá nastavení fázových destiček. Podle velikostí hodnotové funkce v těchto bodech navrhl algoritmus nový bod měření. Ten byl spolu se dvěma předchozími s nejmenší hodnotou C použit k nalezení dalšího bodu. Takto se postupně dokonvergovalo až k nastavení pro minimální hodnotu C. Konečné nastavení destiček se od hodnoty spočítané teoreticky lišilo přibližně o tři stupně. To může být způsobeno tím, že jsme do našeho teoretického modelu nezapočítali nedokonalost polarizátorů, které mají sice téměř stoprocentní odrazivost pro V polarizaci, ale odrazí i přibližně 5 % horizontální složky. Dalším možným důvodem rozdílu je nedokonalá kalibrace hlavních os půlvlnných destiček. Nicméně při experimentu se algoritmus snažil najít optimální fidelity pomocí změn parametrů, které měl k dispozici. A dosáhl hodnot fidelit $F_1 = 0.840 \pm 0.033$ a $F_2 = 0.849 \pm 0.040$ už po 40 krocích (měřených bodech).

V druhé části experimentu jsme povolili algoritmu optimalizovat navíc i nastavení HWP_1, tedy polarizaci pomocného fotonu. Zvýšili jsme tím sice dimenzi funkce pro hledání a prodloužili dobu optimalizace, ale algoritmus nakonec už po 60 krocích dospěl k hodnotám fidelit $F_1 = 0.843 \pm 0.046$ a $F_2 = 0.853 \pm 0.022$. Pokud by jsme zautomatizovali ještě další volné parametry experimentu a zahrnuli je do optimalizačního algoritmu, mohli bychom po delším čase dosáhnout i o něco lepších výsledků (a mohli bychom propustit šikovného experimentátora pro nadbytečnost).

Účelem experimentu nebylo najít vhodné nastavení destiček pro fázově kovariantní klonování, to jsem pro tento jednoduchý případ znali předem. Snahou bylo naučit vhodné univerzální zařízení určitou kvantovou operaci. Operaci klonování jsme vybrali z toho důvodu, protože ji máme na pracovišti dostatečně zažitou a víme také přibližně, jaké výsledky jsou očekávatelné.

4.3 HOM klonování s filtrací

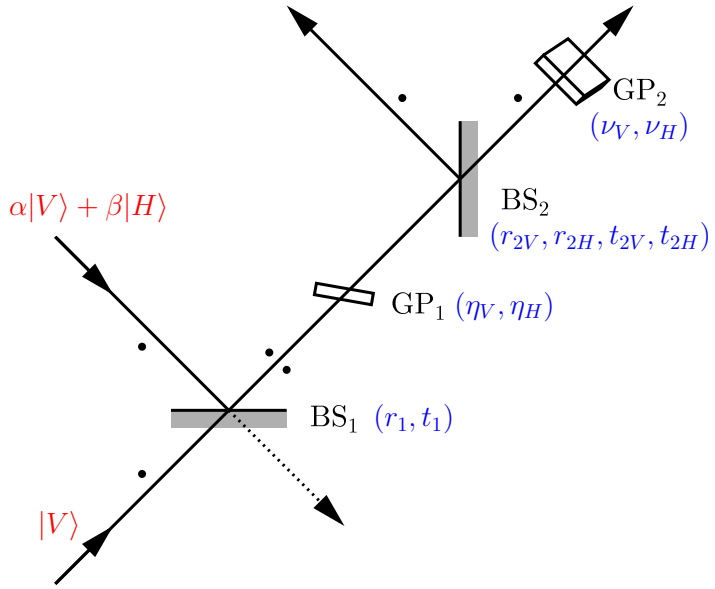
Další možností dosáhnutí fázově kovariantního klonování je filtrace za HOM klonováním [A4]. Tato metoda je ztrátová, filtrování se provádí pomocí polarizačně závislých ztrát. Pravděpodobnost úspěchu bude menší jak úspěšnost univerzálního HOM klonování, při kterém se klonování povede (fotony se shluknou) v šesti případech z osmi. Navíc přetrvává problém se stejným výstupním prostorovým módem obou klonů.

Funkční schéma klonovacího zařízení je na obrázku 4.16. Na prvním, polarizačně nezávislém děliči BS_1 dochází k HOM klonování. Předpokládáme, že tento dělič je nevyvážený tak, jak většina reálných děličů opravdu je. Spodní výstup z tohoto děliče pomineme, ztratíme tím polovinu signálu. Poté dochází k polarizačním ztrátám (GP), které umožní klonovat s vyšší fidelitou výstupních stavů, ale za cenu toho, že musíme znát informaci o tom, z které polokoule Blochovi sféry pochází vstupní qubit. Druhý dělič potřebujeme na to, aby nám klony od sebe oddělil. To nastane s pravděpodobností 1/2. Předpokládáme, že tento dělič má propustnost a odrazivost závislou na polarizaci vstupního fotonu. K potlačení tohoto neduhu, který způsobuje asymetrii ve fidelitách klonů, se použijí druhé polarizačně závislé ztráty (GP_2).

Výsledkem transformace celého zařízení je stav

$$-r_1 t_1 \eta_V [2\alpha \eta_V r_{2V} t_{2V} \nu_V |VV\rangle + \beta \eta_H (t_{2H} r_{2V} \nu_H |HV\rangle + r_{2H} t_{2V} \nu_V |VH\rangle)]. \tag{4.9}$$

Nastavíme GP_2 tak, aby kompenzoval nevyvážení druhého děliče, tj. $r_{2V} = t_{2V}\nu_V = r_{2H} =$



Obrázek 4.16: Fázově kovariantního režimu klonování lze dosáhnout filtrací výstupu HOM klonování. V případě polarizačního kódování se příslušná filtrace provede polarizačně závislými ztrátami (GP – skleněná destička) za prvním děličem BS_1. Polarizační ztráty za druhým děličem BS_2 kompenzují nevyváženost tohoto děliče. Při asymetrickém klonování se mění polarizační ztráty pomocí GP_1 a GP_2.

$t_{2H}\nu_H = r_2$. Pokud vytkneme pravděpodobnost úspěchu $P_{succ} = (2\,\eta_V^2\,r_1\,t_1\,r_2^2)^2$, tak bude mít výsledná transformace tvar

$$|V\rangle \to |VV\rangle, \qquad |H\rangle \to \frac{\eta_H}{2\eta_V}\left(|HV\rangle + |VH\rangle\right). \tag{4.10}$$

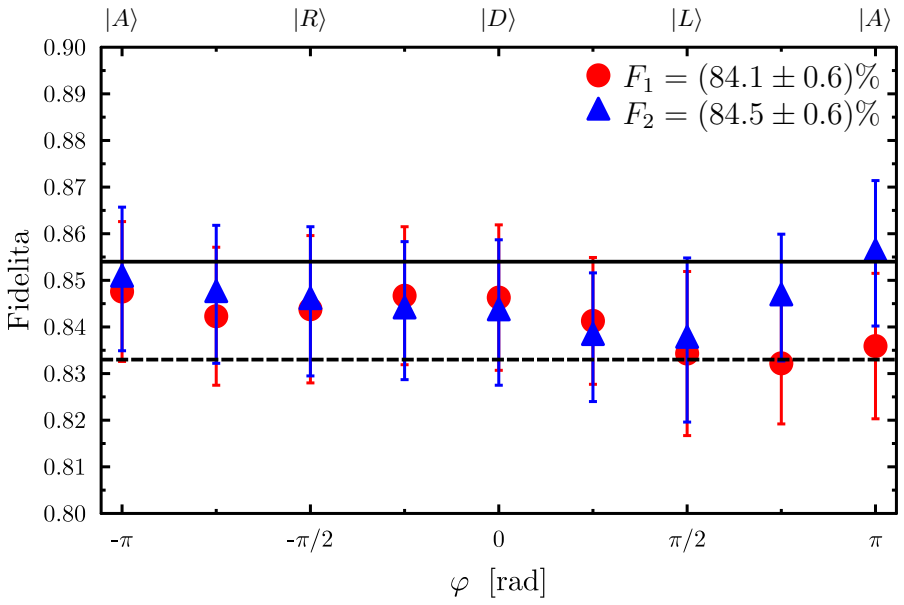
Podobnost s transformací fázově kovariantního klonování (2.7) je zřejmá. K úplné shodě stačí nastavit filtraci tak, aby $2\eta_V = \sqrt{2}\eta_H$.

V ideálním případě, kdy $r_1 = t_1 = r_2 = \frac{1}{\sqrt{2}}$, $\eta_H = 1 \to \eta_V = 1/\sqrt{2}$, bude hodnota pravděpodobnosti úspěchu $P_{succ} = \frac{1}{16} = 6.25\,\%$, což je výrazně méně než v případě kloneru se speciálním děličem.

