PATENTOVÝ SPIS

(11) Číslo dokumentu:
310 249
(13) Druh dokumentu: **B6**
(51) Int. Cl.:

G06F 21/60	(2013.01)
H04L 9/00	(2022.01)
H04B 3/00	(2006.01)
H04B 10/2575	(2013.01)

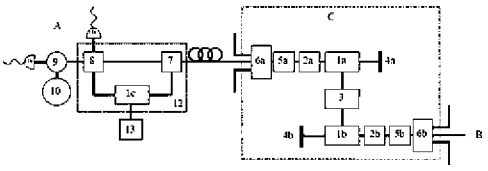
(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2023-350**
(22) Přihlášeno: **11.09.2023**
(40) Zveřejněno: **01.01.2025**
(Věstník č. 1/2025)
(47) Uděleno: **21.11.2024**
(24) Oznámení o udělení ve věstníku: **01.01.2025**
(Věstník č. 1/2025)

(56) Relevantní dokumenty:
CN 110233670 A; CN 109274491 A; WO 2017084380 A1; US 8041039 B2; CZ 283044 B6; CN 104579643 B.

(73) Majitel patentu:
České vysoké učení technické v Praze, Praha 6, Dejvice, CZ
(72) Původce:
Ing. Jiří Weiss, Pardubice, Svítkov, CZ
(74) Zástupce:
Mgr. Michal Poljak, Nové sady 988/2, 602 00 Brno, Staré Brno



(54) Název vynálezu:
Centrální uzel pro dvousměrný kvantový přenos šifrovacího klíče v síti typu „hvězda“, zapojení centrálního uzlu a způsob dvousměrného kvantového přenosu

(57) Anotace:
Předmětem vynálezu je centrální uzel (C) pro dvousměrný kvantový přenos šifrovacího klíče mezi alespoň dvěma periferními zařízeními (A, B) v síti typu „hvězda“. Centrální uzel (C) obsahuje jednak první optický spínač (6a), první polarizační kontrolér (5a), první fázový modulátor (1a) a první Faradayovo zrcadlo (4a), jednak druhý optický spínač (6b), druhý polarizační kontrolér (5b), druhý fázový modulátor (1b) a druhé Faradayovo zrcadlo (4b), a jednak generátor (3) náhodných čísel připojený k prvnímu a druhému fázovému modulátoru (1a, 1b). Komponenty jsou zapojeny lineárně v pořadí optický snímač (6a, 6b), polarizační kontrolér (5a, 5b), fázový modulátor (1a, 1b) a Faradayovo zrcadlo (4a, 4b), kde optické spínače (6a, 6b) jsou připojitelné k prvnímu, resp. druhému periferního zařízení (A, B) přes kvantový kanál. Předmětem vynálezu je dále zapojení centrálního uzlu (C), alespoň jednoho prvního a alespoň jednoho druhého periferního zařízení (A, B), a rovněž způsob dvousměrného kvantového přenosu šifrovacího klíče pomocí uvedeného zapojení.

CZ 310249 B6

Centrální uzel pro dvousměrný kvantový přenos šifrovacího klíče v síti typu „hvězda“, zapojení centrálního uzlu a způsob dvousměrného kvantového přenosu

Oblast techniky

Tento vynález se týká centrálního uzlu, jeho zapojení s periferními zařízeními a způsobu pro dvousměrný kvantový přenos šifrovacího klíče mezi alespoň dvěma periferními zařízeními a centrálním uzlem v síti typu „hvězda“.

Dosavadní stav techniky

Kvantový přenos šifrovacího klíče (QKD, „quantum key distribution“) je bezpečná komunikační metoda implementující šifrovací protokol na základě kvantové mechaniky. Umožňuje dvěma stranám generovat sdílený náhodný tajný klíč, který je známý pouze jim a který lze následně použít k šifrování a dešifrování zpráv. Příkladem protokolu pro kvantový přenos šifrovacího klíče je protokol označený jako BB84, kde BB84 odkazuje na jména jeho vynálezců, Charlese Bennetta a Gillese Brassarda, a na rok vynalezení 1984.

V současnosti jsou v sítích používány centrální uzly typu point-to-point pro jednosměrný kvantový přenos šifrovacího klíče. Jejich kombinací v jednom uzlu lze vytvořit uzel umožňující dvousměrný kvantový přenos šifrovacího klíče, avšak je navíc nutné použít systém managmentu klíče (KMS, „key management system“) pro manipulaci s klíči a jejich přerozdělování mezi jednotlivými periferními zařízeními.

Pro účely tohoto popisu se klasickým informačním kanálem (nebo klasickým kanálem) rozumí komunikační kanál neumožňující přenos kvantové informace, např. optický kabel pro vedení světla nebo elektrický kabel pro vedení elektrického proudu. Pro účely tohoto popisu se kvantovým kanálem rozumí komunikační kanál umožňující přenos kvantové informace, např. kvantového stavu qubitu (kvantového bitu).

V americkém patentu US 10432395 B2 je popsán blíže nespecifikovaný dvousměrný a nepřetržitý kvantový přenos šifrovacího klíče mezi prvním zařízením (odesílatelem) a druhým zařízením (příjemcem) přes centrální uzel.

V americkém patentu US 11483140 B2 je popsán blíže nespecifikovaný dvousměrný kvantový přenos šifrovacího klíče mezi periferními uživatelskými zařízeními přes vícero centrálních uzlů.

V americkém patentu US 8903094 B2 je popsán opakovací uzel (repeater node), který neumožňuje distribuci šifrovacích klíčů dalším neautorizovaným stranám, tedy zajišťuje bezpečný přenos. Kvantový přenos šifrovacího klíče je pouze jednosměrný a pracuje s protokolem BB84.

V americkém patentu US 10630469 B2 je popsán centrální uzel (relay), který zahrnuje generátor náhodných čísel. Na obr. 7 tohoto patentu vedou dva opačné komunikační kanály mezi centrálním uzlem a serverem. Kvantový přenos šifrovacího klíče je pouze jednosměrný a pracuje s protokolem BB84.

V britském patentu GB 2581528 A je na obr. 3 tohoto patentu popsán centrální uzel (intermediate/repeater node) typu point-to-point s přenosem klíče pomocí one-time-pad. Kryptografický klíč KR1 se nejdříve připojí v periferním zařízení ke klíči K12, dojde k přenosu mezi prvním periferním zařízením a centrálním uzlem, v centrálním uzlu se odpojí a připojí ke klíči K23, dojde k přenosu mezi centrálním uzlem a druhým periferním zařízením, kde se klíč KR1 odpojí od klíče K23. Kvantový přenos šifrovacího klíče je pouze jednosměrný a pracuje

s protokolem BB84 s časově-fázovým kódováním (viz fázové modulátory na obr. 2 tohoto patentu). Pro uvedené předání klíče se obvykle používá KMS.

