Metodický list: Protokol BB84

Cíl:	Praktické představení kvantové kryptografie studentům, konkrétně nejstaršího šifrovacího protokolu BB84.
Charakter aktivity:	laboratorní práce
Potřebný čas:	2 vyučovací hodiny
Cílová skupina:	SŠ studenti (fyzika – optika, kvantová fyzika)
Vyučovací metody:	experimentování, řešení problémů
Doporučené znalosti:	polarizace světla
Potřeby a materiál:[1]	• stavebnice O3Q s moduly: – baterie, – tlačítko, – LED, – čočka (65 mm), – „Alicin“ polarizátor (2 ks – jeden pro orientaci $+$, resp. orientaci $\times$), – dělič svazku, – zrcátko (stočené o $45°$ vzhledem ke stěnám modulu), – „Bobův“ polarizátor, – stínítko (2 ks), – deska, na níž se moduly umisťují, – hrací kostky (4 ks – dva pro orientaci, resp. bit) • pracovní list Protokol BB84

Toto je metodický list k aktivitě „Protokol BB84“, která je primárně zamýšlena jako dvouhodinové laboratorní cvičení pro SŠ studenty v předmětu fyzika.

Naleznete zde *tipy a vysvětlení* (psány kurzívou) k vedení tohoto laboratorního cvičení, přibližnou časovou náročnost jednotlivých částí a řešení úkolů z pracovního listu.

Průběh aktivity

Úvod (5 min)

V úvodní části hodiny se studenti rozdělí do skupinek (optimální je práce ve trojicích až čtveřicích, záleží na celkovém počtu studentů a množství stavebnic). Vyučující rozdá studentům:

[1] Počty pomůcek jsou vztaženy na skupinu studentů.

- pracovní listy k aktivitě, které obsahují všechny potřebné informace, díky čemuž mohou studenti pracovat samostatně,
- stavebnice O3Q (viz obrázek 1) s moduly:
  - baterie,
  - tlačítko,
  - LED,
  - čočka (65 mm),
  - „Alicin“ polarizátor (2 ks – pro orientaci $+$, resp. orientaci $\times$),
  - dělič svazku (polopropustné zrcátko),
  - zrcátko (stočené o $45°$ vzhledem ke stěnám modulu),
  - „Bobův“ polarizátor,
  - stínítko (2 ks),
  - deska, na níž se moduly umisťují,
  - hrací kostky[2] (ideálně 4 ks – pro 2 ks orientaci, resp. 2 ks bit).

Klasické šifrování (15 min)

První část pracovního listu, která obsahuje tři úkoly, je zaměřena na představení Caesarovy šifry. Je na ni však nahlíženo kriticky jako na šifru pro potřeby dnešní doby silně nedostačující. Proto je zde snaha o její vylepšení.

Kvantová kryptografie (50 min)

Klasickými metodami však nelze docílit našich požadavků na šifru (šifra využívá silný klíč, který je dlouhý v ideálním případě stejně jako šifrovaná zpráva a zároveň náhodný, výroba klíče bude bezpečná, případně nám dát navíc informaci o tom, zda někdo odposlouchával), ale je to možné pomocí metody založené na principech kvantové fyziky. Studenti se seznámí s prvním kvantovým protokolem BB84. Skupinky studentů se pro plnění úkolů se simulací protokolu ještě rozdělí na dvě části a hraním rolí odesílatelky Alice a příjemce Boba vytvoří šifrovací klíč a poté jej i aplikují při šifrování, resp. dešifrování zprávy.