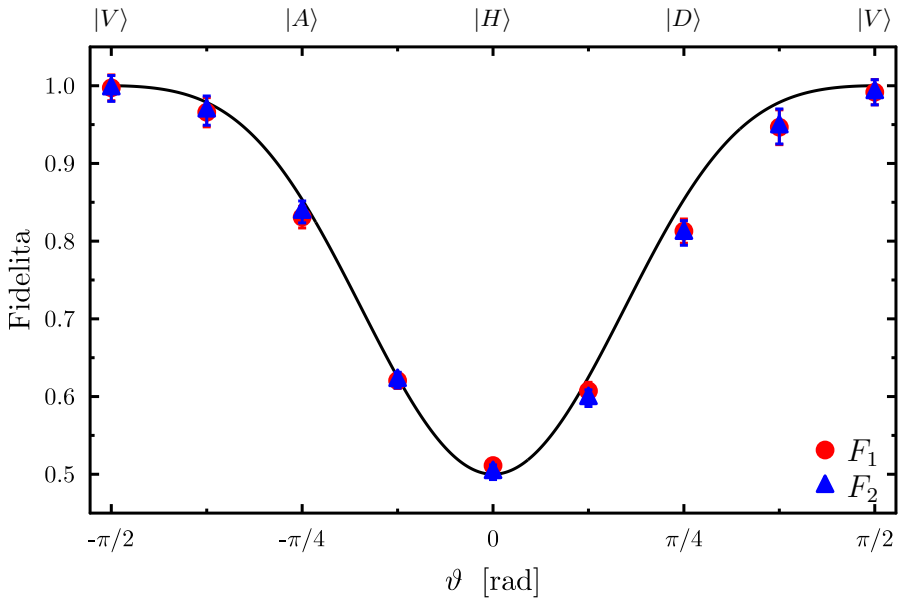
4.3.1 Hybridní fázově kovariantní zařízení

K experimentálnímu ověření fázově kovariantního klonování na bázi HOM klonování s filtrací jsme použili hybridní sestavu, viz obr. 3.3, výsledky měření byly opublikovány v článcích [A4, A6]. Tato sestava využívá jak vláknové optiky, na jednomodovém vláknovém děliči dochází k téměř ideálnímu shlukování fotonů, tak objemových komponent, kde můžeme využít polarizační kódování. Oproti sestavě pro univerzální klonování se změní jen míra polarizačně závislých ztrát. V případě univerzálního klonování tyto ztráty pouze vyvážily neideální dělič. V případě symetrického fázově kovariantního klonování musí tyto ztráty splňovat podmínku $\eta_V = 1/\sqrt{2}\eta_H$. Teoretická pravděpodobnost úspěchu klonování klesne na $1/16 = 6.25\,\%$. V praxi, jelikož sklíčky utlumujeme obě složky polarizace, jsme dosáhli hodnoty kolem $4\,\%$.

Výsledné fidelity klonů pro vstupní rovníkové stavy jsou na obr. 4.17. Průměrné hodnoty byly více jak jednu standardní odchylku nad limitem univerzálního klonování.



Obrázek 4.17: Závislost fidelit klonů na parametru φ pro rovníkové stavy ($\vartheta = \pi/2$) v případě symetrického fázově kovariantního klonování. Pomocný foton měl vertikální lineární polarizaci. Černá plná a přerušovaná čára značí limity fázově kovariantního resp. univerzálního klonování. Čísla v legendě jsou průměry přes všechna měření.



Obrázek 4.18: Závislost fidelit klonů na úhlu ϑ pro $\varphi = 0$ (stavy z poledníku Blochovy sféry) pro symetrické fázově kovariantní klonování. Pomocný foton byl stále ve stavu V. Plná čára představuje teoretickou předpověď.

V případě klonování signálních stavů z poledníku Blochovy sféry (viz obr. 4.18) se fidelita měnila od hodnoty 1 (signál a ancila měli shodnou polarizaci) po 1/2 (signál a ancila měli ortogonální polarizace). Pokud by mělo klonovací zařízení pracovat správně, tak by se pro stavy z dané polokoule měla použít ancila s adekvátního pólu (vertikální resp. horizontální lineární polarizace). Při přechodu signálního stavu přes rovník by se měla polarizace pomocného fotonu změnit, což se při našich měření záměrně nestalo.

Díky vláknovému děliči jsme dosáhli 98 % vizibility dvoufotonové interference. Na druhou stranu, jelikož jsme nepoužili jednomodová vlákna zachovávající polarizaci, museli jsme zdlouhavě kompenzovat polarizační změny vlákna pomocí polarizačních rotátorů. Po prvotní úpravě byly potřeba už jen malé korekce pro různé vstupní polarizace. Nicméně jako zařízení pro útok na kvantovou kryptografii by se tato klonovací sestava nedala použít. Její klíčové vlastnosti by se měnily podle vstupního stavu signálního fotonu.

Pro filtraci současných detekcí se použilo dvojice modulů TAC a SCA s nastavenou šířkou okna 2 ns, což se ukázalo jako rozumný kompromis, kdy ještě výrazně neklesl počet signálních koincidencí a počet náhodných už byl zanedbatelně malý. Vliv různých detekčních účinností detektorů byl potlačen sekvenčním měřením, kdy jsme prováděli projekce jak do stavu signálního fotonu, tak i do stavu k němu kolmému. Sobě příslušné naměřené hodnoty pro různé páry detektorů se zprůměrovaly.

4.4 Asymetrické klonování

Nejjednodušší způsob asymetrického fázově kovariantního klonování je s využitím polarizačně závislého děliče, jehož dělící poměry lze měnit v závislosti na asymetrii, které hodláme dosáhnout. Takový dělič lze simulovat pomocí Machova-Zehnderova interferometru. Nebo můžeme přejít ke dráhovému kódování, kdy dvě ortogonální polarizace nahradí dva možné prostorové módy. Pro tuto realizaci je potřeba dvou děličů s různým dělícím poměrem.

Pro jednoduchost budeme v následujícím výpočtu uvažovat, že ke klonování dochází na dvou děličích s odrazivostmi $R_1 = r_1^2$, $R_2 = r_2^2$ a propustnostmi $T_1 = t_1^2$, $T_2 = t_2^2$. Pro daný parametr asymetrie q se musí nastavit různé dělící poměry obou děličů tak, aby byly splněny rovnosti

$$\sqrt{q} = \frac{r_1 r_2}{\sqrt{P_{succ}}}, \qquad \sqrt{1-q} = -\frac{t_1 t_2}{\sqrt{P_{succ}}}, \qquad \text{kde} \qquad P_{succ} = (2R_1 - 1)^2. \tag{4.11}$$

Z těchto rovností můžeme vyjádřit vztah pro odrazivost druhého děliče a také získat kubickou rovnici pro odrazivost prvního děliče,

$$R_2 = \frac{q(1-R_1)}{q-(2q-1)R_1}, \qquad 4(2q-1)R_1^3 + (3-12q)R_1^2 + 6qR_1 - q = 0.$$

Pro symetrické klonování ($q = 0.5$) se kubická rovnice zredukuje na kvadratickou s řešením $R_1 = \frac{1}{2} \pm \frac{1}{2\sqrt{3}}$, tedy $R_1 \approx 0.788$ nebo $R_1 \approx 0.212$. Odrazivost druhého děliče bude komplementární, $R_2 \approx 0.212$ nebo $R_2 \approx 0.788$. V asymetrickém případě musíme řešit kubickou rovnici pro R_1 s proměnnou $q \in (0.5; 1]$. Na tomto intervalu jsou fyzikálně platné dva kořeny ze tří,

$$-\frac{3-12q+\sqrt[3]{4}\sqrt[6]{\Delta_1^2+\Delta_0^2}\cos\left[\left(\arctan\frac{\Delta_0}{\Delta_1}-\pi\right)/3\right]}{24q-12}, \qquad q \in \left(\frac{1}{2}; \frac{1}{2}+\sqrt{\frac{1}{8}}\right),$$