V evropském patentu EP 2003812 B1 je na obr. 4 tohoto patentu popsán centrální uzel typu point-to-point, který umožňuje pouze jednosměrný kvantový přenos šifrovacího klíče. Detektory jsou zapojeny v centrálním uzlu a fázový modulátor pro kódování bitů v periferním zařízení. Tento systém pracuje s protokolem BB84 typu alternativně posunuté fázové modulace v plug-and-play zařízení.

V čínské patentové přihlášce CN 110233670 A je popsán systém a síť pro kvantový přenos šifrovacího klíče, obsahující centrální uzel pro dvousměrný kvantový přenos šifrovacího klíče. Tento centrální uzel obsahuje: první sadu optoelektronických komponent, kromě jiného zahrnující první optický spínač, první polarizační kontrolér a první fázový modulátor; a druhou sadu optoelektronických komponent, kromě jiného zahrnující druhý optický spínač. První optický spínač je připojitelný k prvnímu periferním zařízení přes kvantový kanál a druhý optický spínač je připojitelný k druhému periferním zařízení přes kvantový kanál. Tento centrální uzel obsahuje vysílací, distribuční a měřicí jednotku. Periferní uzly slouží pouze ke kódování logických bitů do fáze vysílaných impulzů. Dvousměrný kvantový přenos šifrovacího klíče je závislý, tj. impulzy se šíří na sobě závisle a po neoddělených trasách. Systém je založen na interferenci dvou optických impulzů, do kterých je zašifrována informace o přenášeném logickém bitu a které jsou tlumeny na úroveň jednotlivých fotonů. Šifrování logických bitů se provádí změnou fáze v optickém impulzu (báze X nebo Y) příslušným fázovým modulátorem. Vzhledem k nutné interferenci obou optických impulzů v „master“ zařízení, je jejich překryv v čase na „děliči/slučovači“ zaručován šířením po stejné optické trase (tj. stejně dlouhé trase), avšak v opačném směru. Šifrovací klíč je generován mezi dvěma účastníky současně a pro výběr účastníka se používá optický spínač (switch). Systém vyžaduje kontrolu stavu polarizace pomocí polarizačních kontrolérů vzhledem k použití šifrování logických bitů do fáze impulzu a fázových modulátorů citlivých na stav polarizace.

V čínské patentové přihlášce CN 109274491 A je popsáno síť a způsob pro kvantový přenos šifrovacího klíče mezi více uživateli. Centrální uzel je vybaven pouze optickým spínačem („quantum switching node“), je tedy pasivním člen generace šifrovacího klíče a neumožňuje dvousměrný kvantový přenos šifrovacího klíče. Řešení využívá vlnového slučování kombinovaný s architekturou typu „Broadcast&select“ (tj. podle vlnové délky). Je uvedeno použití koherentního vícevlnného zdroje pro přenos kvantového signálu. Každá vlnová délka je poté nezávisle modulována tak, že logické bity jsou zašifrovány do změny fáze záření, a signál se šíří od Alice k m kombinovaným uzlům Carol, které signál zpracují. Dále je vybraný uzel Carol spojen s n přijímacími uzly Bob a opět podle vlnové délky je těmto uzlům poslán modulovaný signál. Využívá se jevu superpozice a pomocí nevyváženého interferometru se generuje výsledný kvantový stav. Není jasné, zdali generace klíče probíhá nejprve a nezávisle mezi Alicí a všemi uzly Carol a poté nezávisle mezi vybraným uzlem Carol a všemi uzly (podle vlnové délky) Bob. Není jasné, jak přesně probíhá distribuce jednotlivých fotonů na jednotlivých vlnových délkách přijímacím uzlům Bob. Síť využívá WDM technologii (technologii vlnového multiplexu, „wavelength-division multiplexing“), nicméně tato technologie vyžaduje vícevlnový zdroj záření a podle počtu vlnových délek i patřičný počet fázových modulátorů. Není jasné, zda signál obsahuje větší počet fotonů pro zaručení, že alespoň nějaký foton o patřičné vlnové délce se prošíří až k patřičnému přijímacímu uzlu Bob. Jelikož WDM demultiplexer je umístěn až v uzlu Bob, a za předpokladu, že kvantový optický přepínač je dělič typu 1 x n s rovnoměrným dělením, je nutné prozkoumat splnění podmínky bezpečnosti kvantového přenosu klíče. Další nevýhodou je nutná teplotní stabilizace všech uzlů.

V mezinárodní patentové přihlášce WO 2017084380 A1 je popsán způsob pro kvantový přenos šifrovacího klíče, podle autorů obzvláště vhodný pro technologii typu „Continuous Variable“ QKD. Je popsána rovněž digitální řídicí jednotka pro určení povahy signálu a následného procesu, která je schopná získat informaci z kvantového i klasického optického signálu. Tento

způsob využívá šifrování logických bitů do fáze záření a nevyužívá centrální uzel. Uzel Alice slouží k vysílání impulzů uzlu Bob (i naopak). Polarizační dělič svazku se používá k oddělení kvantové a klasické informace. Dvousměrný kvantový přenos šifrovacího klíče sice je možný, avšak pouze jako zdvojení přenosu typu bod-bod a bez možnosti přepínání mezi uživateli. Alice přeposílá kvantové stavy Bobovi, a ten zároveň posílá kvantové stavy zpět Alici (podle obr. 2b uvedeného spisu po odděleném kanálu).

V americkém patentu US 8041039 B2 je popsán způsob a systém pro kvantový přenos šifrovacího klíče za použití kvantového přenosu šifrovacího klíče tzv. typu one-way a plug&play. Periferní uzly Alice slouží k přijímání vysílaných impulzů centrálním uzlem Bob. Nicméně, generace klíče mezi centrálním uzlem Bob a periferními uzly Alice probíhá sekvenčně, tedy nejdříve Alice 1, pak Alice 2 atd. Tento způsob neumožňuje současný kvantový přenos šifrovacího klíče dvěma periferním zařízením (Alice) zároveň. Pro síť typu multipoint-to-miltipoint je popsána funkce nadstavbového systému, tzv. Key Management System, kde je v tomto případě nejprve vygenerován samostatný klíč v uzlu Bob a poté je s pomocí Vernamovy šifry (tj. one-time pad) přeposlán patřičným uzlům Alice. Tento způsob využívá šifrování logických bitů do fáze záření. Systém obsahuje generátor náhodných čísel (RNG) pro určení šifrovaného bitu a šifrovací báze, a fázový modulátor.