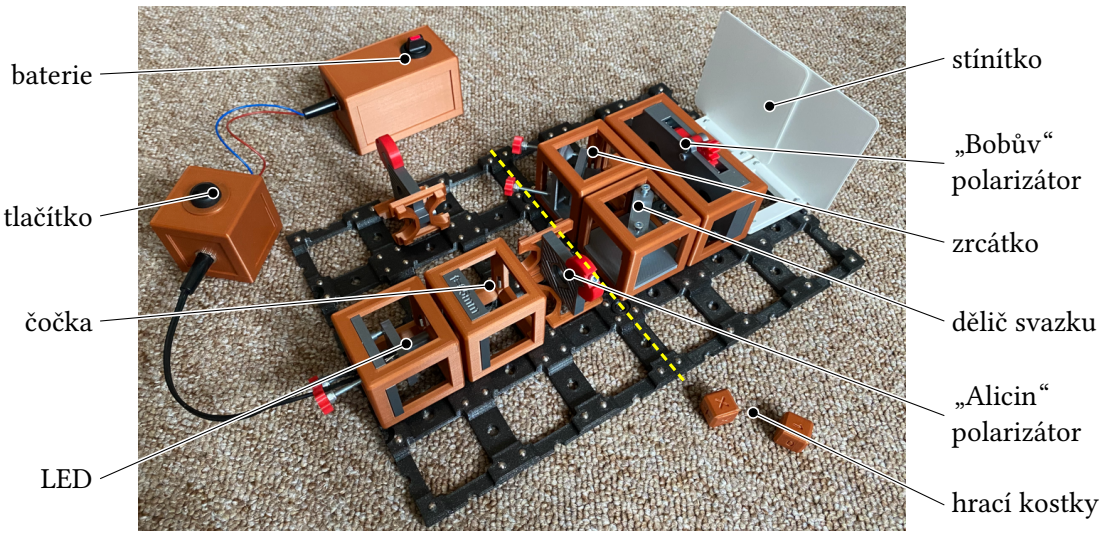
Na závěr je ještě diskutováno, jakým způsobem lze odhalit případné nežádoucí odposlechy.

Co je dobré vědět?

Jak protokol BB84 probíhá?

Popis průběhu protokolu BB84 se ve formě několika návodů k úkolům rovněž nachází v pracovním listu, zde však uvádíme shrnutí, které může být nápomocné v případě reflexe aktivity.

[2] V případě nedostatku kostek, které využíváme k simulaci náhody, lze použít např. mince nebo normální hrací kostky – v obou případech je ale potřeba dohodnout, jakým orientacím, resp. hodnotám bitu jednotlivé možnosti odpovídají.



Obrázek 1 Fotografie sestavené aparatury (Alici patří část vlevo a Bobovi část vpravo)

1. Alice posílá Bobovi náhodně polarizované fotony. Existují přitom dvě různé orientace polarizátorů, s nimiž měří, každá se dvěma směry polarizace – celkem tedy čtyři různé směry polarizace. Zároveň si Alice zaznamenává, jakou orientaci použila a v jakém směru byl poslaný foton polarizován.

2. Bob zvolí náhodně orientaci, přijme foton od Alice a změří směr jeho polarizace pomocí polarizačních filtrů se zvolenou orientací. Údaje o orientaci a směru polarizace si zaznamenává.

3. Po ukončení přenosu celého klíče, tj. po zaslání všech fotonů, si Alice s Bobem porovnají orientace polarizátorů, které v jednotlivých měřeních používali. Toto porovnání na rozdíl od předchozích kroků už probíhá pomocí veřejného kanálu. Pro bezpečnost celého procesu je důležité, že porovnávají pouze orientace, nikoliv směry polarizace.

4. Oba dále uvažují pouze ta měření, v nichž měřili se stejnými orientacemi, a ostatní měření „vyškrtnou“. Jedná se o přibližně polovinu všech měření, která provedli. U ponechaných měření převedou naměřené směry polarizace na odpovídající hodnoty bitů a oba tak získávají shodný klíč složený z nul a jedniček.