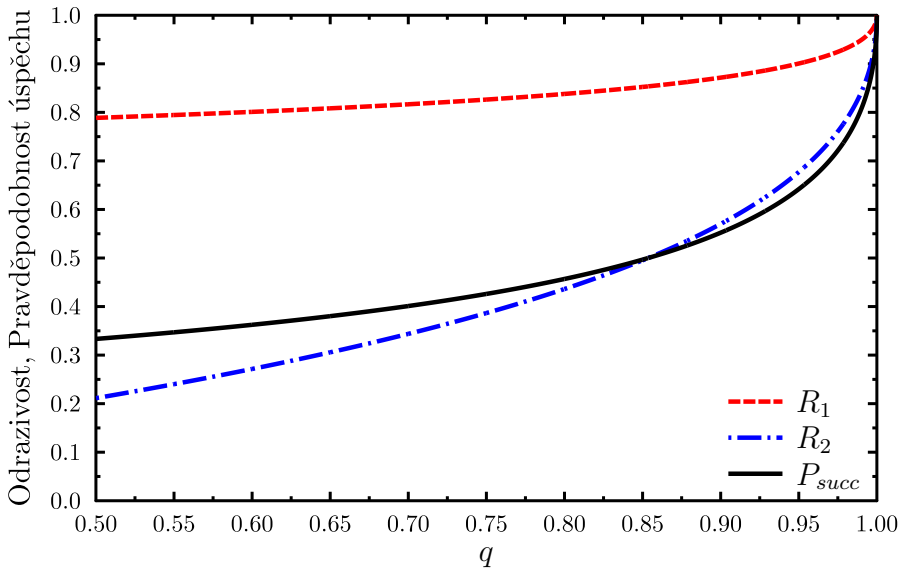
$$-\frac{3-12q-\sqrt[3]{4}\sqrt[6]{\Delta_1^2+\Delta_0^2}\cos\left[\left(\arctan\frac{\Delta_0}{\Delta_1}+\pi\right)/3\right]}{24q-12}, \qquad q \in \left(\frac{1}{2}+\sqrt{\frac{1}{8}}; 1\right],$$

kde $\Delta_1 = 54(8q^2-8q+1)$ a $\Delta_0 = 216\sqrt{-4q^4+8q^3-5q^2+q}$. Asymetrie $q = 1$ je triviální, obě odrazivosti R_1 i R_2 jsou jednotkové, signální i pomocný foton prochází zařízením beze změny. Dělící poměry děličů pro dva polarizační resp. prostorové módy a pravděpodobnost úspěchu klonování v závislosti na koeficientu asymetrie q jsou znázorněny na obr. 4.19.

Složitější a více ztrátová metoda je nahradit nastavitelný dělič děličem s pevným dělícím poměrem a měnit polarizačně závislé ztráty na výstupech. Aby byla splněna podmínka stejné účinnosti klonování, musí polarizačně selektivní propustnosti η_H a η_V splňovat podmínku $\eta_V^2 = 1/(2-\eta_H^2)$. Fidelity klonů se budou měnit se změnou polarizační filtrace

$$F_1 = \frac{1}{2}\left(1 + \frac{\eta_H}{\sqrt{2}}\right) \qquad F_2 = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}\eta_V}\right). \tag{4.12}$$

Srovnáním s předpisy pro fidelity (2.13) získáme hodnotu parametru asymetrie $q = \eta_H^2/2 = 1 - \frac{1}{2\eta_V^2}$. Pravděpodobnost úspěchu je oproti symetrickému případu vynásobena propustností polarizačního filtru $\eta_V^2/3$.



Obrázek 4.19: Závislost odrazivostí děliče (děličů) a pravděpodobnosti úspěchu v závislosti na koeficientu asymetrie q fázově kovariantního klonování.

Asymetrie pomocí polarizačně závislých ztrát lze dosáhnout i u HOM klonování s filtrací. Pokud neprovedeme úpravu výstupního stavu v rovnici (4.9), která symetrizuje druhý dělič, zařízení provede tuto transformaci

$$|V\rangle \to |VV\rangle, \qquad |H\rangle \to \left(\frac{\eta_H t_{2H}\nu_H}{2\eta_V t_{2V}\nu_V}|HV\rangle + \frac{\eta_H r_{2H}}{2\eta_V r_{2V}}|VH\rangle\right). \tag{4.13}$$

Zde můžeme ztotožnit parametr asymetrie q s výrazy před členy $|HV\rangle$ a $|VH\rangle$:

$$\sqrt{q} = \frac{\eta_H t_{2H}\nu_H}{2\eta_V t_{2V}\nu_V}, \qquad \sqrt{1-q} = \frac{\eta_H r_{2H}}{2\eta_V r_{2V}}. \tag{4.14}$$

4.4.1 Celovláknové klonovací zařízení

V případě celovláknového klonovacího zařízení [A4, A5] jsme mohli spojitě měnit asymetrii klonování bez toho, abychom byli nuceni zavádět jakékoliv další přidané ztráty. Tuto výhodu nám daly vláknové děliče s proměnným dělícím poměrem (VRC, viz obr. 4.6). Nevýhodou je interferometrické zařízení z důvodu nutnosti použít dráhové kódování.

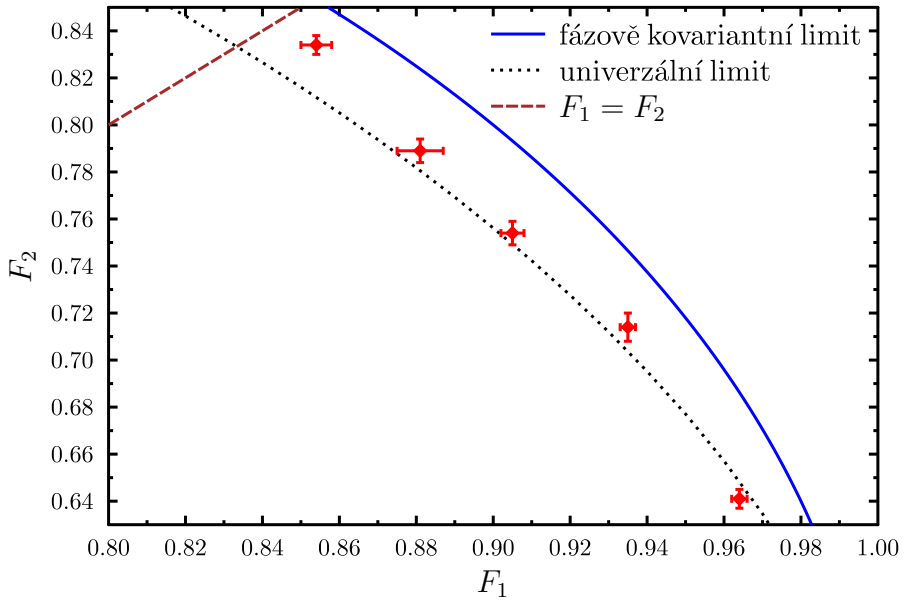
V tabulce 4.3 jsou vypsány průměrné hodnoty fidelit a pravděpodobnost úspěchu pro různé asymetrie zařízení. Závislost fidelit je zobrazena v grafu na obr. 4.20, až na jedno měření všechny body včetně chybové úsečky leží v oblasti nedosažitelné pro univerzální klonovací zařízení.

4.4.2 Speciální dělič se skleněnými destičkami

Klonovací zařízení na bázi speciálního děliče s pevným dělícím poměrem klonuje asymetricky v závislosti na dělicím poměru tohoto děliče. Pokud chceme míru asymetrie změnit,

q	F_{1T}[%]	F_{2T}[%]	F_1 [%]	F_2 [%]	P_{succ} [%]
0.5	85.35	85.35	85.4±0.4	83.4±0.4	37.2±0.1
0.6	88.73	81.62	88.1±0.6	78.9±0.5	37.7±0.1
0.7	91.83	77.39	90.5±0.3	75.4±0.5	43.0±0.1
0.8	94.72	72.36	93.5±0.3	71.4±0.6	47.4±0.1
0.9	97.43	65.81	96.4±0.2	64.1±0.4	57.4±0.2

Tabulka 4.3: Tabulka naměřených hodnot fidelit klonů a pravděpodobnosti úspěchu vláknového klonovacího zařízení. Hodnoty F_{1T} a F_{2T} značí teoretické hodnoty dle rovnice (2.13).

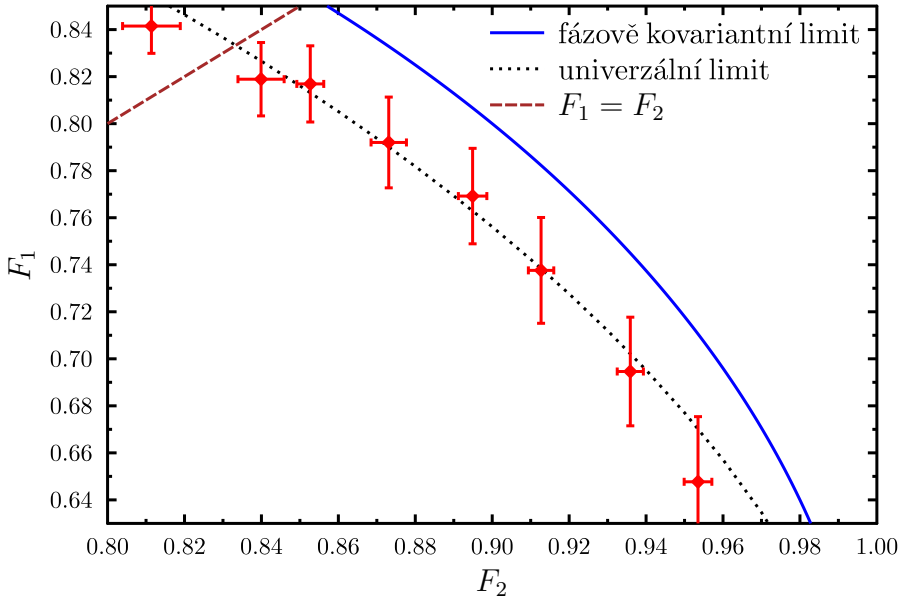


Obrázek 4.20: Závislost fidelit v asymetrickém režimu fázově kovariantního klonování vláknového zařízení. Průměr a chyba hodnot fidelit byly určeny z měření pro různé hodnoty fáze φ.

musíme změnit dělicí poměr. V tomto případě jsme změnu prováděli polarizační filtrací, tedy polarizačně závislými ztrátami skleněných destiček GP (viz obr. 4.8).