V českém patentu CZ 283044 B6 je popsán způsob pro kvantovou kryptografickou identifikaci s pomocí identifikační karty. Způsob je využitelný k identifikaci oprávněného uživatele a vzájemná identifikace se děje mezi identifikační kartou a interferometrickým, kvantově kryptografickým, identifikaci ověřujícím přístrojem v souladu s kvantově kryptografickým protokolem. Tento způsob využívá šifrování logických bitů do fáze záření. Nicméně, tento způsob nevyužívá centrální uzel, neumožňuje současný kvantový přenos šifrovacího klíče dvěma periferním zařízením (Alice) zároveň, ani nepodporuje kvantový přenos šifrovacího klíče (a jeho generaci) pro užití pro přenos šifrované informace klasickým kanálem pomocí symetrického kryptosystému. Tento způsob slouží k identifikaci oprávněného uživatele, nikoliv ke generaci náhodného klíče pro následné užití v symetrickém kryptosystému a k přenosu dat.

V čínském patentu CN 104579643 B je popsán způsob a systém pro kvantový přenos šifrovacího klíče, založený na metodě kvantového přenosu šifrovacího klíče, nezávislého na měřicím zařízení (tzv. „measurement device-independent quantum key distribution“). Způsob s výhodou redukuje standardní počet uzlů ze tří na dva (jedním z uzlů je centrální uzel) a má samokompenzující schopnost akumulované fáze a akumulovaných změn polarizace při šíření záření optickým vláknem. Jedná se tedy o „fázově modulované polarizační šifrování“. Systém obsahuje fázový modulátor, generátor náhodných čísel, Faradayovo zrcadlo i polarizační kontrolér. Způsob dále popisuje generaci klíče mezi párem Alice a Bob, nepopisuje však generaci klíče mezi jiným, volitelným párem Alice a Bob, a tudíž není „síťovým“ řešením a nejedná se o dvousměrný kvantový přenos šifrovacího klíče. Měření v tomto způsobu je založeno na tzv. Bellově měření.

Nevýhodou výše uvedených systémů je možnost pouze jednosměrného kvantového přenosu šifrovacího klíče, případně dvousměrného kvantového přenosu šifrovacího klíče pouze s nadstavbovým systémem managmentu klíče (KMS).

Ve stavu techniky tedy vzniká potřeba poskytnout centrální uzel, jeho zapojení s periferními zařízeními a odpovídající způsob umožňující dvousměrný kvantový přenos šifrovacího klíče bez nutnosti nadstavbového systému managmentu klíče (KMS).

Podstata vynálezu

Cílem vynálezu je poskytnout centrální uzel jeho zapojení s periferními zařízeními a odpovídající způsob umožňující dvousměrný kvantový přenos šifrovacího klíče bez nutnosti nadstavbového systému managmentu klíče (KMS).

Uvedeného cíle je v prvním aspektu tohoto vynálezu dosaženo centrálním uzlem pro dvousměrný kvantový přenos šifrovacího klíče mezi alespoň dvěma periferními zařízeními v síti typu „hvězda“. Tento centrální uzel obsahuje:

a. první sadu optoelektronických komponent, zahrnující první optický spínač, první polarizační kontrolér, první fázový modulátor a první Faradayovo zrcadlo, přičemž uvedené komponenty jsou zapojeny lineárně v pořadí první optický spínač, první polarizační kontrolér, první fázový modulátor a první Faradayovo zrcadlo, kde první optický spínač je připojitelný k prvnímu periferním zařízení přes kvantový kanál;

b. druhou sadu optoelektronických komponent zahrnující druhý optický spínač, druhý polarizační kontrolér, druhý fázový modulátor a druhé Faradayovo zrcadlo, přičemž uvedené komponenty jsou zapojeny lineárně v pořadí druhý optický spínač, druhý polarizační kontrolér, druhý variabilní optický zeslabovač, druhý fázový modulátor a druhé Faradayovo zrcadlo, kde druhý optický spínač je připojitelný k druhému periferním zařízení přes kvantový kanál; a

c. generátor náhodných čísel připojený k prvnímu a druhému fázovému modulátoru.

Podstata centrálního uzlu podle tohoto vynálezu spočívá v tom, že generátor náhodných čísel je připojen k prvnímu i k druhému fázovému modulátoru. Generátor náhodných čísel (v kombinaci s řídicí elektronikou) tedy propojuje dvě „odrazné“ části pro plug-and-play konfiguraci do jednoho centrálního uzlu. Propojení umožní kódování stejných bitů do posílaných kvantových stavů a přeposlání takových stavů dvěma periferním zařízením zároveň. Důsledkem použití tohoto centrálního uzlu v kvantové síti typu „hvězda“ je odlišný algoritmus pro prosévání (sifting) detekovaných qubitů.

První a druhý optický spínač slouží k otevření a uzavření kvantových kanálů mezi centrálním uzlem a periferními zařízeními. První a druhý polarizační kontrolér slouží k nastavení stavu polarizace pro správnou modulaci korektního impulzu a výslednou detekci. Tyto prvky obecně slouží k zajištění úspěšného přenosu kvantových stavů mezi periferními zařízeními a centrálním uzlem.

První a druhý fázový modulátor slouží k modulaci druhého, v čase zpožděného impulzu z periferního zařízení (viz níže, odstavec pojednávající nevyvážený Machův-Zehnderův interferometr). Modulace je řízena vnitřní elektronikou a (kvantovým) generátorem náhodných čísel podle vnitřního rozhodovacího algoritmu. Kvantové stavy z obou periferních zařízení jsou fázově modulovány stejně, což tvoří podstatu uvedeného centrálního uzlu.

První a druhé Faradayovo zrcadlo slouží k otočení stavu polarizace záření o 90° a k odražení takto ortogonálně polarizovaného záření zpět do periferních zařízení, s odpovídající modulací a útlumem.

První a druhá sada optoelektronických komponent jsou s výhodou zapojeny do konfigurace plug-and-play pro protokol BB84.

Výhodou centrálního uzlu podle tohoto vynálezu je současné vysílání qubitů dvěma směry, tj. ve dvou volitelných periferních zařízeních dojde k vygenerování stejného symetrického klíče zároveň. To v případě použití zařízení pro point-to-point komunikaci nelze, přičemž tento nedostatek se dnes překlenuje použitím nadstavbového systému KMS pro distribuci symetrického klíče s použitím, například, one-time-pad šifrování. Tato výhoda je dána konstrukcí centrálního uzlu a na tom postavené celé kvantové sítě. Centrální uzel je navržen pro síť využívající např. kvantový protokol BB84 s časově-fázovým kódováním přenášených bitů v zapojení plug-and-play.

Další výhodou centrálního uzlu podle tohoto vynálezu je ekonomičtější výroba, jelikož jeden centrální uzel dokáže obhospodařovat N periferních zařízení, která tím pádem můžou být stejné konstrukce. Výroba jednoho stejného periferního zařízení zefektivňuje výrobní linku.

S výhodou je první a/nebo druhý optický spínač typu 1xN (tj. 1 vstup z centrálního uzlu a N výstupů do periferních zařízení), kde $N \geq 1$ pro připojení více prvních a/nebo druhých periferních zařízení, čímž lze vytvořit síť typu „hvězda".