5. Posledním krokem je porovnání několika číslic v klíči. Účelem tohoto je odhalení případného odposlechu, který by způsobil odlišnosti cca ve čtvrtině číslic klíče. Pokud nejsou odhaleny nesrovnalosti, pak se zveřejněné číslice z klíče také „vyškrtnou“ a k šifrování se použije kratší klíč. V případě, že by k odhalení došlo, je potřeba provést proces znovu úplně od začátku a na jiném kvantovém kanálu, který nebude odposlouchávaný.

Před samotnou hodinou vřele doporučujeme si protokol BB84 vyzkoušet. Jednou z variant je pomocí stavebnice – nespornou výhodou je, že si aparaturu sami vyzkoušíte sestavit a seznámíte se tedy s jednotlivými moduly, zároveň vám bude jasnější, jak správně nastavit polarizátory do požadovaného směru v jednotlivých orientacích. Nabízí se rovněž využití apletů, zde doporučujeme aplet QuVis, který je dostupný v češtině na internetových stránkách https://fyzweb.cz/materialy/kvantovka/BB84_photons/BB84_photons.html.

Proč jsou na Bobově stínítku v některých případech dvě stopy?

Dvě stopy, které mají velmi podobnou intenzitu, se na Bobově stínítku objevují v momentě, kdy se orientace „Alicina“ polarizátoru liší od toho Bobova. Je pravda, že někdy se dvě stopy objeví i v momentě, kdy jsou orientace stejné – jedna ze stop je však o dost méně výrazná. V tomto případě je to způsobeno použitím levných polarizačních fólií v polarizátorech. Pokud bychom se však zabývali situacemi, v nichž jsou orientace obou polarizátorů stejné a stopy jsou podobně jasné, je tento jev způsoben použitím našeho stavebnicového modelu. Tím, že v našem modelu svícením LED diodou posíláme světelný svazek (mnoho fotonů), se objeví dvě stopy. Oba Bobovy filtry svírají se směrem polarizace zaslaného světelného svazku úhel $45°$, takže je stejná pravděpodobnost, že světlo projde, jako že neprojde, proto Bob vidí na stínítku dvě stopy se stejným jasem, který je v praxi asi poloviční v porovnání s tím, pokud by filtry nepoužil.

Pokud bychom posílali skutečně jeden jediný foton a měřili jeho směr polarizace, získáme jen jednu stopu. Po tom, co Alice připraví foton s určitým směrem polarizace, putuje foton k Bobovi a v případě, že Bob nastaví tutéž orientaci polarizátoru co Alice, změří foton se stejným směrem polarizace jako ona, Bob vidí tedy na stínítku jedinou stopu. V případě, že by však měřil s druhou orientací, nedalo by se před měřením s jistotou říct, který ze směrů Bob změří. Foton se totiž před samotným měřením nachází ve stavu, který kombinuje oba možné směry polarizace orientace polarizátoru (tzv. superponovaný stav). V případě, že je stav fotonu superponovaný, lze před samotným měřením říct pouze s jakou pravděpodobností je možné jednotlivé směry polarizace v dané orientaci naměřit. Bob musí zvolit jen jeden z filtrů, který je v jeho orientaci. Ať zvolí kterýkoli z nich, je stejná pravděpodobnost (jelikož orientace jsou navzájem pootočeny o $45°$), že foton od Alice jím projde jako, že neprojde. Podle toho Bob pozná, zda naměřil daný směr, nebo směr druhý. Až při měření se rozhodne směr polarizace fotonu a superponovaný stav se změní na tzv. vlastní stav, tj. takový, který je jedním ze směrů polarizace v orientaci.

Tento nedostatek modelu, který způsobí, že při zvolení různých orientací polarizátorů u jednotlivých aktérů se na Bobově stínítku objeví dvě podobně jasné stopy, lze vykompenzovat výběrem směru polarizace hodem hrací kostkou, která má roli náhody.

Proč si Alice s Bobem rovnou nesdělí orientace polarizátorů, s nimiž měří, ale dělají to až po měření?