Zavedením polarizačních ztrát, a tedy s menší pravděpodobnosti úspěchu, jsme provedli měření fidelit klonování stavů z rovníku Blochovi sféry ($\vartheta = \pi/2$) pro různé hodnoty asymetrie. Průměrné hodnoty fidelit jsou vynesené v grafu na obrázku 4.21 a spolu s pravděpodobností úspěchu jsou vypsány v tabulce 4.4.

Samotný speciální dělič bez ztrátových sklíček (tzn. bez GP) klonuje lehce asymetricky, přibližně s parametrem asymetrie $q = 0.46$. Zvyšováním ztrát procházíme symetrickým režimem ($q = 0.5$) až k výrazně nesymetrickému klonování. Zde už jsou přidané ztráty natolik velké, že pravděpodobnost úspěchu klonování klesla na desetinu. Ve všech případech se fidelity klonů pohybují na teoretické hranici pro univerzální klonování. Lepších výsledků by nejspíš bylo dosaženo s použitím elektronických modulů TAC a SCA s dvounanosekundovým koincidenčním oknem.



Obrázek 4.21: Závislost fidelit klonů v asymetrickém režimu fázově kovariantního klonování pomocí speciálního děliče. Polarizačně závislých ztrát bylo dosaženo nakloněnými sklíčky. Průměr a chyba hodnot fidelit byly určeny z měření pro různé hodnoty fáze φ.

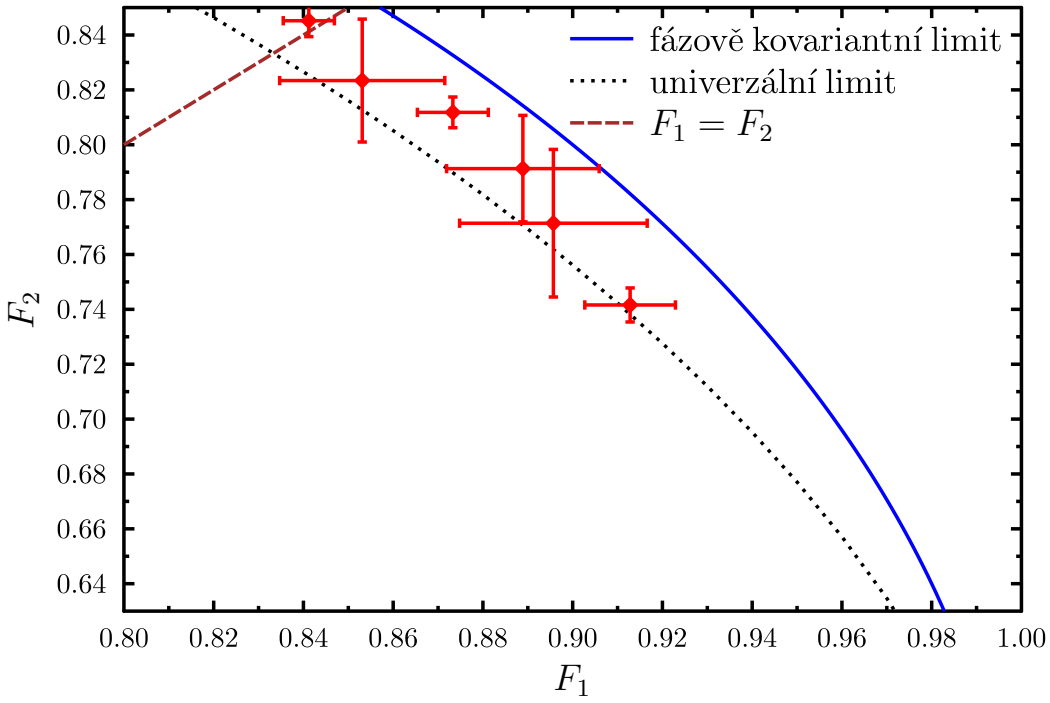
q	F_{1T}[%]	F_{2T}[%]	F_1 [%]	F_2 [%]	P_{succ} [%]
bez GP	86.74	83.91	84.2±1.2	81.1±0.8	31.2±0.8
0.50	85.35	85.35	82.2±0.2	82.2±0.2	28.8±0.1
0.51	85.00	85.71	81.9±1.6	84.0±0.6	23.6±0.2
0.55	83.54	87.08	81.7±1.6	85.3±0.4	20.0±0.2
0.63	80.41	89.69	79.2±1.9	87.3±0.5	18.8±0.2
0.70	77.39	91.83	76.9±2.0	89.5±0.4	17.4±0.2
0.78	73.45	94.16	73.8±2.3	91.3±0.3	13.8±0.1
0.85	69.36	96.10	69.5±2.3	93.6±0.3	10.3±0.1
0.93	63.23	98.22	64.8±2.8	95.4±0.4	2.9±0.1

Tabulka 4.4: Tabulka průměrných hodnot fidelit klonů a pravděpodobnosti úspěchu klonovacího zařízení se speciálním děličem pro různé úrovně asymetrie. Hodnoty F_{1T} a F_{2T} značí teoretické hodnoty dle rovnice (2.13), bez GP značí případ bez ztrátových sklíček.

4.4.3 Hybridní klonovací zařízení

Asymetrický režim klonování lze dosáhnout změnou polarizačních ztrát před i za objemovým děličem BS hybridního zařízení [A4, A6] (viz schéma na obrázku 3.3), jehož amplitudové propustnosti jsou popsaným parametry r_{2H}, r_{2V}, t_{2H} a t_{2V}. Po dosazení parametrů odrazivosti a propustnosti objemového děliče, $R_{2H} = R_{2V}$ a $T_{2H} = 1.16\,T_{2V}$, do rovnic (4.14) můžeme nastavit filtraci podle potřebné asymetrie q:

$$\left(\frac{\eta_H}{\eta_V}\right)^2 = 4(1-q), \qquad \left(\frac{\nu_V}{\nu_H}\right)^2 = 1.16\frac{1-q}{q}.$$



Obrázek 4.22: Závislost fidelit klonů v asymetrickém režimu fázově kovariantního klonování hybridního zařízení. Průměr a chyba hodnot fidelit byly určeny z měření pro různé hodnoty fáze φ.

S rostoucí asymetrií klonování se polarizačně závislé ztráty před děličem zmenšují a za ním zvětšují. Pravděpodobnost úspěchu klonování závisí i na dělícím poměru prvního vláknového děliče,

$$P_{succ} = (2r_1 t_1 \eta_V^2 r_{2V} t_{2V} \nu_v)^2. \tag{4.15}$$

Experimentálně určená hodnota s větší asymetrií mírně roste ze 4.2 % (symetrické klonování, $q = 0.5$) po 6 % ($q = 0.75$). Větší míry asymetrie nebylo možné s párem ztrátových skel dosáhnout. Naměřené hodnoty fidelit asymetrického klonování jsou vypsány v tabulce 4.5 a graficky znázorněny na obr. 4.22.

q	F_{1T} [%]	F_{1T} [%]	F_1 [%]	F_2 [%]	P_{succ} [%]
0.50	85.35	85.35	84.5±0.6	84.1±0.6	4.2±0.1
0.55	83.54	87.08	82.3±2.2	85.3±1.8	4.4±0.2
0.60	81.62	88.73	81.2±0.6	87.3±0.8	5.0±0.1
0.65	79.58	90.31	79.1±1.9	88.9±1.7	4.8±0.1
0.70	77.39	91.83	77.1±2.7	89.6±2.1	4.8±0.2
0.75	75.00	93.30	74.2±0.6	91.3±1.0	6.2±0.2

Tabulka 4.5: Tabulka naměřených hodnot fidelit klonů a pravděpodobnosti úspěchu hybridního klonovacího zařízení. Hodnoty F_{1T} a F_{2T} značí teoretické hodnoty dle rovnice (2.13).

