MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA DI INVENZIONE NUMERO	**102022000009479**
Data Deposito	**09/05/2022**
Data Pubblicazione	**09/11/2023**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L	9	08

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	B	10	70

Titolo

Method for generating a cryptographic key using quantum sources of light

Ing. Giancarlo Penza
(Albo iscr. n. 1335 B)

DESCRIZIONE

Annessa a domanda di brevetto per INVENZIONE INDUSTRIALE avente per titolo

"Metodo per generare una chiave crittografica utilizzando sorgenti di luce quantistiche"

A nome: LEVELQUANTUM S.R.L.
Piazzale Luigi Cadorna, 4
20123 MILANO (MI)

****

Campo tecnico dell'invenzione

La presente invenzione si riferisce in generale al settore della crittografia.

Più in particolare, l'invenzione riguarda un metodo per generare una chiave crittografica sicura utilizzando sorgenti di luce quantistiche.

Tecnica nota

La comunicazione quantistica (QC, Quantum Communication) è un ramo dell'elaborazione delle informazioni quantistiche che è dedicato alla creazione di canali crittografati utilizzando chiavi casuali ottenute da stati di fotoni in correlazione quantistica [1]. Si basa su un entanglement quantistico, un fenomeno fisico che consente a parti distanti di ottenere gli stessi bit casuali da stati fotonici che sono loro inviati per esempio mediante una fibra ottica o attraverso lo spazio libero (atmosfera). I bit casuali sono quindi utilizzati per crittografare e decrittografare un canale classico (non quantistico). La sicurezza della QC deriva dal fatto che qualsiasi interazione supplementare con uno stato quantistico, che potrebbe essere causata per esempio da intercettazioni, la altera e rovina le correlazioni quantistiche esistenti. Le correlazioni quantistiche nonché la casualità prodotta sono sottoposte a test con un test di entanglement, che forma un controllo di sicurezza in tempo reale del canale quantistico che è eseguito in parallelo con lo schema di QC. Se questo test fallisce, significa che i simboli generati

non sono casuali o la comunicazione è compromessa e pertanto non può essere affidabile.

Finora i simboli casuali nelle soluzioni di QC sono stati generati dalla polarizzazione o dalla fase dei fotoni, che sono difficili da mantenere e deboli [1]. I protocolli erano basati su coppie di fotoni singoli che sono difficili da ottenere con le apparecchiature attuali e pertanto, la maggior parte delle soluzioni utilizzava stati quantistici debolmente compressi (squeezed) dove i contributi di ordine superiore venivano trascurati. Poiché soltanto una frazione di coppie di fotoni generate era ricevuta dalle parti comunicanti per via per esempio di perdite nell'atmosfera, esse dovevano comunicare in aggiunta con un canale separato e campionare/filtrare gli stati quantistici che erano adatti per produrre bit casuali [4]. Tuttavia, questo campionamento/filtraggio introduceva una falla che poteva essere utilizzata da un pirata informatico (un intercettatore) per falsificare i risultati del test di entanglement [3]. I tassi di chiave ottenuti, specialmente in presenza di perdite atmosferiche importanti, erano molto bassi, rendendo la generazione di una chiave casuale di lunghezza appropriata un processo debole e lungo [4].

Sommario dell'invenzione

La presente invenzione riguarda un metodo per generare una chiave crittografica per la crittografia/decrittografia di dati come definito nella annessa rivendicazione 1 e dalle sue forme di realizzazione preferite descritte nelle rivendicazioni dipendenti da 2 a 7.

La Richiedente ha percepito che il metodo secondo la presente invenzione presenta i vantaggi seguenti:

- consente di costruire sistemi di comunicazione quantistica più sicuri ed efficaci, pur utilizzando soltanto componenti prontamente disponibili;
- ottiene un tasso più elevato di generazione di chiavi.

Un ulteriore oggetto della presente invenzione è un supporto di memorizzazione leggibile da un elaboratore elettronico come definito nella annessa rivendicazione 8.

Un ulteriore oggetto della presente invenzione è un sistema optoelettronico quantistico come definito nella unita rivendicazione 9 e dalla sua forma di realizzazione preferita descritta nella rivendicazione dipendente 10.