S výhodou je mezi prvním polarizačním kontrolérem a prvním fázovým modulátorem nebo mezi prvním optickým spínačem a prvním polarizačním kontrolérem zapojen první variabilní optický zeslabovač a rovněž je mezi druhým polarizačním kontrolérem a druhým fázovým modulátorem nebo mezi druhým optickým spínačem a druhým polarizačním kontrolérem zapojen druhý variabilní optický zeslabovač. První a druhý variabilní optický zeslabovač slouží k nastavení stavu útlumu pro zajištění informační bezpečnosti použitého protokolu. Impulzy záření jsou variabilním optickým zeslabovačem tlumeny na úroveň jednotlivých fotonů. Variabilní optické zeslabovače nejsou v centrálním uzlu nutné v případě použití jednofotonového zdroje.

S výhodou je mezi prvním optickým spínačem a s ním sousedící komponentou zvolenou z prvního polarizačního kontroléru a prvního variabilního optického zeslabovače zapojen první nesymetrický dělič svazku, za kterým je zapojen první pomocný fotodetektor, jakož i mezi druhým optickým spínačem a s ním sousedící komponentou zvolenou z druhého polarizačního kontroléru a druhého variabilního optického zeslabovače je zapojen druhý nesymetrický dělič svazku, za kterým je zapojen druhý pomocný fotodetektor k nastavení časování a periody impulzů pro správnou modulaci korektního impulzu a pro synchronizaci časování impulzů a detekci výkonu záření. Nesymetrický dělič svazku slouží k oddělení části signálu pro pomocný fotodetektor.

Uvedeného cíle je v druhém aspektu tohoto vynálezu dosaženo zapojením výše uvedeného centrálního uzlu, alespoň jednoho prvního periferního zařízení a alespoň jednoho druhého periferního zařízení. Každé periferní zařízení je s centrálním uzlem spojeno přes klasický informační kanál a kvantový kanál, kde spojení periferního zařízení s centrálním uzlem přes klasický informační kanál je přímé nebo nepřímé. Pod spojením periferního zařízení a centrálního uzlu přes klasický informační kanál se tedy rozumí i jakékoliv nepřímé spojení, kde je centrální uzel spojen přes klasický informační kanál s okolím, a v rámci tohoto okolí se informace může přenést do periferního zařízení např. přes sérii routerů. Každé periferní zařízení obsahuje zdroj záření, první detektor, druhý detektor a nevyvážený Machův-Zehnderův interferometr obsahující polarizační dělič svazku, symetrický dělič svazku (tzv. 50:50 dělič svazku) a třetí fázový modulátor. První optický spínač centrálního uzlu je připojen k polarizačnímu děliči svazku prvního periferního zařízení a druhý optický spínač centrálního uzlu je připojen k polarizačnímu děliči svazku druhého periferního zařízení. Polarizační dělič svazku každého periferního zařízení je dále připojen k symetrickému děliči svazku přímo (jednou větví) a přes třetí fázový modulátor (další větví). Symetrický dělič svazku je dále připojen k zdroji záření, prvnímu detektoru a druhému detektoru. Třetí fázový modulátor je připojen ke generátoru náhodných čísel periferního zařízení.

Nevyvážený Machův-Zehnderův interferometr má jedno rameno delší než druhé. Impulz záření generovaný zdrojem záření prochází nevyváženým Machovým-Zehnderovým interferometrem, čímž vzniká první, v čase nezpožděný impulz procházející kratším ramenem a druhý, v čase zpožděný impulz procházejícím delším ramenem. Druhý, v čase zpožděný impulz je v centrálním uzlu fázově modulován pomocí generátoru náhodných čísel, což platí pro impulzy z obou periferních zařízení stejně (viz výše). Odražením od Faradayova zrcadla zpět k nevyváženému Machovu-Zehnderovu interferometru dochází i k ortogonalizaci polarizace záření. Kombinací polarizačního děliče svazku a třetího fázového modulátoru však nyní prochází delším ramenem první, v čase nezpožděný impulz (s ortogonální polarizací), což umožňuje modulovat fázi

prvního, v čase nezpožděného impulzu. Modulace je řízena vnitřní elektronikou a (kvantovým) generátorem náhodných čísel každého periferního zařízení podle vnitřního rozhodovacího algoritmu. Kvantové stavy v obou periferních zařízení jsou fázově modulovány nezávisle, s výhodou podle protokolu BB84 s časově-fázovým kódováním.

Následná detekce na detektorech je závislá na modulaci impulzů v centrálním uzlu a v obou periferních zařízeních, s výhodou podle protokolu BB84 s časově-fázovým kódováním. Detektory jsou s výhodou lavinové fotodiody.

S výhodou je symetrický dělič svazku připojen k druhému detektoru přímo a k zdroji záření a prvnímu detektoru přes optický cirkulátor.

Uvedeného cíle je v třetím aspektu tohoto vynálezu dosaženo způsobem dvousměrného kvantového přenosu šifrovacího klíče pomocí výše uvedeného zapojení mezi dvěma periferními zařízeními přes centrální uzel v síti typu „hvězda“.

V prvním kroku je vytvořeno spojení mezi dvěma periferními zařízeními a centrálním uzlem přes kvantový kanál sepnutím optických spínačů na základě požadavku periferních zařízení centrálnímu uzlu přes klasický informační kanál. Periferní zařízení oznámí centrálnímu uzlu svůj záměr po klasickém informačním kanálu. Centrální uzel požadavek potvrdí nebo odmítne. V případě odmítnutí, zařadí požadavek periferních zařízení do fronty požadavků a po jejich vyřízení, akceptuje požadavek periferních zařízení.

V druhém kroku je provedena volitelná modulace impulzu mezi oběma periferními zařízeními a centrálním uzlem pomocí optických spínačů, s výhodou v kombinaci s nesymetrickými děliči svazku a pomocnými fotodetektory (časování a perioda impulzů), a/nebo polarizačních kontrolérů (stav polarizace) a/nebo variabilních optických zeslabovačů (stav útlumu). Volitelná modulace je výsledkem kontroly kvality kvantového kanálu s úmyslem úspěšného přenosu kvantových stavů mezi periferními zařízeními a centrálním uzlem.

V třetím kroku je odeslán impulz z obou periferních zařízení do centrálního uzlu přes nevyvážený Machův-Zehnderův interferometr pro vytvoření prvního, v čase nezpožděného impulzu (který prochází kratším ramenem) a druhého, v čase zpožděného impulzu (který prochází delším ramenem) z obou periferních zařízení.

Ve čtvrtém kroku je provedena modulace fáze druhého, v čase zpožděného impulzu z obou periferních zařízení fázovým modulátorem, s výhodou podle protokolu BB84 s časově-fázovým kódováním. Tato modulace je řízena generátorem náhodných čísel tak, že druhý, v čase zpožděný impulz z obou periferních zařízení je modulován stejně, což tvoří podstatu tohoto způsobu.