Kapitola 5

Aplikace kvantového klonování

V našich prvních experimentech a článcích jsme se zaměřili přímo na konstrukci klonovacích zařízení, na jejich popis, meze dosažitelných fidelit klonů a pravděpodobností úspěchu. V druhé dekádě našeho klonování jsme se zaměřili spíše na využití těchto zařízení pro určitou aplikaci, ověření bezpečných limitů provozu kvantové kryptografie a používání kvantových peněz nebo zvýšení vzdálenosti pro přenos kvantového stavu ztrátovým prostředím.

5.1 Odposlech kryptografie

Jednou z mála oblastí kvantové informatiky (prakticky jediná), která dospěla až do fáze komerčního využití, je kvantová kryptografie. Ta se zabývá bezpečným přenosem náhodné sekvence klasických bitů pomocí kvantových stavů. Pro ověření správného fungování komerčních zařízení se provedlo mnoho testů [13, 61]. Většinou se jednalo o testy koncových zařízení Alice (odesilatele) či Boba (příjemce), kdy se hledali jejich technické nedokonalosti umožňující Evě (narušiteli) zjistit část nebo celou sekvenci klíče. My jsme se zaměřili na přenosovou linku mezi Alicí a Bobem a zkoumali jsme Eviny možnosti pomocí klonovacího útoku [A9].

Jak už bylo zmíněno v sekci 2.3.1, pokud by přenosová linka byla ideální, neměla by Eva šanci. Jakýkoliv pokus o zjištění stavů qubitů v komunikační lince by vedl k změně jejich kvantového stavu, která by byla následnou kontrolou odhalena. Při této kontrole se zjistí relativní chybovost přenosu kvantových stavů (QBER – *Quantum Bit Error Rate*) jednoduše tak, že Alice s Bobem obětují část přeneseného klíče (kterou už nelze použít k šifrování) a u ní spočítají podíl případů, kdy Bob změřil jiný stav než Alice poslala, k celkovému počtu. V případě použití ideálních komponent by byla chybovost nulová. V reálných podmínkách musíme ale počítat s nárůstem chybovosti vlivem šumu v komunikační lince, ztrátám při přenosu, nedokonalým detektorům atd. Nenulové QBER může využít Eva pro krytí své činnosti. Například může zaměnit obyčejné křemíkové optické vlákno za vlákno z materiálu s menší absorpcí a odstínit jej lépe od zdrojů šumu. Potom může použít klonovací zařízení k získání informace o kvantových stavech přenášených mezi Alicí a Bobem bez toho, aby byla odhalena. Aby k tomuto nedošlo, definovala se mezní chybovost. Pokud by se překročila, nešlo by přenos považovat za bezpečný, ať už z jakýkoliv příčin. Protože by měla Eva možnost, byť jen teoretickou, získat informaci o přenášeném tajném klíči.

Hodnota mezní chybovosti je různá v závislosti na použitém kryptografickém protokolu a na typu klonovacího útoku. Jako příklad jsme se rozhodli testovat dva známé protokoly – BB84 [32] a R04 [33]. Pokud Alice s Bobem neznají Eviny technologické možnosti, například dnes se dá předpokládat že Eva nedokáže provést koherentní útok, tj. změřit všechny své kopie současně, potom je jejich mezní chybovost bezpečného přenosu limitována hodnotou 11% pro BB84 [62] a 9.85% pro R04 [33]. Další práce určují hodnotu mezní chybovosti v případě, kdy Eva nemá informaci o nastavení Bobova měření [63]. My jsme se rozhodli zjistit mez chybovosti v případě použití klonovací strategie, která je už v dnešní době dosažitelná.

Narušitel Eva připojí své klonovací zařízení na telekomunikační linku, po které Alice posílá Bobovi kvantové stavy v podobě polarizačního stavu jednotlivých fotonů. Eva provede klonování, díky nemožnosti bezchybného klonování jsou obě kopie zatížené šumem. Nejednotková účinnost způsobí též ztráty. Bob provede měření na jedné kopii, s Alici si potom veřejně oznámí použité báze. Tuto „veřejnou“ informaci použije Eva k optimalizaci měření svých klonů, které si zatím podržela v kvantové paměti. Ačkoliv použitelné kvantové paměti jsou již dneska k dispozici, stále se jedná o komplexní zařízení, které není v naši laboratoři možné realizovat. Proto jsme funkci kvantové paměti pouze simulovali. Změřili jsme úplnou tomografii dvou fotonů na výstupu klonovacího zařízení a estimovali jsme matice hustoty stavu sdíleného Evou a Bobem. Po tom, co Bob „provedl své měření“, se matice redukovala na stav, který by byl uložen v kvantové paměti.

Pro experimentální ověření se použilo zrcadlově fázově kovariantní klonovací zařízení (MPPC). Na jednom vstupu byl foton s polarizačním stavem nastaveným Alicí, v případě kryptografického protokolu BB84 to byly polarizační stavy z rovníku Blochovy sféry $|A\rangle$, $|D\rangle$ nebo $|R\rangle$, $|L\rangle$, v případě R04 pak stavy $|a_n\rangle$,

$$|a_n\rangle = \left(|H\rangle + e^{\imath 2\pi/3}|V\rangle\right)/\sqrt{2}, \quad |b_n\rangle = \left(|H\rangle + e^{\imath 2\pi/3}e^{\imath\pi/3}|V\rangle\right)/\sqrt{2}, \quad n = 0, 1, 2. \tag{5.1}$$

Druhý vstupní foton měl náhodně H nebo V polarizaci. Na výstupech se provádělo úplné tomografické měření. Potom se „vyprojektovala“ Bobova kopie v bázi A/D popř. R/L v případě protokolu BB84 a nebo se projektovala na stav $|b_n\rangle$ v případě protokolu R04. Aby se účinněji zamaskoval Evin útok, tak by měl klon poslaný Bobovi ležet v rovině rovníku, toho lze docílit například snížením čistoty. To zajistí MPPC s určitým nastavením parametru Λ (2.10) a q (2.14). Hodnota parametru míry klonování Λ stejně jako parametru asymetrie q se nastavila tak, aby byla pro daný kryptografický protokol optimální.

Numerická optimalizace parametrů klonování se snažila minimalizovat chybovost QBER za předpokladu nulové frekvence tajného klíče R (*secret-key rate*). Frekvence R odpovídá četnosti zaručeně bezpečných bitů, které mohou Alice s Bobem z kryptografického přenosu vyextrahovat. Pokud je $R = 0$, značí to, že Alice s Bobem spolu nesdílí žádnou informaci, o které by Eva nevěděla. Optimální parametry pro BB84 jsou $\Lambda^2 = 1/3$ a $q = 1/2$, pro R04 potom $\Lambda^2 = 4/11$ a $q = 4/7$.

Experimentálně zjištěné hodnoty stejně jako teoretické odhady pro oba testované protokoly jsou vypsány v tabulce 5.1. Naše teoreticky zjištěná a experimentálně ověřená mezní hodnota chybovosti v případě BB84 opravila dosavadní hodnotu 14.6% [64] resp. 15% [65]. Nově jsme určili tuto hodnotu pro protokol R04, pro tento typ útoku zatím nebyla zkoumána.

	Λ^2	q	R		QBER [%]		P_{succ} [%]	
			teorie	experiment	teorie	experiment	teorie	experiment
BB84	1/3	1/2	0.00	0.03 ± 0.03	16.7	18.5 ± 1.5	13.7	15.1 ± 1.1
R04	4/11	4/7	0.00	0.01 ± 0.08	16.7	18.0 ± 3.5	12.7	7.4 ± 0.1

Tabulka 5.1: Tabulka teoretických a experimentálně naměřených hodnot pro dva zkoumané kryptografické protokoly. Λ a q – parametry MPPC, R – frekvence tajného klíče, QBER – mezní hodnota tolerované chybovosti, P_{succ} – pravděpodobnost úspěchu klonování.

5.2 Zesilovač

V článku [A10] jsme se snažili zvýšit přenosovou kapacitu ztrátové linky pomocí klonování (viz 2.3.2). Nerovnost 2.15 se nám podařilo splnit díky kombinovanému klonování, kdy v části případů jsme prováděli triviální klonování a v části případů jsme klonovali fázově kovariantně nebo zrcadlově fázově kovariantně. Zatímco triviální klonování má jednotkovou úspěšnost ale fidelitu klonů pouze 3/4, má například fázově kovariantní klonování třetinovou úspěšnost ale fidelitu klonů minimálně 85 %. Zvolením stejného poměru obou typů klonování jsme nerovnost experimentálně splnili, čímž jsme dokázali, že jsme zvýšili přenosovou kapacitu ztrátové linky.