Jednoduše proto, že předchozí či okamžité sdělení orientací polarizátorů, s nimiž Alice a Bob měří, vede v momentě, kdy jsou odposlouchávání Evou a Eva by měla v tom případě v průběhu svého měření tuto informaci k dispozici, v podstatě k prozrazení klíče.

Eva díky této znalosti může měřit rovnou ve správné orientaci, díky čemuž získává údaje o klíči a zároveň ji nelze při odposlechu odhalit. Měření s náhodnými orientacemi je tedy pro fungování protokolu klíčové.

Proč si Eva „nenakopíruje“ před svým měřením foton od Alice?

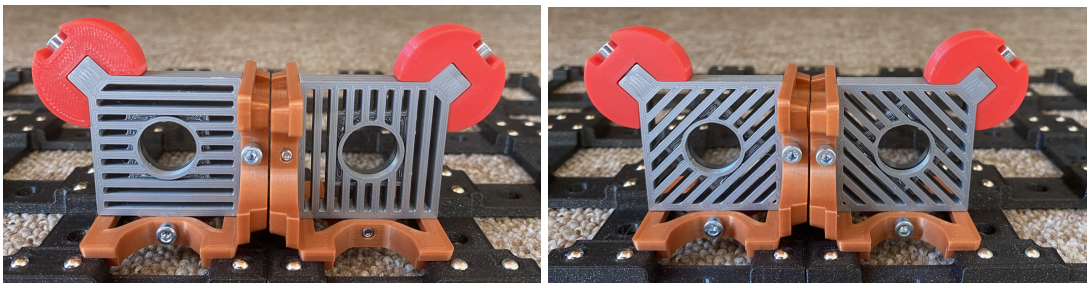
Okopírování kvantového stavu jednoho fotonu na jiný foton prostě podle principů kvantové fyziky není možné. Říká se tomu neklonovací teorém (anglicky *no-cloning theorem*), který ukazuje, že pokud je foton v neznámém stavu, pak nelze vytvořit druhý foton v tomtéž stavu, aniž bychom pozměnily stav fotonu prvního.[3] Pro Evu je stav Alicina fotonu opravdu neznámý kvůli tomu, že Alice volí orientaci polarizátoru náhodně.

Eva by si tak jedině mohla fotony od Alice schovat, Bobovi poslat nějaké jiné a změřit směry polarizace těch Aliciných až po porovnání orientací. Tím, že však poslala Bobovi náhodně polarizované fotony, způsobí opět chybovost klíče (a to vyšší, než kdyby měřila rovnou a posílala Bobovi fotony se změřeným směrem polarizace), takže by byla i v tomto případě odhalena právě při porovnání číslic v klíči.

Jak správně nastavit při měření polarizátor?

Kromě ukázek nastavení polarizátorů na obrázcích 2 a 3, je vhodné zmínit, že velmi nápomocné při určování nastavení „Alicina“ polarizátoru jsou „pruhové štěrbiny“ na něm, které názorně naznačují směr polarizace.

Rovněž stojí za zmínku fakt, že Alici pro celý experiment stačí pouze dva polarizátory – jeden polarizátor s orientací $+$, resp. $\times$. Ač by se mohlo z obrázku 2 mohlo zdát, že jsou potřeba čtyři, je možné umístit polarizátor na desku dvěma způsoby navzájem pootočenými o $90°$ a získat tak druhý ze směrů polarizace v dané orientaci.