Breve descrizione dei disegni

Ulteriori caratteristiche e vantaggi dell'invenzione risulteranno dalla descrizione seguente di una forma di realizzazione preferita e da sue varianti, detta descrizione essendo fornita a titolo esemplificativo con riferimento agli disegni allegati, in cui:

- la Figura 1 mostra schematicamente un sistema opto-elettronico quantistico per implementare un protocollo di distribuzione di entanglement a lungo raggio secondo l'invenzione;
- la Figura 2 mostra schematicamente il sistema opto-elettronico quantistico per implementare uno schema di distribuzione di chiave quantistica e il test di entanglement utilizzando il protocollo di distribuzione di entanglement a lungo raggio della Figura 1.

Descrizione dettagliata dell'invenzione

Si noti che nella descrizione che segue, blocchi, componenti o moduli identici o simili presentano numeri di riferimento identici, a prescindere dal fatto che essi siano mostrati in forme di realizzazione differenti dell'invenzione.

L'invenzione riguarda un metodo di comunicazione a sicurezza elevata che si basa su proprietà quantistiche di sorgenti di luce multifotoniche. Ciò consente a due parti 10, 20 di ottenere una chiave condivisa composta da simboli casuali, la sicurezza della chiave essendo garantita dalle leggi della fisica. La chiave può quindi essere utilizzata per una crittografia e una decrittografia sicura di una comunicazione successiva [1].

Le parti 10, 20 sono implementate con dispositivi opto-elettronici quantistici.

L'invenzione comprende tre componenti (vale a dire, fasi), il che la rende uno stack tecnologico completo:

1) un metodo per stabilire un canale quantistico tra parti distanti;

2) un controllo di sicurezza in tempo reale del canale quantistico; e

3) un metodo per utilizzare il canale quantistico per generare una chiave segreta condivisa dalle due parti che può essere utilizzata per la comunicazione crittografata.

Lo schema utilizza un apparato quantistico che contiene soltanto elementi quantistici fotonici prontamente disponibili.

Il primo componente mostrato nella Figura 1 è un protocollo efficace per stabilire un canale quantistico mediante un collegamento ottico in un modo resistente contro perdite elevate per esempio nell'atmosfera, rendendolo particolarmente adatto per le comunicazioni quantistiche (QC) basate su satellite [2]. Il canale quantistico assume la forma di stati quantistici multifotonici altamente intrecciati (entangled) che sono condivisi tra due parti distanti.

Un controllo di sicurezza in tempo reale del canale quantistico forma il secondo componente, questo test controlla alla fine che gli stati quantistici della luce portino sufficienti correlazioni quantistiche e forniscano simboli veramente casuali che possano formare una chiave segreta condivisa. Un risultato positivo di questo test indica una sicurezza completa di una comunicazione successiva contro qualsiasi possibile intercettatore, anche se l'hardware è stato fornito o alterato da questo intercettatore e pertanto non può essere affidabile (crittografia indipendente dal dispositivo).

La conversione reale di stati quantistici in simboli casuali è realizzata con il protocollo di distribuzione di chiave quantistica (QKD, Quantum Key Distribution) basata sull'entanglement implementato in parallelo al controllo di sicurezza, che forma il terzo componente.

Le caratteristiche del canale quantistico sottostante, nel quale non vi è la necessità di campionare/filtrare stati quantistici, consentono al controllo di sicurezza di essere senza falle e pertanto alla segretezza della chiave di

essere incontestabile [3]. Se gli utenti decidono che possono fidarsi del loro hardware, il controllo di sicurezza non deve essere così rigido, e questa libertà supplementare aumenta il tasso di generazione di chiavi (tasso di chiave). Questa modalità di funzionamento commutabile in funzione delle necessità dell'utente, senza alcuna modifica all'hardware o a caratteristiche essenziali, è una caratteristica importante dello schema.

Lo schema inventato non si basa inoltre su una fase debole degli stati quantistici prodotti e poiché utilizza stati multifotonici, possiede il potenziale di ottenere un tasso più elevato di generazione di chiavi rispetto alle soluzioni esistenti. Tutte queste caratteristiche rendono il nuovo schema particolarmente adatto per le applicazioni satellitari del prossimo futuro.