V pátém kroku jsou odraženy impulzy od Faradayových zrcadel, čímž se mění polarizace všech impulzů na ortogonální.

V šestém kroku jsou vráceny impulzy s ortogonální polarizací do obou periferních zařízení přes nevyvážený Machův-Zehnderův interferometr a je provedena modulace fáze prvního, v čase nezpožděného impulzu (dosud fázově nemodulovaného) z centrálního uzlu třetím fázovým modulátorem, s výhodou podle protokolu BB84 s časově-fázovým kódováním. Tato modulace je řízena generátorem náhodných čísel a vnitřní elektronikou každého periferního zařízení zvlášť.

V sedmém kroku dochází za symetrickým děličem svazku k interferenci prvního, v čase nezpožděného impulzu a druhého, v čase zpožděného impulzu, a následně je detekován výsledek interference obou impulzů v prvním detektoru nebo v druhém detektoru každého periferního zařízení na základě fázové modulace impulzů v centrálním uzlu a obou periferních zařízeních, s výhodou podle protokolu BB84 s časově-fázovým kódováním. V optimálním případě se jedná o detekci jednoho fotonu na buď jednom, nebo druhém detektoru, nikoliv na obou detektorech

zároveň. Může však dojít k situacím, kdy se foton ztratí a na detektorech není detekován žádný signál, nebo se nemusí jednat o jednofotonové impulzy a poté může nastat koincidence na obou detektorech. Může dojít i na náhodné vygenerování signálu na detektoru s nenulovou pravděpodobností a tedy např. k detekci „více“ fotonů.

V osmém kroku jsou porovnány detekční báze u shodně detekovaných impulzů mezi oběma periferními zařízeními přes klasický informační kanál. Pokud pro konkrétní impulz použila periferní zařízení stejnou detekční bázi, výsledek měření si ponechají, ostatní výsledky měření zahazují. Následně obě periferní zařízení porovnají přes klasický kanál svou detekční bázi s šifrovací bází centrálního uzlu. Pokud pro konkrétní impulz použila periferní zařízení stejnou detekční bázi jako centrální uzel šifrovací bázi, výsledek měření si ponechají, ostatní výsledky měření zahazují.

S výhodou se v osmém kroku šifrovací a detekční báze u shodně detekovaných impulzů porovnají mezi oběma periferními zařízeními navzájem a mezi každým periferním zařízením a centrálním uzlem, což umožňuje trojí porovnání shodně detekovaných impulzů.

Alternativně se v osmém kroku šifrovací a detekční báze u shodně detekovaných impulzů porovnají mezi každým periferním zařízením a centrálním uzlem (ale nikoliv mezi periferními zařízeními navzájem), načež si obě periferní zařízení navzájem sdělí, zda pro daný impulz se shodnou šifrovací a detekční bází došlo k detekci impulzu v obou periferních zařízeních.

S výhodou následuje v devátém kroku proces odhadu parametrů (parametr estimation), proces korekce chyb (error correction) a proces amplifikace soukromí (privacy amplicifation) v obou periferních zařízeních a při vzájemné komunikaci. Například pro proces amplifikace soukromí si po klasickém informačním kanálu periferní zařízení vymění tzv. seed, což je krátká sekvence bitů, podle něhož určí, jakou hashovací funkci použijí pro generování bezpečného šifrovacího klíče ze zbylých bitů. Tím vzniká bezpečný symetrický šifrovací klíč v obou periferních zařízeních, např. o délce 256 bitů.

Objasnění výkresů

Obrázek 1 znázorňuje zapojení periferního zařízení a centrálního uzlu.

Obrázek 2 znázorňuje zapojení periferního zařízení a centrálního uzlu s pomocnými fotodetektory.

Příklady uskutečnění vynálezu

Příklad 1

Prvním příkladem uskutečnění je zapojení centrálního uzlu C a prvního periferního zařízení A (obr. 1). Druhé periferní zařízení B je zapojeno k centrálnímu uzlu C symetricky po vzoru prvního periferního zařízení A (neznázorněno). Každé periferní zařízení A, B je s centrálním uzlem C spojeno přes klasický informační kanál (neznázorněno) a kvantový kanál.

Centrální uzel C obsahuje první sadu optoelektronických komponent, zahrnující první optický spínač 6a typu 1xN (kde $N \geq 1$), první polarizační kontrolér 5a, první variabilní optický zeslabovač 2a, první fázový modulátor 1a a první Faradayovo zrcadlo 4a. Uvedené komponenty jsou zapojeny lineárně v uvedeném pořadí, kde první optický spínač 6a je připojen k prvnímu periferímu zařízení A přes kvantový kanál. Mezi prvním optickým spínačem 6a a prvním polarizačním kontrolérem 5a může být zapojen první nesymetrický dělič 14a svazku, za kterým

je zapojen první pomocný fotodetektor 15a pro synchronizaci časování impulzů a detekci výkonu záření (obr. 2).

Centrální uzel C dále obsahuje druhou sadu optoelektronických komponent zahrnující druhý optický spínač 6b typu 1xN (kde N ≥1), druhý polarizační kontrolér 5b, druhý variabilní optický zeslabovač 2b, druhý fázový modulátor 1b a druhé Faradayovo zrcadlo 4b. Uvedené komponenty jsou zapojeny lineárně v uvedeném pořadí, kde druhý optický spínač 6b je připojen k druhému periferním zařízení B přes kvantový kanál. Mezi druhým optickým spínačem 6b a druhým polarizačním kontrolérem 5b může být zapojen druhý nesymetrický dělič 14b svazku, za kterým je zapojen druhý pomocný fotodetektor 15b synchronizaci časování impulzů a detekci výkonu záření (obr. 2).

Centrální uzel C dále obsahuje generátor 3 náhodných čísel připojený k prvnímu a druhému fázovému modulátoru 1a, 1b.

Každé periferní zařízení A, B obsahuje zdroj 10 záření, první detektor 11a, druhý detektor 11b a nevyvážený Machův-Zehnderův interferometr 12 obsahující polarizační dělič 7 svazku, symetrický dělič 8 svazku a třetí fázový modulátor 1c. Centrální uzel C (konkrétně první/druhý optický spínač 6a/6b) je připojen k polarizačnímu děliči 7 svazku, který je dále připojen k symetrickému děliči 8 svazku přímo a přes třetí fázový modulátor 1c. Symetrický dělič 8 svazku je dále připojen k zdroji 10 záření a prvnímu detektoru 11a (přes optický cirkulátor 9) a k druhému detektoru 11b (přímo). Třetí fázový modulátor 1c je připojen ke generátoru 13 náhodných čísel periferního zařízení A, B.