(a) Vlevo $|\leftrightarrow\rangle$ (bit 0) a vpravo $|\updownarrow\rangle$ (bit 1)

(b) Vlevo $|\nearrow\rangle$ (bit 1) a vpravo $|\nwarrow\rangle$ (bit 0)

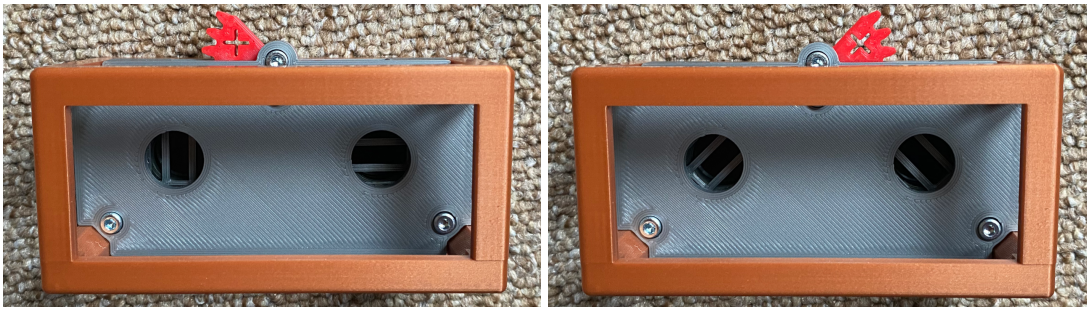
Obrázek 2 Všechny varianty nastavení „Aliciných“ polarizátorů

V případě „Bobova“ polarizátoru (viz obrázek 3) stačí k experimentu jeden kus, přičemž v jeden moment jsou nastaveny na polarizátoru oba směry polarizace ve zvolené orientaci, kterou lze vidět na červeném dílku na vrchu polarizátoru. Mezi orientacemi se přechází stlačením červeného dílku, čímž se polarizační filtry otočí o $45°$ a zaujmou směry polarizace druhé orientace.

Bob vlastně používá dva polarizátory zároveň (oba jsou zabudované v jednom modulu) a díky děliči svazku, umístěnému před nimi, měří v obou směrech dané orientace. Toto by při posílání jednoho fotonu opravdu nešlo a je to řešení jen v našem modelu, který při rozsvícení LED diody posílá mnohem více fotonů než jeden.

[3] Neznámý stav však lze přenést z fotonu na jiný foton. Ten první ovšem bude nakonec v jiném stavu než na začátku. Stav původního fotonu tedy nenávratně pozměníme. Tato technika se nazývá kvantová teleportace.

Při určování konkrétního směru polarizace u Boba doporučujeme rovněž sledovat pozorně stopu na stínítku, z níž je rovněž směr polarizace patrný, díky dvojici stínů vytvořených pomocí přepážek umístěných u polarizačních filtrů.



(a) Vlevo $|\updownarrow\rangle$ (bit 1) a vpravo $|\leftrightarrow\rangle$ (bit 0)

(b) Vlevo $|\nearrow\rangle$ (bit 1) a vpravo $|\nwarrow\rangle$ (bit 0)

Obrázek 3 Všechny varianty nastavení „Bobova“ polarizátoru

Řešení a vysvětlení úkolů

Úkol 1.1

Pro kontrolu šifrování můžete využít online nástroje, zde se nabízí např. na webových stránkách `https://cryptii.com/pipes/caesar-cipher` v angličtině nebo `https://www.matweb.cz/caesarova-sifra/` v češtině.

Úkol 1.2

Klasickou Caesarovu šifru není obtížné prolomit ani hrubou silou. Kvůli tomu, že je v abecedě 26 písmen, existuje právě 26 možností, jak zprávu zašifrovat (resp. 25, jelikož při jedné by byla šifra identická se zprávou). Stačí tedy projít všechny možnosti. K prolomení šifry proto nejsou potřeba pokročilejší nástroje jako např. frekvenční analýza výskytu písmen v daném jazyce.

Úkol 1.3

Pro kontrolu šifrování můžete využít online nástroje, zde se nabízí např. na webových stránkách `https://cryptii.com/pipes/vigenere-cipher` v angličtině nebo `https://www.matweb.cz/vigenerova-sifra/` v češtině.