La configurazione per la distribuzione di un entanglement multifotonico (si veda la Figura 1) richiede due sorgenti 11, 12 di stati Squeezed Vacuum (SV) a due modalità $|\Psi\rangle$ [5], un divisore di fascio 31 e due rivelatori di fotoni 32, 33. Questi rivelatori di fotoni 32, 33 sono idealmente a risoluzione di numero di fotoni (PNR, Photon-Number-Resolving) per esempio sensori di bordo di transizione (TES, Transition-Edge Sensors) [13], ma se i numeri di fotoni totali sono bassi essi possono essere sostituiti con altri schemi di rilevamento della luce come uno o più rivelatori a singolo fotone, fotodiodi a valanga o loro combinazioni. Gli stati squeezed vacuum a due modalità sono prodotti naturalmente per mezzo di conversione discendente parametrica spontanea (SPDC, Spontaneous Parametric Down Conversion) o di una miscelazione a quattro onde in materiali che presentano una non linearità ottica. Esempi includono il cristallo di borato di beta-bario (BBO), il cristallo di niobato di litio ($LiNbO_3$) o il cristallo di potassio-diidrogeno-fosfato (KTP), che possono essere integrati su chip ottici grazie agli ultimi progressi nell'ottica quantistica integrata.

I fasci idler dei due stati SV sono diretti dalle parti 10 e 20 verso un'autorità centrale 30 che li interferisce sul divisore di fascio 31 e misura le uscite con i rivelatori di fotoni 32, 33. Di conseguenza, i fasci segnale degli

stati SV diventano entangled in modo che le parti 10 e 20 condividono uno stato quantistico entangled. L'autorità centrale 30 può essere situata a una grande distanza dalle sorgenti di luce quantistica, le parti 10 e 20, poiché i canali che collegano le sorgenti e la BS sono altamente resistenti alle perdite di trasmissione. Essa può anche essere situata su un satellite per applicazioni di comunicazioni quantistiche Terra-spazio.

Per le procedure di verifica di entanglement e che generano una chiave segreta condivisa, è richiesto un numero di componenti extra: un divisore di fascio variabile 14, 24 per entrambe le parti 10 e 20, una sorgente 11, 21 di luce coerente (laser) e due rivelatori di fotoni aggiuntivi 15, 16, 25, 26 ciascuno, si veda la Figura 2. Nel processo di verifica, ciascun fascio dello stato di uscita interferisce con lo stato coerente sul divisore di fascio variabile e quindi le uscite del divisore di fascio sono misurate dai rivelatori di fotoni 15, 16, 25, 26. Il processo è ripetuto per molte impostazioni di ampiezze/fasi a stato coerente e riflettività del divisore di fascio, alcune delle quali sono utilizzate per stabilire bit di chiave condivisi mentre altre sono utilizzate per effettuare il test di entanglement che garantisce la sicurezza della chiave.

L'autorità centrale 30 è implementata con un dispositivo opto-elettronico quantistico.

Il metodo di produrre un entanglement quantistico multifotonico inizia con due parti distanti 10 e 20, ciascuna producendo uno stato squeezed vacuum a due modalità (due fasci) $|\Psi\rangle$. Questo stato quantistico multifotonico della luce è caratterizzato da due fasci che sono entangled nel numero di fotoni, vale a dire che misurando n i fotoni in un fascio risulterà in n fotoni misurati nel secondo fascio, anche se n di per sé è indeterminato fino alla prima misurazione.

Gli stati squeezed vacuum a due modalità sono prodotti naturalmente proiettando luce laser su materiali con una non linearità ottica, mediante conversione discendente parametrica spontanea (SPDC) [5] o una miscelazione a quattro onde [6]. In questo modo sono generati quattro fasci

di luce, i fasci a_1 e a_2 sono generati alla parte 10, mentre i fasci b_1 e b_2 sono generati alla parte 20. I fasci a_2 e b_2 (i fasci idler) sono inviati a un'autorità centrale 30 che effettua una misurazione di entanglement, interferendo con i due fasci su un divisore di fasci 31 e misurando i fasci di uscita con rivelatori a risoluzione di numero di fotoni (PNR). Di conseguenza le parti 10 e 20 condividono uno stato entangled $\left|\Psi_{\text{out}}^{(k,S)}\right\rangle$ nei fasci rimanenti a_1 e b_1 (i fasci segnale). L'autorità 30 informa quindi le parti 10 e 20 circa i risultati della misurazione k e $S-k$ mediante un canale classico autenticato cosicché esse sanno quale stato è stato generato.