Příklad 2

Druhým příkladem uskutečnění je způsob dvousměrného kvantového přenosu šifrovacího klíče pomocí výše uvedeného zapojení mezi dvěma periferními zařízeními A, B (Alice, Bob) přes centrální uzel C (Charlie) v síti typu „hvězda“.

Dvě periferní zařízení, $Alice_i$ a Bob_j, se přes klasický informační kanál dohodnou, že navážou komunikaci s centrálním uzlem, Charliem, za účelem generace společného symetrického klíče.

$Alice_i$ a Bob_j oznámí Charliemu svůj záměr po klasickém informačním kanálu. Centrální uzel požadavek potvrdí nebo odmítne. V případě odmítnutí, zařadí požadavek $Alice_i$ a $Boba_j$ do fronty požadavků a po jejich vyřízení, akceptuje požadavek $Alice_i$ a $Boba_j$.

Charlie otevře kvantové kanály $Alice_i$ – Charlie, Bob_j – Charlie užitím optických spínačů 6a, 6b.

$Alice_i$, Bob_j a centrální uzel Charlie zkontrolují kvalitu kvantového kanálu $Alice_i$ – Charlie, Bob_j – Charlie, a případně nastaví patřičné parametry (časování impulzů, periodu impulzů, stav polarizace a útlumu) tak, aby došlo k úspěšnému přenosu kvantových stavů mezi $Alicí_i$ – Charliem a $Bobem_j$ – Charliem. Synchronizace časování a periody je nutná pro správnou modulaci korektního impulzu. Řízení stavu polarizace záření je nutné pro správnou modulaci korektního impulzu a výslednou detekci. Řízení útlumu je nutné pro zajištění informační bezpečnosti použitého protokolu.

$Alice_i$ (Bob_j) pošle směrem k Charliemu impulz záření, ten prochází skrze nevyvážený Machův.Zehnderův interferometr 12, a takovýto stav (první, v čase nezpožděný impulz a druhý, v čase zpožděný impulz) postupuje směrem k Charliemu.

Stavy (od $Alice_i$ a $Boba_j$) přicházejí do Charlieho, kde je fáze druhého, v čase zpožděného impulzu patřičně modulována ve fázových modulátorech 1a, 1b, s výhodou podle protokolu BB84 s časově-fázovým kódováním. Modulace je řízena vnitřní elektronikou a (kvantovým) generátorem náhodných čísel 3 podle vnitřního rozhodovacího algoritmu. Stavy $Alice_i$ a $Boba_j$

jsou fázově modulovány stejně. Současná stejná obousměrná modulace je podstatou uvedeného řešení.

Stavy se odráží od Faradayových zrcadel 4a, 4b a vrací se zpět do $Alice_i$ a $Boba_j$ řádně modulovány a utlumeny a s ortogonálním stavem polarizace (oproti příchozím impulzům).

Stavy záření prochází opět nevyváženým Machovým-Zehnderovým interferometrem 12. Ovšem díky ortogonálnímu stavu polarizace a polarizačnímu děliči svazku 7 prochází odlišnými rameny nevyváženého Machova-Zehnderova interferometru 12 než původně. To umožňuje modulovat fázi prvního, v čase nezpožděného impulzu, s výhodou podle protokolu BB84 s časově-fázovým kódováním, přičemž za symetrickým děličem 8 svazku následuje interference obou impulzů. Modulace impulzů v $Alice_i$ a $Bobovi_j$ je řízena vnitřní elektronikou a generátorem 13 náhodných čísel.

Následná detekce na detektorech buď 11a nebo 11b je závislá na modulaci impulzů v Charliem a v $Alice_i$ a $Bobovi_j$, s výhodou podle protokolu BB84 s časově-fázovým kódováním.

$Alice_i$ a Bob_j po klasickém informačním kanálu porovnají, které impulzy oba shodně detekovali (stavy odpovídající stejnému bitu). Následuje prosévání klíče (tzv. sifting), kde $Alice_i$ a Bob_j po klasickém informačním kanálu kontaktují Charlieho a porovnají si použité šifrovací a detekční báze u shodně detekovaných impulzů. Pokud pro konkrétní impulz použili stejnou šifrovací a detekční bázi, výsledek měření si ponechají. Ostatní výsledky měření zahazují. Výhodou je trojí porovnání shodně detekovaných impulzů mezi A_i-B_j, A_i-C a B_j-C. Následují proces odhadu parametrů, proces korekce chyb a proces amplifikace soukromí. Výsledkem je bezpečný symetrický šifrovací klíč o zvolené délce (např. 256 bitů) v periferních zařízeních $Alice_i$ a Bob_j.

Průmyslová využitelnost

Výše popsaný centrální uzel, jeho zapojení s periferními zařízeními a výše popsaný způsob lze využít v sítích s kvantovým přenosem šifrovacího klíče, které umožní zabezpečenou komunikaci i v případě dosažení nadřazenosti kvantových počítačů (quantum supremacy) a položí základy pro tzv. kvantový internet.

PATENTOVÉ NÁROKY

1. Centrální uzel (C) pro dvousměrný kvantový přenos šifrovacího klíče mezi alespoň dvěma periferními zařízeními (A, B) v síti typu „hvězda“, obsahující:
a. první sadu optoelektronických komponent, zahrnující první optický spínač (6a), první polarizační kontrolér (5a) a první fázový modulátor (1a), přičemž první optický spínač (6a) je připojitelný k prvnímu periferním zařízení (A) přes kvantový kanál;
b. druhou sadu optoelektronických komponent, zahrnující druhý optický spínač (6b), přičemž druhý optický spínač (6b) je připojitelný k druhému periferním zařízení (B) přes kvantový kanál,
vyznačující se tím, že první sada optoelektronických komponent dále zahrnuje první Faradayovo zrcadlo (4a), přičemž uvedené komponenty jsou zapojeny lineárně v pořadí první optický spínač (6a), první polarizační kontrolér (5a), první fázový modulátor (1a) a první Faradayovo zrcadlo (4a);
přičemž druhá sada optoelektronických komponent dále zahrnuje druhý polarizační kontrolér (5b), druhý fázový modulátor (1b) a druhé Faradayovo zrcadlo (4b), přičemž uvedené komponenty jsou zapojeny lineárně v pořadí druhý optický spínač (6b), druhý polarizační kontrolér (5b), druhý fázový modulátor (1b) a druhé Faradayovo zrcadlo (4b),
přičemž centrální uzel (C) dále obsahuje:
c. generátor (3) náhodných čísel připojený k prvnímu a druhému fázovému modulátoru (1a, 1b).

2. Centrální uzel (C) podle nároku 1, **vyznačující se tím**, že první a/nebo druhý optický spínač (6a, 6b) je typu 1xN, kde $N \geq 1$ pro připojení více prvních a/nebo druhých periferních zařízení (A, B).