Úkol 2.1

Uvedené sérii směrů polarizace $|\updownarrow\rangle$ $|\nearrow\rangle$ $|\nwarrow\rangle$ $|\updownarrow\rangle$ $|\leftrightarrow\rangle$ $|\nwarrow\rangle$ jednoznačně odpovídá posloupnost $1\,1\,0\,1\,0\,0$.

Úkol 2.2

Uvedenou sérii bitů $1\,0\,0\,1\,0\,1$ lze přepsat na libovolnou posloupnost směrů polarizací, která má:

- na první pozici buď $|\updownarrow\rangle$, nebo $|\swarrow\!\!\nearrow\rangle$,
- na druhé pozici buď $|\leftrightarrow\rangle$, nebo $|\nwarrow\!\!\searrow\rangle$,
- na třetí pozici buď $|\leftrightarrow\rangle$, nebo $|\nwarrow\!\!\searrow\rangle$,
- na čtvrté pozici buď $|\updownarrow\rangle$, nebo $|\swarrow\!\!\nearrow\rangle$,
- na páté pozici buď $|\leftrightarrow\rangle$, nebo $|\nwarrow\!\!\searrow\rangle$,
- na šesté pozici buď $|\updownarrow\rangle$, nebo $|\swarrow\!\!\nearrow\rangle$.

Povšimněme si, že v tomto směru, tj. ze série bitů na posloupnost směrů polarizací, není jedna správná možnost, jak tomu bylo v předchozím úkolů, nýbrž je tu nejednoznačnost. Toto je důležité pro bezpečnost tvorby klíče v protokolu BB84. Můžete na to proto studenty případně nějak upozornit.

Úkoly 2.3 a 2.4

Vygenerování stejných klíčů a následné poslání zašifrované zprávy a její dešifrování je ověřením, že se klíč podařilo předat.

Alice i Bob tedy mají stejný klíč, díky němuž je jeden schopen dešifrovat zprávu, kterou druhý zašifroval.

Úkol 2.5

Pokud Alice Bobovi odeslala foton se směrem $|\swarrow\!\!\nearrow\rangle$, tedy bit 1 v orientaci $\times$, který však zachytila Eva, naměří Eva jednotlivé směry s pravděpodobností P podle tabulky 1. V levé polovině tabulky jsou měření, při nichž Eva používá polarizátor s orientací $\times$, v pravé polovině potom s polarizátorem s orientací $+$.

Eva dostala foton $\|\swarrow\!\!\nearrow\rangle$ a měří s orientací $\times$			Eva dostala foton $\|\swarrow\!\!\nearrow\rangle$ a měří s orientací $+$		
směr	**bit**	P	**směr**	**bit**	P
$\|\swarrow\!\!\nearrow\rangle$	1	100 %	$\|\updownarrow\rangle$	1	50 %
$\|\nwarrow\!\!\searrow\rangle$	0	0 %	$\|\leftrightarrow\rangle$	0	50 %

Tabulka 1 Řešení úkolu 2.5

Úkol 2.6

Alice Bobovi odeslala foton se směrem $|\swarrow\!\!\nearrow\rangle$, tedy bit 1 v orientaci $\times$, který však zachytila Eva, která měřila s orientací $+$. Eva změřila polarizaci $|\updownarrow\rangle$, tj. bit 1. Takto polarizovaný foton poslala dále Bobovi.

V tabulce 2 je zaznamenáno, s jakou pravděpodobností P změří Bob foton s jedním ze směrů v orientaci $\times$.