Ciascuna delle parti 10 e 20 utilizza una configurazione aggiuntiva costituita da un divisore di fascio variabile 14, 24, una sorgente a stato coerente 11, 21 (un laser) e rivelatori di fotoni 15, 16, 25, 26. Esse effettuano quindi un test di entanglement secondo la procedura seguente: le parti 10 e 20 utilizzano ciascuna n impostazioni distinte di riflettività di divisore di fascio $r_{\text{a1}}, r_{\text{a2}}, r_{\text{a3}}, \ldots r_{\text{an}}$ e $r_{\text{b1}}, r_{\text{b2}}, r_{\text{b3}}, \ldots r_{\text{bn}}$ rispettivamente, e n impostazioni distinte di ampiezze/fasi a stato coerente, rappresentate congiuntamente dai parametri $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_{\text{n}}$ e $\beta_1, \beta_2, \beta_3, \ldots \beta_{\text{n}}$ per le parti 10 e 20 rispettivamente.

Per ciascuna delle n impostazioni, la parte 10 interferisce con uno stato coerente $|\alpha\rangle$ di ampiezza α con il loro fascio segnale su un divisore di fascio 14 con la riflettività r e misura i due fasci di uscita con rivelatori di fotoni 15, 16. Esse ripetono questo processo per creare statistiche affidabili per ciascuna impostazione e risultato di misurazione, e quindi si comunicano tra loro queste statistiche mediante un canale classico autenticato. Insieme utilizzano queste statistiche per effettuare un test di entanglement che conferma l'entanglement dello stato condiviso.

Questo test potrebbe essere la valutazione di una disuguaglianza di Bell come la disuguaglianza di Clauser-Horne-Shimony-Holt (CHSH) [7], la disuguaglianza di Collins-Gisin-Linden-Massar-Popescu (CGLMP) [8], le

disuguaglianze concatenate [9], o qualsiasi altro test basato su queste misurazioni che confermi l'entanglement quantistico [10].

Preferibilmente, la parte 10 utilizza impostazioni aggiuntive r_{a0} e α_0 scelte in modo che se la parte 10 utilizza queste impostazioni e la parte 20 utilizza r_{b1} e β_1, i risultati di misurazione ottenuti dalle parti 10 e 20 sono altamente correlati. In altri termini, se la parte 10 ottiene un risultato X e la parte 20 ottiene un risultato Y, la parte 20 può ottenere facilmente X mediante una trasformata matematica fissa, per esempio, il capovolgimento di un solo bit, con errori minimi. I risultati per queste impostazioni sono mantenuti segreti, e le serie di risultati X sono una sorgente di simboli che formano la stringa condivisa di bit di chiave.

Preferibilmente, le parti 10 e 20 utilizzano le impostazioni r_{a_0}, α_0 e r_{b_1}, β_1 con probabilità elevata cosicché la maggior parte delle misurazioni generano bit di chiave, lasciando altre misurazioni appena sufficienti per eseguire in modo affidabile il test di entanglement al fine di massimizzare il tasso di chiavi, garantendo al contempo la segretezza della chiave.

Preferibilmente, l'autorità centrale 30 che effettua la misurazione di entanglement è situata su un satellite, una nave, un drone o un qualsiasi altro oggetto volante.

Preferibilmente, l'autorità centrale 30 che effettua la misurazione di entanglement è collegata alle parti 10 e 20 mediante fibre ottiche, una connessione a spazio libero o una loro combinazione.

L'invenzione verrà ora descritta dettagliatamente con riferimento all'illustrazione le cui figure sono presenti,

La Figura 1 mostra lo schema di un sistema opto-elettronico quantistico 50 che implementa il protocollo di distribuzione di entanglement a lungo raggio. Le parti 10 e 20 producono localmente due copie dello stato squeezed vacuum a due modalità $|\Psi\rangle$, per esempio utilizzando la SPDC o la miscelazione a quattro onde. Un fascio da ciascuno stato, i fasci idler a_2 e b_2, sono inviati all'autorità centrale 30, che effettua una misurazione di entanglement utilizzando un divisore di fascio 31 e rivelatori di fotoni PNR

32, 33 che rilevano il numero di fotoni che passano attraverso il divisore di fascio 31. Questi risultati di misurazione, k e $S-k$, vengono annunciati. Di conseguenza, le parti 10 e 20 condividono nei loro fasci segnale a_1 e b_1 uno stato entangled multifotonico $\left|\Psi_{\text{out}}^{(S,k)}\right\rangle$ parametrizzato mediante S e k.