5.3 Kvantové peníze

Koncept kvantových peněz byl navržen už v sedmdesátých letech minulého století Wiessnerem. V principu využívá nemožnosti klonovat kvantový stav stejně jako u kvantové kryptografie. Jenže zatímco kryptografie slouží k tajnému přenosu zpráv, kvantové peníze autorizují finanční transakci.

5.3.1 Padělání kvantových peněz

V článku [A11] jsme využili klonovaní k testování bezpečnosti finančních transakcí pomocí kvantových peněz. Opět jsme použili kombinovanou strategii klonování – zrcadlově fázově kovariantní a triviální – z toho důvodu, že pro autentizaci kvantové bankovky musí zpět do banky dorazit alespoň polovina qubitů tvořící danou bankovku. Ukázali jsme, že banka musí být v přípravě qubitů tvořící kvantovou bankovku důsledná v tom smyslu, že musí rovnoměrně pokrýt celý dostupný Hilbertův prostor. Pokud tak neučiní, lze vhodnou volbou typu klonování získat dostatek informace k případnému padělání kvantových bankovek.

5.3.2 Zranitelnost platby kvantovou kreditkou

Dalším naším výzkumným projektem [A2] byl test bezpečnosti protokolu pro platbu kvantovou kreditní kartou, který navrhl Bozzio a kol. [66]. Jedním z klíčových okamžiků jakékoliv (nejen kvantové) platby je ověření pravosti platidla. Zatímco v běžném "klasickém"platebním styku se o to postará samotný prodavač, popř. šifrovaná klasická komunikace banky s platebním terminálem, tak v případě platby kvantovými penězi by bylo

potřeba, aby bankovky zkontrolovala sama banka. Pokud jsou tyto peníze uchovány v podobě kvantových bitů v nějaké formě kvantové paměti na kvantové kreditní kartě, museli by se z této karty oddělit (např. převést na fotonové qubity) a poslat do banky kvantovou linkou k ověření v podobě projekčního měření. Pokud chceme, aby platba proběhla tzv. online, musí nejméně polovina fotonových qubitů dorazit optickým vláknem do banky. I za předpokladu nízkoztrátové linky (cca $0.16\,\mathrm{dB\,km^{-1}}$) je tedy vzdálenost terminálu od banky limitována na přibližně 20 km.

Bozzio a kol. navrhli způsob jak ověřit platnost kvantové bankovky přímo v obecně nedůvěryhodném platebním terminálu, který je s bankou spojen pouze klasickou linkou, která nemusí být dokonce ani šifrovaná. Trik spočívá ve využití tzv. *quantum retreavel games* [67]. Návrh předpokládal kódování qubitů do polarizačního stavu jednotlivých fotonů. Samotný způsob uložení qubitů v kvantové paměti na kreditní kartě je pro náš výzkum irelevantní. Předpokládejme, že při transakci budou z kvantové paměti převedeny na optické qubity. Jednotlivé bankovky (tokeny) byly tvořeny sekvencí párů qubitů, které se skládaly z těchto osmi kombinací stavů

$$|AR\rangle,\ |AL\rangle,\ |DR\rangle,\ |DL\rangle,\ |RA\rangle,\ |LA\rangle,\ |RD\rangle,\ |LD\rangle.$$

Při platbě nahlásil terminál bance sériové číslo bankovky, kterou hodlá autentizovat. Banka si podle tohoto čísla vyhledala, jak byla tato bankovka zakódovaná. Následně terminálu poslala báze, ve kterých má provést projekční měření na každém páru qubitů tvořící bankovku, náhodně buď D/A nebo R/L projekci. Terminál provedl projekční měření všech párů a výsledky poslal bance. V případě, kdy měřící báze koincidovala se stavem qubitu, měření dalo deterministický výsledek, pokud ne (např. projekce D/A provedená na qubit ve stavu $|R\rangle$), výsledek byl náhodný. Nikdo, krom banky, ale neví, který z páru qubitů dá onen deterministický výsledek. Bez této znalosti je výsledné měření pouze sekvence náhodných bitů. Banka nicméně ví, které bity má kontrolovat. Pokud zjistí shodu výsledků a původní sekvence pro kódování bankovky, tak potvrdí pravost bankovky a provede finanční transakci. Pokud míra chybovosti překročí bezpečnostní limit, tak bankovku označí za falešnou. Stejně tak transakce neproběhne, pokud banka nebude mít alespoň polovinu z očekávaných výsledků měření.

Z výsledků našeho výzkumu jsme dospěli k závěru, že banka musí použít jedinečnou náhodnou sekvenci sériového čísla pro každou bankovku, aby mohla být tato metoda považována za bezpečnou. Nicméně pro větší množství vydaných bankovek by bance nastal problém s velikostí databáze sériových čísel. Navíc by v té databázi bylo potřeba rychle vyhledávat sekvence bankovek pro ověření plateb. Předpokládejme, že si banka ulehčí život a ke kódování kvantových bankovek využije pseudonáhodné sekvence vygenerované pomocí hešovací funkce (*hash function*), kde bude společný vstup v podobě tajného klíče (*seed, salt*). V našem článku ukazujeme, že jeden klíč je použitelný jen pro velmi omezený počet bankovek. Použitím nenáhodné sekvence sériového čísla pro kódování kvantových bankovek se protokol stane zranitelný vůči klonování.

Podstata útoku spočívá v úpravě platebního terminálu tak, aby v určitých případech prováděl před projekčním měřením fázově kovariantní klonování qubitového páru. Z každého qubitu z páru vzniknou dvě kopie (pokud klonování uspěje), z výsledků měření na obou kopiích lze odhadnout, zda byl daný qubit měřen ve své bázi, v tom případě by oba klony daly stejný výsledek projekčního měření. Samozřejmě je tento odhad zatížen chybou, která je důsledkem nejednotkové fidelity klonování. Ze stejného důvodu při klonování

vzniknou chyby. Aby banka útok nezjistila, je toto klonování prováděno s dostatečně malou četností. Z vytěžené informace, tj. který qubit byl kódován ve své bázi a jaký měl stav, lze při dostatečném množství opakování odhadnout klíč hešovací funkce. Odhadnutí klíče lze provést tzv. hrubou silou, tj. zkoušíme všechny známé hešovací funkce a všechny možné sekvence klíče, nebo pomocí strojového učení. Obě metody vedou k cíli, jen různě rychle. Předpokládejme ale, že výpočetním časem nejsme omezeni. Výsledky našich měření ukazují, že jeden klíč známé hešovací funkce je objeven už po 1 200 úspěšných klonování obou qubitů z páru. My jsme použili lineárně optický způsob klonování pomocí nevyváženého děliče s limitní pravděpodobností úspěchu jednoho qubitu 1/3. Pro celý pár qubitů je tedy pravděpodobnost úspěchu 1/9, museli jsme se pokusit klonovat nejméně 11 000 krát.

Experimentální sestava tohoto klonovacího zařízení měla oproti předchozím jednu specialitu. Aby jsme simulovali reálné podmínky v platebním terminálu, museli jsme zaznamenávat jednotlivé detekční (koincidenční) události pomocí rychlých klopných obvodů v modulu JP2 (SLO). Aby jsme nemuseli přerušovat měření při každé zdlouhavé změně natočení fázových destiček pro změnu vstupního stavu či projekce, zapisovali jsme události pro jeden vstupní stav (např. $|A\rangle$) a jednu projekci (např. R) do jednoho souboru (pojmenovaného AR). Výsledkem byla jedna ze čtyř možností, buď se oba fotony vyprojektovali do stavu $|R\rangle$, nebo se oba odrazili na polarizátorech a byla detekována koincidence značící projekce obou fotonů do stavů $|L\rangle$, nebo se první foton vyprojektoval do stavu $|R\rangle$ a druhý do $|L\rangle$ a nebo naopak. Zaznamenali jsme to tak pro všechny kombinace vstupních stavů a projekcí. Potom jsme tato data využili následovně: Předpokládejme, že je kvantová bankovka tvořena pouze dvěma páry qubitů: $|DR\rangle$ a $|RA\rangle$. Pro první pár banka určí projekci v R bázi, pro druhý v D bázi. Výsledky klonovacího procesu vyextrahujeme postupně ze souborů DR, RR, RD a AD (samozřejmě se pokaždé načtou jiné události z jednoho souboru). Dál už se výsledky klonování zpracovávaly podle postupu popsaného v článku.

Závěr

Obsahem této práce je popis experimentálního klonování kvantových stavů jednotlivých fotonů ve Společné laboratoři optiky UP a FZÚ AV ČR v Olomouci, přičemž značná část experimentů proběhla ve spolupráci s kolegy z katedry Optiky UP. Je až s podivem, že nám toto téma vydrželo téměř dvě dekády. Nicméně není jisté, zda se už toto odvětví výzkumu nadobro vyčerpalo.