3. Centrální uzel (C) podle nároku 1 nebo 2, **vyznačující se tím**, že mezi prvním polarizačním kontrolérem (5a) a prvním fázovým modulátorem (1a) nebo že mezi prvním optickým spínačem (6a) a prvním polarizačním kontrolérem (5a) je zapojen první variabilní optický zeslabovač (2a), přičemž mezi druhým polarizačním kontrolérem (5b) a druhým fázovým modulátorem (1b) nebo že mezi druhým optickým spínačem (6b) a druhým polarizačním kontrolérem (5b) je zapojen druhý variabilní optický zeslabovač (2b).

4. Centrální uzel (C) podle kteréhokoliv z předchozích nároků, **vyznačující se tím**, že mezi prvním optickým spínačem (6a) a s ním sousedící komponentou zvolenou z prvního polarizačního kontroléru (5a) a prvního variabilního optického zeslabovače (2a) je zapojen první nesymetrický dělič (14a) svazku, za kterým je zapojen první pomocný fotodetektor (15a),

přičemž mezi druhým optickým spínačem (6b) a s ním sousedící komponentou zvolenou z druhého polarizačního kontroléru (5b) a druhého variabilního optického zeslabovače (2b) je zapojen druhý nesymetrický dělič (14b) svazku, za kterým je zapojen druhý pomocný fotodetektor (15b).

5. Zapojení centrálního uzlu (C) podle kteréhokoliv z předchozích nároků, alespoň jednoho prvního periferního zařízení (A) a alespoň jednoho druhého periferního zařízení (B), přičemž každé periferní zařízení (A, B) je s centrálním uzlem (C) spojeno přes klasický informační kanál a kvantový kanál, kde spojení periferního zařízení (A, B) s centrálním uzlem (C) přes klasický informační kanál je přímé nebo nepřímé, **vyznačující se tím**, že každé periferní zařízení (A, B) obsahuje zdroj (10) záření, první detektor (11a), druhý detektor (11b) a nevyvážený Machův-Zehnderův interferometr (12) obsahující polarizační dělič (7) svazku, symetrický dělič (8) svazku a třetí fázový modulátor (1c), přičemž první optický spínač (6a) centrálního uzlu (C) je připojen k polarizačnímu děliči (7) svazku periferního zařízení (A) a druhý optický spínač (6b) centrálního uzlu (C) je připojen k polarizačnímu děliči (7) svazku periferního zařízení (B), přičemž polarizační dělič (7) svazku každého periferního zařízení (A, B) je dále připojen k symetrickému děliči (8) svazku přímo a přes třetí fázový modulátor (1c), přičemž symetrický dělič (8) svazku je dále připojen k zdroji (10) záření, prvnímu detektoru (11a) a druhému detektoru (11b), přičemž třetí fázový modulátor (1c) je připojen ke generátoru (13) náhodných čísel periferního zařízení (A, B).

6. Zapojení podle nároku 5, **vyznačující se tím**, že symetrický dělič (8) svazku je připojen k druhému detektoru (11b) přímo a k zdroji (10) záření a prvnímu detektoru (11a) přes optický cirkulátor (9).

7. Způsob dvousměrného kvantového přenosu šifrovacího klíče pomocí zapojení podle kteréhokoliv z nároků 5 až 6 mezi dvěma periferními zařízeními (A, B) přes centrální uzel (C) v síti typu „hvězda“, **vyznačující se tím**, že obsahuje následující kroky:
a. vytvoření spojení mezi dvěma periferními zařízeními (A, B) a centrálním uzlem (C) přes kvantový kanál sepnutím optických spínačů (6a, 6b) na základě požadavku periferních zařízení (A, B) centrálnímu uzlu (C) přes klasický informační kanál;
b. volitelná modulace impulzu mezi oběma periferními zařízeními (A, B) a centrálním uzlem (C) pomocí optických spínačů (6a, 6b) a/nebo polarizačních kontrolérů (5a, 5b) a/nebo variabilních optických zeslabovačů (2a, 2b);
c. odeslání impulzu z obou periferních zařízení (A, B) do centrálního uzlu (C) přes nevyvážený Machův-Zehnderův interferometr (12) pro vytvoření prvního, v čase nezpožděného impulzu a druhého, v čase zpožděného impulzu z obou periferních zařízení (A, B);
d. modulace fáze druhého, v čase zpožděného impulzu z obou periferních zařízení (A, B) fázovým modulátorem (1a, 1b), přičemž tato modulace je řízena generátorem (3) náhodných čísel tak, že druhý, v čase zpožděný impulz z obou periferních zařízení (A, B) je modulován stejně;
e. odražení impulzů od Faradayových zrcadel (4a, 4b), čímž se mění polarizace všech impulzů na ortogonální;
f. vrácení impulzů s ortogonální polarizací do obou periferních zařízení (A, B) přes nevyvážený Machův-Zehnderův interferometr (12) a modulace fáze prvního, v čase nezpožděného impulzu z centrálního uzlu (C) třetím fázovým modulátorem (1c), přičemž tato modulace je řízena generátorem (13) náhodných čísel každého periferního zařízení (A, B) zvlášť;
g. interference prvního, v čase nezpožděného impulzu a druhého, v čase zpožděného impulzu za symetrickým děličem (8) svazku a následná detekce výsledku interference obou impulzů v prvním detektoru (11a) nebo v druhém detektoru (11b) každého periferního zařízení (A, B); a
h. porovnání detekčních bází u shodně detekovaných impulzů mezi oběma periferními zařízeními (A, B) přes klasický informační kanál za vzniku bezpečného symetrického šifrovacího klíče v obou periferních zařízeních (A, B).

8. Způsob podle nároku 7, **vyznačující se tím**, že v kroku h. se detekční báze u shodně detekovaných impulzů porovnají mezi oběma periferními zařízeními (A, B) navzájem a šifrovací a detekční báze u shodně detekovaných impulzů se porovnají mezi každým periferním zařízením (A, B) a centrálním uzlem (C).

9. Způsob podle nároku 7, **vyznačující se tím**, že v kroku h. se šifrovací a detekční báze u shodně detekovaných impulzů porovnají mezi každým periferním zařízením (A, B) a centrálním uzlem (C), načež si obě periferní zařízení (A, B) navzájem sdělí, zda pro daný impulz se shodnou šifrovací a detekční bází došlo k detekci impulzu v obou periferních zařízeních (A, B).