La Figura 2 mostra lo schema del sistema opto-elettronico quantistico 50 che implementa lo schema di distribuzione di chiave quantistica (QKD) e il test di entanglement utilizzando il protocollo di distribuzione di entanglement a lungo raggio. Le parti 10 e 20 effettuano la distribuzione di entanglement a lungo raggio utilizzando due sorgenti squeezed vacuum e un'autorità centrale 30 secondo la Figura 1. Inoltre, le parti 10 e 20 mantengono configurazioni costituite da sorgenti a stato coerente (laser) 11, 21, $|\alpha\rangle$ e $|\beta\rangle$ rispettivamente, divisori di fascio variabile 14, 24 con riflettività, r_a e r_b rispettivamente, e rivelatori di fotoni 15, 16, 25, 26. Eseguendo una procedura, nella quale sono effettuate misurazioni per impostazioni di divisore di fascio differenti r_{a0}, r_{a1}, r_{a2}, r_{a3}, ... r_{an} e r_{b1}, r_{b2}, r_{b3}, ... r_{bn}, e ampiezze a stato coerente differenti α_0, α_1, α_2, α_3, ... α_{n} e β_1, β_2, β_3, ... β_{n}, le parti 10 e 20 possono realizzare una procedura di verifica di entanglement utilizzando un test di entanglement e uno schema di distribuzione di chiave quantistica (QKD).

Componente 1 - Metodo per stabilire un canale quantistico

L'entanglement multifotonico è creato naturalmente proiettando luce laser su materiali con una non linearità ottica, mediante o la conversione discendente parametrica spontanea (SPDC) [5] o la miscelazione a quattro onde [6], entrambe le quali producono in maniera deterministica uno stato squeezed vacuum (SV) a due modalità.

Lo stato SV $|\Psi\rangle$ è entangled, vale a dire che esso presenta correlazioni quantistiche perfette che sono manifestate da numeri di fotoni uguali in due fasci di luce chiamati segnale e idler che possono essere separati spazialmente. Nel protocollo proposto, raffigurato nella Figura 1, sono necessarie due copie separate dello stato $|\Psi\rangle$ come input. I fasci idler

provenienti dalle due sorgenti, a_2 dalla sorgente in corrispondenza della parte 10 e b_2 dalla sorgente in corrispondenza della parte 20, interferiscono su un divisore di fascio 31 situato su un'autorità centrale remota 30, dove sono successivamente rilevati da rivelatori a risoluzione di numero di fotoni (PNR).

Se non vi sono perdite di fotoni tra le sorgenti in corrispondenza delle parti 10, 20 e l'autorità centrale remota 30, il rilevamento di S fotoni in totale in corrispondenza dell'autorità centrale 30 significa che S fotoni distribuiti tra due fasci idler a_2 e b_2 sono entrati nel divisore di fascio 31 e che devono esserci S fotoni in totale nei fasci segnale a_1 e b_1.

Il rilevamento in corrispondenza dell'autorità centrale 30 è denominato misurazione di entanglement perché, di conseguenza, i fasci segnale a_1 e b_1 diventano entangled, formando uno stato quantistico condiviso $\left|\Psi_{\text{out}}^{(k,S)}\right\rangle$. La quantità dell'entanglement finale condiviso tra le parti è parametrizzata univocamente dai risultati di misurazione k e $S-k$ e può essere quantificato, per esempio mediante entropia di entanglement o negatività logaritmica [11]. La quantità di entanglement è vicino al massimo, anche con perdite importanti nei fasci idler. Questa caratteristica è molto importante dal punto di vista della QC a spazio libero (per esempio, basata su un satellite), quando lo stato quantistico entangled prodotto conserva ancora una quantità elevata di entanglement nonostante l'attenuazione significativa nell'atmosfera.

Se i numeri totali di fotoni sono bassi al punto che una probabilità di misurare $S>1$ è minima, i rivelatori PNR in corrispondenza di C possono essere sostituiti con altri metodi di rilevamento di luce come uno o più rivelatori a singolo fotone, fotodiodi a valanga o loro combinazioni.

Componente 2– Controllo di sicurezza in tempo reale del canale quantistico

L'entanglement può essere definito come una casualità condivisa tra più parti, che produce correlazioni tra misurazioni effettuate da queste parti

che non possono essere spiegate con la fisica o la statistica classica (non quantistica). Queste correlazioni quantistiche possono essere distinte dalle correlazioni classiche mediante la violazione di certe disuguaglianze matematiche derivate dalle statistiche classiche come le disuguaglianze di Bell/steering [10]. Gli stati quantistici di luce generata nella componente 1 possono pertanto essere certificati per mezzo di un test di entanglement che controlla la violazione di una di queste disuguaglianze. Questo test garantisce che le due parti di terra 10 e 20 condividano stati entangled quantistici che possono essere impiegati nella distribuzione di chiavi crittografiche o in altri compiti di informazioni quantistiche. Oltre allo stato entangled condiviso, le parti 10 e 20 includono entrambe un rispettivo divisore di fascio ottico 14, 24 con riflettività variabile, e una rispettiva sorgente 11, 12 di luce coerente, vale a dire un laser. Questo schema è raffigurato nella Figura 2.