Naše zkonstruovaná zařízení nebyla zamýšlena pro přímý útok na kvantovou kryptografii, zkoumali jsme klonování proto, aby jsme ukázali experimentální limity a ověřovali tak správnost těch teoretických. Našli jsme také maximální míry chybovosti některých kryptografických protokolů. Doporučili jsme bankám, jakých chyb se vyvarovat, pokud by chtěli v praxi implementovat koncept kvantových peněz. A také jsme sestrojili robota, který se naučil klonovat.

Z experimentálního hlediska je vidět určitý posun v použité technice. Neefektivní plynový laser po konci jeho několikrát prodlužované životnosti nahradil téměř „nesmrtelný“ polovodičový laser s osminásobným výkonem, přičemž jeho příkon je zlomkem toho plynového. Sofistikované kombinace nelineárních krystalů umožňují generovat fotonové páry s větší účinností a navíc entanglované v polarizaci. Výrobci vyvíjejí jednofotonové detektory se stále větší kvantovou účinností, klasickým lavinovým fotodiodám roste konkurence v podobě supravodivých nanovláken s kvantovou účinností větší jak 90 %. Nicméně jejich cena výrazně navýšená nezbytným kryostatem nedovoluje zatím jejich širšímu používání. Také se výrazně zjednodušila technika zpracování vícenásobných detekčních událostí. Schopnost nanosekundové digitalizace signálů ulehčila detekci vícenásobných koincidenčních událostí, už nejsou potřeba složitě pospojované moduly *Time-to-Amplitude* a *Single Channel Analyzer*, stačí jedna krabička v ceně půlky jednoho tohoto modulu.

Nicméně všechno mezi tím, mezi přípravou fotonových qubitů a detekcí, je víceméně po celé ty roky stejné. Jde jen o ten správný nápad, jak ty fázové destičky a děliče poskládat dohromady tak, aby prováděli takovou výslednou transformaci, která se od nich očekává.

Články autora komentované v práci

[A1] A. Černoch, L. Bartůšková, J. Soubusta, M. Ježek, J. Fiurášek a M. Dušek, „*Experimental phase-covariant cloning of polarization states of single photons*," Phys. Rev. A **74**, 042327 (2006).

[A2] K. Jiráková, K. Bartkiewicz, A. Černoch a K. Lemr, „*Experimentally attacking quantum money schemes based on quantum retrieval games*," Scientific Reports **9**, 16318 (2019).

[A3] J. Jašek, K. Jiráková, K. Bartkiewicz, A. Černoch, T. Fürst a K. Lemr, „*Experimental hybrid quantum-classical reinforcement learning by boson sampling: how to train a quantum cloner*," Optics Express **27**, 32454 (2019).

[A4] J. Soubusta, L. Bartůšková, A. Černoch, J. Fiurášek a M. Dušek, „*Several experimental realizations of symmetric phase-covariant quantum cloners of single-photon qubits*," Phys. Rev. A **76**, 042318 (2007).

[A5] L. Bartůšková, M. Dušek, A. Černoch, J. Soubusta a J. Fiurášek, „*Fiber-Optics Implementation of an Asymmetric Phase-Covariant Quantum Cloner*," Phys. Rev. Lett. **99**, 120505 (2007).

[A6] J. Soubusta, L. Bartůšková, A. Černoch, M. Dušek a J. Fiurášek, „*Experimental asymmetric phase-covariant quantum cloning of polarization qubits*," Phys. Rev. A **78**, 052323 (2008).

[A7] A. Černoch, J. Soubusta, L. Čelechovská, M. Dušek a J. Fiurášek, „*Experimental demonstration of optimal universal asymmetric quantum cloning of polarization states of single photons by partial symmetrization*," Phys. Rev. A **80**, 062306 (2009).

[A8] K. Lemr, K. Bartkiewicz, A. Černoch, J. Soubusta a A. Miranowicz, „*Experimental linear-optical implementation of a multifunctional optimal qubit cloner*," Phys. Rev. A **85**, 050307 (2012).

[A9] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta a A. Miranowicz, „*Experimental Eavesdropping Based on Optimal Quantum Cloning*," Phys. Rev. Lett. **110**, 173601 (2013).

[A10] K. Bartkiewicz, A. Černoch, K. Lemr, J. Soubusta a M. Stobińska, „*Efficient amplification of photonic qubits by optimal quantum cloning*," Phys. Rev. A **89**, 062322 (2014).

[A11] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz a F. Nori, „*Experimental quantum forgery of quantum optical money*," npj Quantum Information **3**, 7 (2017).

Ostatní citované práce autora

[A12] K. Bartkiewicz, A. Černoch, K. Lemr a A. Miranowicz, „*Priority Choice Experimental Two-Qubit Tomography: Measuring One by One All Elements of Density Matrices*," Scientific Reports **6**, 19610 (2016).

[A13] A. Černoch, J. Soubusta, L. Bartůšková, M. Dušek a J. Fiurášek, „*Experimental Realization of Linear-Optical Partial swap Gates*," Phys. Rev. Lett. **100**, 180501 (2008).

[A14] A. Černoch, J. Soubusta, L. Bartůšková, M. Dušek a J. Fiurášek, „*Experimental implementation of partial symmetrization and anti-symmetrization of two-qubit states*," New Journal of Physics **11**, 023005 (2009).

[A15] K. Lemr, A. Černoch, J. Soubusta a J. Fiurášek, „*Experimental preparation of two-photon Knill-Laflamme-Milburn states*," Phys. Rev. A **81**, 012321 (2010).

[A16] K. Lemr, A. Černoch, J. Soubusta, K. Kieling, J. Eisert a M. Dušek, „*Experimental Implementation of the Optimal Linear-Optical Controlled Phase Gate*," Phys. Rev. Lett. **106**, 013602 (2011).

[A17] J. Roik, K. Bartkiewicz, A. Černoch a K. Lemr, „*Accuracy of Entanglement Detection via Artificial Neural Networks and Human-Designed Entanglement Witnesses*," Physical Review Applied **15**, 054006 (2021).

[A18] J. Roik, K. Bartkiewicz, A. Černoch a K. Lemr, „*Entanglement quantification from collective measurements processed by machine learning*," Physics Letters A **446**, 128270 (2022).

[A19] J. Soubusta, A. Černoch, J. Fiurášek a M. Dušek, „*Experimental realization of a programmable quantum-state discriminator and a phase-covariant quantum multimeter*," Phys. Rev. A **69**, 052321 (2004).

[A20] A. Černoch, „*Experimentální přenos a zpracování informace v podobě polarizačního stavu fotonu*," dis. pr. (Univerzita Palackého, Olomouc, 2006) (cit. na s. 40, 41).

Použitá literatura ostatních autorů

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe a J. L. O'Brien, „*Quantum computers*," Nature **464**, 45–53 (2010).

[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro a S. Lloyd, „*Gaussian quantum information*," Rev. Mod. Phys. **84**, 621–669 (2012).

[3] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling a G. J. Milburn, „*Linear optical quantum computing with photonic qubits*," Rev. Mod. Phys. **79**, 135–174 (2007).

[4] M. A. Nielsen a I. L. Chuang, *Quantum computation and quantum information*, 1. vyd. (Cambridge University Press, 2000) (cit. na s. 3, 12).

[5] A. Galindo a M. A. Martín-Delgado, „*Information and computation: Classical and quantum aspects*," Rev. Mod. Phys. **74**, 347–423 (2002).

[6] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon a Y. Yamamoto, „*Indistinguishable photons from a single-photon device*," Nature **419**, 594–597 (2002).

[7] C. W. Chou, S. V. Polyakov, A. Kuzmich a H. J. Kimble, „*Single-Photon Generation from Stored Excitation in an Atomic Ensemble*," Phys. Rev. Lett. **92**, 213601 (2004).

[8] A. Kuhn, M. Hennrich a G. Rempe, „*Deterministic Single-Photon Source for Distributed Quantum Networking*," Phys. Rev. Lett. **89**, 067901 (2002).

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

[10] J. Soubusta, *Využití sestupné frekvenční parametrické konverze v optických experimentech*, habilitační práce, UP Olomouc, 2009 (cit. na s. 5, 25).

[11] M. Ježek, J. Fiurášek a Z. Hradil, „*Quantum inference of states and processes*," Phys. Rev. A **68**, 012305 (2003).

[12] G. Brassard, N. Lütkenhaus, T. Mor a B. C. Sanders, „*Limitations on Practical Quantum Cryptography*," Phys. Rev. Lett. **85**, 1330–1333 (2000).

[13] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer a V. Makarov, „*Full-field implementation of a perfect eavesdropper on a quantum cryptography system*," Nature Communications **2**, 349 (2011).

[14] P. Jouguet, S. Kunz-Jacques a E. Diamanti, „*Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution*," Phys. Rev. A **87**, 062313 (2013).

[15] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu a A. Sanpera, „*Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*," Phys. Rev. Lett. **77**, 2818–2821 (1996).