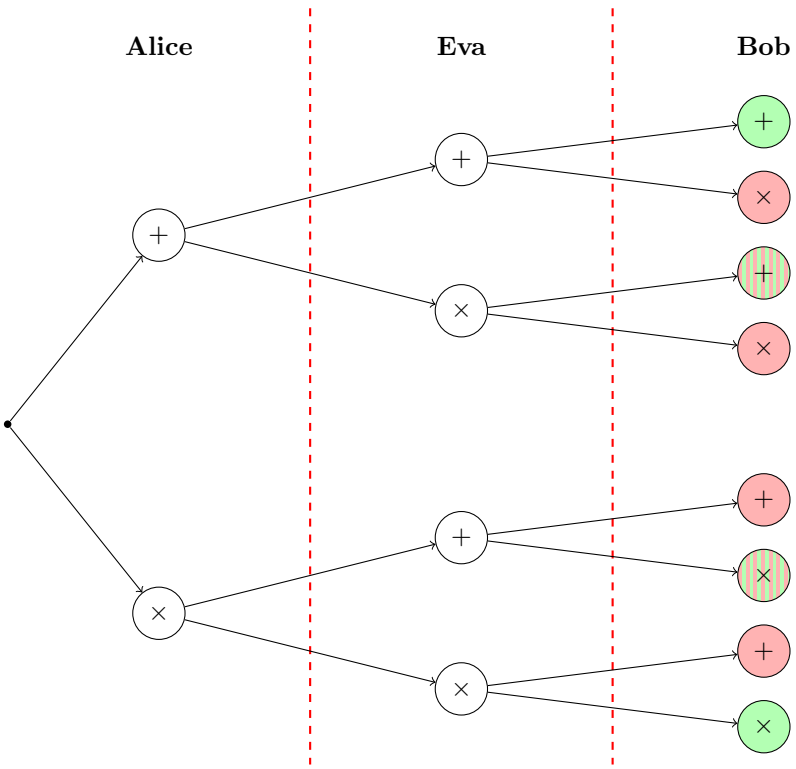
Bob dostal foton $\vert\updownarrow\rangle$ a měří s orientací $\times$		
směr	**bit**	P
$\vert\nearrow\rangle$	1	50 %
$\vert\nwarrow\rangle$	0	50 %

Tabulka 2 Řešení úkolu 2.6

Úkol 2.7

Pokud Eva odposlouchává a všichni účastnící volí náhodně orientace svých polarizátorů, s nimiž měří, lze očekávat 25% chybovost v číslicích klíčů. Jedná se tedy o rozdíly v tom, co zbyde, po „vyškrtání“ výsledků měření, kdy používali odlišně orientované polarizátory.

Pojďme rozebrat, jaké varianty mohou při měření nastat. Využijeme k tomu obrázek 4, který zobrazuje, jaké varianty mohou při volbě orientací jednotlivými aktéry nastat.



Obrázek 4 Všechny varianty volby orientací polarizátorů, význam barev je vysvětlen v textu

V případě, že se zvolené orientace polarizátorů Alice, Evy i Boba shodují (na obrázku 4 vyznačeno zeleně), změří všichni stejné směry polarizace. Tato měření přispívají číslicemi do klíče a tyto číslice se u Alice a Boba neliší.

Další varianty měření, která můžeme „vyškrtnout“, jelikož k chybovosti klíče nepřispívají, jsou ta, kde má Alice nastavenou jinou orientaci než Bob (na obrázku 4 vyznačeny červeně). Tato měření se totiž k tvorbě klíče vůbec nepoužijí.

Poslední dvě varianty, které nám zbyly (na obrázku 4 vyznačeny zeleno-červenými proužky), jsou případy, kdy Alice a Bob měří sice ve stejných orientacích, nicméně Eva má orientaci polarizátoru nastavenou odlišně. V těchto případech má Bob vždy 50% šanci, že u sfotonu naměří stejný směr polarizace jako u fotonu, který mu Alice poslala – taková měření opět žádné rozdíly v klíčích obou nezpůsobí. Kde však už problém nastane je právě těch zbylých 50 % případů, kdy se směry polarizace u Alice a Boba budou zaviněním Evy lišit. Tyto případy pak jako jediné způsobí to, že se číslice v Alicině klíči cca z jedné čtvrtiny nebudou shodovat s číslicemi Bobova klíče.