Entrambe le parti 10, 20 interferiscono con la metà del loro stato condiviso con una luce coerente su un rispettivo divisore di fascio 14, 24, e misurano quindi il numero di fotoni trasmessi utilizzando rivelatori di fotoni 15, 16, 25, 26. Le riflettività di divisore di fascio e le ampiezze a stato coerente sono scelte casualmente immediatamente prima dell'interferenza tra molti valori possibili. Le parti 10 e 20 utilizzano ciascuna n impostazioni distinte di riflettività di divisore di fascio $r_{\mathrm{a1}}, r_{\mathrm{a2}}, r_{\mathrm{a3}}, \ldots r_{\mathrm{an}}$ e $r_{\mathrm{b1}}, r_{\mathrm{b2}}, r_{\mathrm{b3}}, \ldots r_{\mathrm{bn}}$ rispettivamente, e n impostazioni distinte di ampiezze a stato coerente $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_{\mathrm{n}}$ e $\beta_1, \beta_2, \beta_3, \ldots \beta_{\mathrm{n}}$ rispettivamente. Le impostazioni ottimali dipendono da quale stato $\left|\Psi_{\mathrm{out}}^{(k,S)}\right\rangle$ hanno generato e stanno cercando di certificare.

Questo processo è ripetuto molte volte fino a quando le parti 10 e 20 non hanno un insieme statisticamente significativo di risultati per ciascuna combinazione di ampiezze/fasi a stato coerente e riflettività. Le parti 10 e 20 possono quindi comunicare pubblicamente queste statistiche su un canale classico autenticato, e mostrare che una disuguaglianza di

Bell/steering è stata violata, provando che le statistiche di misurazione potrebbero essersi prodotte soltanto per via dell'entanglement del loro stato condiviso.

Come esempio specifico, le parti 10 e 20 possono scegliere di utilizzare $n = 2$ impostazioni distinte ciascuna. La parte 10 utilizza r_{a1}, α_1 e r_{a2}, α_2, mentre la parte 20 utilizza r_{b1}, β_1 e r_{b2}, β_2. La parte 10 può assegnare un risultato $X = +1$ a eventi dove non è trasmesso alcun fotone mediante il loro divisore di fascio locale 14, e $X = -1$ altrimenti, mentre la parte 20 analogamente può assegnare $Y = +1$ o $Y = -1$. Comunicando i loro risultati e la scelta di ampiezze a stato coerente e impostazioni di riflettività, queste calcolano il valore medio di $(X \times Y)$ per ciascuna combinazione di impostazioni. Da queste medie, queste mostrano che la disuguaglianza di Clauser-Horne-Shimony-Holt (CHSH) [7] è violata e pertanto provano l'entanglement dello stato condiviso.

La scelta ottimale delle quattro impostazioni di riflettività, vale a dire quelle che massimizzano $|B|$, dipende dallo stato generato, vale a dire i valori di k e S. Per lo stato più comune $k = 0$, $S = 1$, il test ha esito positivo a condizione che l'efficacia del rivelatore in corrispondenza delle parti 10 e 20 sia superiore all'85%, anche con perdite di trasmissione molto elevate dalla parte 10 all'autorità centrale 30 e dalla parte 20 all'autorità centrale 30. Per alcuni altri stati è meglio assegnare $a = +1$ o -1 ($b = +1$ o -1) a eventi in cui il numero di fotoni trasmessi è pari o dispari, piuttosto che zero o diverso da zero, ma per il resto il test è invariato.