[16] E. Hutterer, „*Not Magic ... Quantum*," 1663 , 14–19 (2016).

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

[18] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven a J. M. Martinis, „*Quantum supremacy using a programmable superconducting processor*," Nature **574**, 505–510 (2019).

[19] M. Sparkes, *IBM creates largest ever superconducting quantum computer*, 2021, `https://www.newscientist.com/article/2297583-ibm-creates-largest-ever-superconducting-quantum-computer/` (cit. na str. 12).

[20] K. Nemoto a W. J. Munro, „*Nearly Deterministic Linear Optical Controlled-NOT Gate*," Phys. Rev. Lett. **93**, 250502 (2004).

[21] J. H. Shapiro, „*Single-photon Kerr nonlinearities do not help quantum computation*," Phys. Rev. A **73**, 062305 (2006).

[22] E. Knill, R. Laflamme a G. J. Milburn, „*A scheme for efficient quantum computation with linear optics*," Nature **409**, 46–52 (2001).

[23] S. Russell a P. Norvig, *Artificial Intelligence, A Modern Approach. Second Edition* (2003) (cit. na str. 13).

[24] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe a S. Lloyd, „*Quantum machine learning*," Nature **549**, 195 (2017).

[25] P. Rebentrost, M. Mohseni a S. Lloyd, „*Quantum Support Vector Machine for Big Data Classification*," Phys. Rev. Lett. **113**, 130503 (2014).

[26] J. Jašek, „*Machine learning for quantum gate optimization*," dipl. pr. (Palacky University, 2020) (cit. na s. 13, 51).

[27] W. K. Wootters a W. H. Żurek, „*A single quantum cannot be cloned*," Nature **299**, 802–803 (1982).

[28] V. Bužek a M. Hillery, „*Quantum copying: Beyond the no-cloning theorem*," Phys. Rev. A **54**, 1844–1852 (1996).

[29] V. Scarani, S. Iblisdir, N. Gisin a A. Acín, „*Quantum cloning*," Rev. Mod. Phys. **77**, 1225–1256 (2005).

[30] L.-M. Duan a G.-C. Guo, „*Probabilistic Cloning and Identification of Linearly Independent Quantum States*," Physical Review Letters **80**, 4999–5002 (1998).

[31] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello a J. A. Smolin, „*Optimal universal and state-dependent quantum cloning*," Phys. Rev. A **57**, 2368–2378 (1998).

[32] C. H. Bennett a G. Brassard, „*Quantum cryptography: Public key distribution and coin tossing*," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175**, 8 (1984).

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

[34] J. Fiurášek, „*Optical implementations of the optimal phase-covariant quantum cloning machine*," Phys. Rev. A **67**, 052314 (2003).

[35] K. Bartkiewicz, A. Miranowicz a Ş. K. Özdemir, „*Optimal mirror phase-covariant cloning*," Phys. Rev. A **80**, 032306 (2009).

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

[37] H. Fan, K. Matsumoto a M. Wadati, „*Quantum cloning machines of a d -level system*," Phys. Rev. A **64**, 064301 (2001).

[38] N. Gisin a S. Massar, „*Optimal Quantum Cloning Machines*," Phys. Rev. Lett. **79**, 2153–2156 (1997).

[39] F. Buscemi, G. M. D'Ariano a C. Macchiavello, „*Economical phase-covariant cloning of qudits*," Phys. Rev. A **71**, 042327 (2005).

[40] F. D. Martini, F. Sciarrino a C. Vitelli, „*Entanglement Test on a Microscopic-Macroscopic System*," Phys. Rev. Lett. **100**, 253601 (2008).

[41] R. T. Glasser, H. Cable, J. P. Dowling, F. De Martini, F. Sciarrino a C. Vitelli, „*Entanglement-seeded, dual, optical parametric amplification: Applications to quantum imaging and metrology*," Phys. Rev. A **78**, 012339 (2008).

[42] N. Spagnolo, C. Vitelli, V. G. Lucivero, V. Giovannetti, L. Maccone a F. Sciarrino, „*Phase Estimation via Quantum Interferometry for Noisy Detectors*," Phys. Rev. Lett. **108**, 233602 (2012).

[43] C. Vitelli, N. Spagnolo, L. Toffoli, F. Sciarrino a F. De Martini, „*Enhanced Resolution of Lossy Interferometry by Coherent Amplification of Single Photons*," Phys. Rev. Lett. **105**, 113602 (2010).

[44] M. Curty a T. Moroder, „*Heralded-qubit amplifiers for practical device-independent quantum key distribution*," Phys. Rev. A **84**, 010304 (2011).

[45] N. Gisin, S. Pironio a N. Sangouard, „*Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier*," Phys. Rev. Lett. **105**, 070501 (2010).

[46] A. Carlini a M. Sasaki, „*Geometrical conditions for completely positive trace-preserving maps and their application to a quantum repeater and a state-dependent quantum cloning machine*," Phys. Rev. A **68**, 042327 (2003).

[47] S. Fasel, N. Gisin, G. Ribordy, V. Scarani a H. Zbinden, „*Quantum Cloning with an Optical Fiber Amplifier*," Phys. Rev. Lett. **89**, 107901 (2002).

[48] A. Lamas-Linares, C. Simon, J. C. Howell a D. Bouwmeester, „*Experimental Quantum Cloning of Single Photons*," Science **296**, 712–714 (2002).

[49] F. D. Martini, D. Pelliccia a F. Sciarrino, „*Contextual, Optimal, and Universal Realization of the Quantum Cloning Machine and of the NOT Gate*," Phys. Rev. Lett. **92**, 067901 (2004).

[50] M. Ricci, F. Sciarrino, C. Sias a F. De Martini, „*Teleportation Scheme Implementing the Universal Optimal Quantum Cloning Machine and the Universal NOT Gate*," Phys. Rev. Lett. **92**, 047901 (2004).

[51] W. T. M. Irvine, A. Lamas Linares, M. J. A. de Dood a D. Bouwmeester, „*Optimal Quantum Cloning on a Beam Splitter*," Phys. Rev. Lett. **92**, 047902 (2004).

[52] I. Ali Khan a J. C. Howell, „*Hong-Ou-Mandel cloning: Quantum copying without an ancilla*," Phys. Rev. A **70**, 010303 (2004).

[53] Z. Zhao, A.-N. Zhang, X.-Q. Zhou, Y.-A. Chen, C.-Y. Lu, A. Karlsson a Jian-Wei Pan, „*Experimental Realization of Optimal Asymmetric Cloning and Telecloning via Partial Teleportation*," Phys. Rev. Lett. **95**, 030502 (2005).

[54] L. Masullo, M. Ricci a F. De Martini, „*Generalized universal cloning and purification in quantum information by multistep state symmetrization*," Phys. Rev. A **72**, 060304 (2005).

[55] R. F. Werner, „*Optimal cloning of pure states*," Phys. Rev. A **58**, 1827–1832 (1998).

[56] F. Sciarrino a F. De Martini, „*Realization of the optimal phase-covariant quantum cloning machine*," Phys. Rev. A **72**, 062313 (2005).

[57] J.-S. Xu, C.-F. Li, L. Chen, X.-B. Zou a G.-C. Guo, „*Experimental realization of the optimal universal and phase-covariant quantum cloning machines*," Phys. Rev. A **78**, 032322 (2008).

[58] L. T. Knoll, I. H. L. Grande a M. A. Larotonda, „*A photonic quantum simulator for phase covariant clonin*," quant-ph **1705.04704** (2017).

[59] M.-D. Choi, „*Completely positive linear maps on complex matrices*," Linear Algebra and its Applications **10**, 285 (1975).

[60] A. Jamiołkowski, „*An effective method of investigation of positive maps on the set of positive definite operators*," Reports on Mathematical Physics **5**, 415 (1974).

[61] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar a V. Makarov, „*Hacking commercial quantum cryptography systems by tailored bright illumination*," Nature Photonics **4**, 686 (2010).

[62] P. W. Shor a J. Preskill, „*Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*," Phys. Rev. Lett. **85**, 441–444 (2000).

[63] N. Lütkenhaus, „*Security against eavesdropping in quantum cryptography*," Phys. Rev. A **54**, 97–111 (1996).

[64] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu a A. Peres, „*Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy*," Phys. Rev. A **56**, 1163–1172 (1997).

[65] N. Gisin a B. Huttner, „*Quantum cloning, eavesdropping and Bell's inequality*," Physics Letters A **228**, 13–21 (1997).

[66] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis a E. Diamanti, „*Experimental investigation of practical unforgeable quantum money*," npj Quantum Information **4**, 5 (2018).

[67] J. M. Arrazola, M. Karasamanis a N. Lütkenhaus, „*Practical quantum retrieval games*," Phys. Rev. A **93**, 062311 (2016).