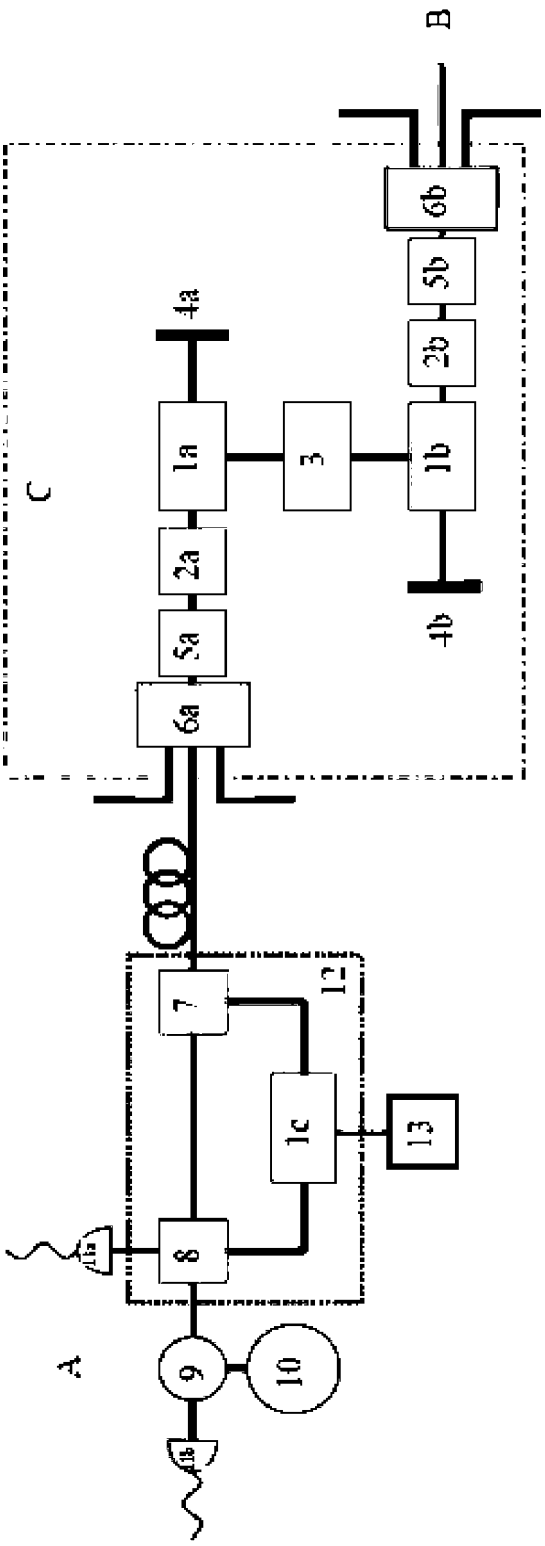
10. Způsob podle kteréhokoliv z nároků 7 až 9, **vyznačující se tím**, že v kroku d. je modulace fáze druhého, v čase zpožděného impulzu z obou periferních zařízení (A, B) fázovým modulátorem (1a, 1b) uskutečněna podle protokolu BB84 s časově-fázovým kódováním, přičemž v kroku f. je modulace fáze prvního, v čase nezpožděného impulzu z centrálního uzlu (C) třetím fázovým modulátorem (1c) uskutečněna podle protokolu BB84 s časově-fázovým kódováním.

2 výkresy

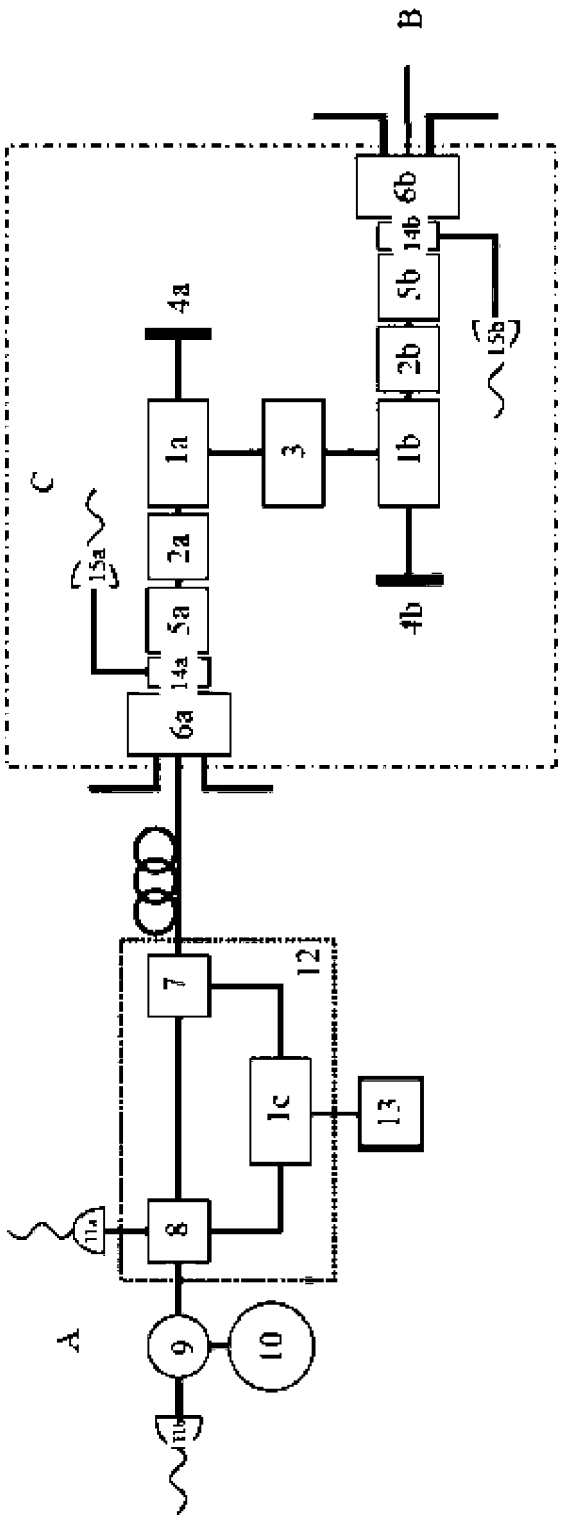
Seznam vztahových značek:

A první periferní zařízení, „Alice“
B druhé periferní zařízení, „Bob“

C centrální uzel, „Charlie“
1a první fázový modulátor
1b druhý fázový modulátor
2a první variabilní optický zeslabovač
2b druhý variabilní optický zeslabovač
3 generátor náhodných čísel centrálního uzlu C
4a první Faradayovo zrcadlo
4b druhé Faradayovo zrcadlo
5a první polarizační kontrolér
5b druhý polarizační kontrolér
6a první optický spínač
6b druhý optický spínač
7 polarizační dělič svazku
8 symetrický dělič svazku
9 optický cirkulátor
10 zdroj záření
11a první detektor
11b druhý detektor
12 nevyvážený Machův-Zehnderův interferometr
13 generátor náhodných čísel periferního zařízení A, B
14a první nesymetrický dělič svazku
14b druhý nesymetrický dělič svazku
15a první pomocný fotodetektor
15b druhý pomocný fotodetektor



Obr. 1


B
6b
14b
5b
15b
2b
4a
1a
3
1b
C
2a
15a
5a
4b
14a
6a
12
7
1c
13
11a
8
A
9
10
11b

Obr. 2