L'esempio suddetto chiude la falla di rilevamento proibitiva [10] per le disuguaglianze di Bell, fornendo una prova incondizionata di entanglement a scapito del requisito di efficacia di rilevatore elevata. Se le parti 10 e 20 confidano nel fatto che il loro apparecchio di misurazione non è stato alterato da una terza parte, possono allentare il requisito di elevata efficacia passando a una modalità di funzionamento secondaria. In questa modalità di funzionamento secondaria, alcuni risultati di misurazione vengono filtrati. Per esempio, la parte 10 può assegnare un risultato a = +

1 a eventi in cui un fotone è trasmesso dal loro divisore di fascio locale 14, e a= -1 a eventi in cui un fotone è riflesso, mentre altri risultati vengono filtrati. La disuguaglianza di Bell può quindi essere valutata come prima, ma con un requisito di efficacia molto inferiore del 22%. Questo test di Bell filtrato fornisce la prova di entanglement nell'ipotesi aggiuntiva che l'apparecchio di misurazione delle parti 10 e 20 sia affidabile. Questa modalità di funzionamento commutabile in funzione delle necessità dell'utente, senza alcuna modifica all'hardware o a caratteristiche essenziali, è una caratteristica importante dello schema.

Il test può essere ulteriormente migliorato dalle parti 10 e 20 impiegando $n > 2$ impostazioni di misurazione per valutare disuguaglianze di Bell concatenate [9], assegnando risultati aggiuntivi per valutare disuguaglianze di tipo Collins-Gisin-Linden-Massar-Popescu (CGLMP) [8], oppure tramite altri mezzi di test di entanglement come il gioco di Bell o la programmazione semidefinita/lineare [10].

Componente 3 - Generazione di una chiave segreta condivisa mediante il canale quantistico

Il test di entanglement conferma la sicurezza del canale quantistico, consentendo alle parti 10 e 20 di stabilire successivamente una chiave segreta condivisa per la crittografia di chiave privata, vale a dire eseguire la QKD. Questo protocollo è garantito dalle leggi della fisica relativamente alla sicurezza contro gli attacchi da parte di un potenziale intercettatore. Per esempio, la parte 20 potrebbe rappresentare una banca, mentre la parte 10 rappresenta un cliente, e l'intercettatore un'entità malintenzionata che cerca di ottenere informazioni riservate.

Il protocollo inizia con la distribuzione di stati entangled alle parti 10 e 20 secondo l'invenzione - le parti 10 e 20 generano ciascuna uno squeezed vacuum a due modalità e inviano una metà a un'autorità centrale 30 che effettua una misurazione di entanglement e comunica il risultato alle parti 10 e 20 attraverso un canale classico.

Una volta stabilito l'entanglement quantistico, le parti 10 e 20 effettuano una misurazione come descritto nel test di entanglement summenzionato - interferendo con gli stati coerenti locali su divisori di fascio variabile 14, 24 e misurando i fotoni trasmessi e/o riflessi. Tuttavia, oltre alle n impostazioni per entrambe le parti, una parte per esempio 10, utilizza un'impostazione aggiuntiva r_{a_0}, α_0. Molte misurazioni sono effettuate con la parte 10 che sceglie casualmente dalle loro $n+1$ impostazioni, e la parte 20 che sceglie casualmente dalle loro n impostazioni.

Le n impostazioni di riflettività per ciascuna parte r_{a1}, r_{a2}, r_{a3}, ... r_{an} e r_{b1}, r_{b2}, r_{b3}, ... r_{bn}, e n ampiezze/fasi a stato coerente α_1, α_2, α_3, ... α_{n} e β_1, β_2, β_3, ... β_{n}, sono scelte per massimizzare la disuguaglianze di Bell come in precedenza. L'impostazione aggiuntiva r_{a_0}, α_0 è scelta in modo tale che quando la parte 10 utilizza questa impostazione e la parte 20 utilizza r_{b_1}, β_1 i risultati di misurazione ottenuti dalle parti 10 e 20 sono altamente correlati. In altri termini, se la parte 10 ottiene un risultato X e la parte 20 ottiene un risultato Y, la parte 20 può ottenere facilmente X mediante una trasformata matematica fissa. Per esempio, nel test CHSH descritto in precedenza, se la parte 10 misura zero fotoni e assegna $X = +1$, la parte 20 misura un numero diverso da zero e assegna $Y = -1$, e viceversa. La parte 20 può quindi capovolgere i risultati di queste cosicché le parti 10 e 20 ottengono una serie condivisa di simboli che formano la chiave segreta. Le misurazioni per altre combinazioni di impostazioni, sono utilizzate per effettuare un test di entanglement come descritto nella Componente 2. Per massimizzare il tasso di generazione di chiavi, le parti 10 e 20 dovrebbero utilizzare le impostazioni r_{a_0}, α_0 e r_{b_1}, β_1 con probabilità elevata cosicché la maggior parte delle misurazioni generano bit di chiave, lasciando altre misurazioni appena sufficienti per eseguire in modo affidabile il test di entanglement.

Una volta che le parti 10 e 20 si sono assicurate che la disuguaglianza di Bell è stata violata e che i loro simboli sono stati generati

da uno stato quantistico entangled, le leggi della fisica garantiscono che l'intercettatore, intercettando gli stati quantistici, potrà ottenere soltanto informazioni limitate riguardanti i risultati di misurazione e i bit di chiave privata. In questo schema indipendente dal dispositivo, questa riservatezza è mantenuta anche se l'intercettatore si è infiltrato nell'autorità centrale remota 30, o ha fabbricato i rivelatori in corrispondenza delle parti 10 e 20.

Se i rivelatori locali in corrispondenza delle parti 10 e 20 sono affidabili, le parti possono commutare lo schema QKD in una modalità di funzionamento secondaria impiegando il test di Bell filtrato come descritto nel Componente 2. L'affidabilità aggiuntiva assegnata ai rivelatori consente di eliminare la necessità di rivelatori ad alta efficacia, aumentando il tasso di generazione di chiavi.

In uno scenario reale vi può essere una piccola quantità di errori tra i bit di chiave delle parti 10 e 20, quindi esse devono effettuare una riconciliazione di informazioni classica (correzione degli errori) mediante un canale classico autenticato utilizzando algoritmi ben noti come i codici di controllo di parità a bassa densità (LDPC, Low Density Parity Check) [12]. Questo processo rivela informazioni parziali a un intercettatore, cosicché come fase finale le parti 10 e 20 effettuano un'amplificazione di riservatezza utilizzando funzioni hash universali. Queste condividono ora una chiave privata completamente casuale di cui l'intercettatore non è a conoscenza, quindi possono crittografare e decrittografare in modo sicuro un messaggio utilizzando una password utilizzabile una sola volta (OTP, One-Time Pad) o altri algoritmi a chiave simmetrica.

Applicazioni possibili

- Comunicazioni quantistiche terra-spazio - Il protocollo può essere utilizzato come mezzo per distribuire un entanglement multifotonico e produrre una chiave segreta condivisa tra due luoghi distanti sulla Terra con un satellite su un'orbita terrestre bassa (LEO, Low Earth Orbit).
- Comunicazione quantistica terra e spazio a spazio libero - Lo schema può essere utilizzato per la distribuzione di un entanglement multifotonico e

produrre una chiave segreta condivisa tra luoghi sulla Terra (edifici, veicoli, navi, o aerei) o nello spazio (per esempio satelliti, navicelle spaziali o stazioni).

- Comunicazione quantistica basata su fibre - Il protocollo può essere utilizzato per la distribuzione di un entanglement multifotonico e per produrre una chiave segreta condivisa tra luoghi connessi con una fibra ottica.
- Stima di fase ottica quantistica migliorata - Il protocollo di distribuzione di entanglement (Componente 1) può essere utilizzato per generare stati che si avvicinano alla prestazione di una sonda ottimale nel rilevamento di cambiamenti molto piccoli in un percorso di un fascio di luce in condizioni rumorose.

Riferimenti:

I numeri in parentesi quadre si riferiscono alle pubblicazioni seguenti:

[1] N. Gisin, R. Thew, *Quantum communication*, Nat. Photonics **1**, 165 (2007).

[2] J.-P. Bourgoin et al. *A comprehensive design and performance analysis of low Earth orbit satellite quantum communication*, New J. Phys. **15**, 023006 (2013).

[3] M. Stobińska, P. Sekatski, A. Buraczewski, N. Gisin, G. Leuchs, *Bell-inequality tests with macroscopic entangled states of light*, Phys. Rev. A **84**, 034104 (2011).

[4] J. Yin et al. *Satellite-based entanglement distribution over 1200 kilometers*, Science **356,** 1140 (2017).

[5] J.-W. Pan et al. *Multiphoton entanglement and interferometry*, Rev. Mod. Phys. **84**, 777 (2012).

[6] A. Dutt et al. *On-chip optical squeezing*, Phys. Rev. Applied **3**, 044005 (2015).

[7] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23**, 880 (1969).

[8] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu, *Bell Inequalities for Arbitrarily High-Dimensional Systems*, Phys. Rev. Letts. **88**, 040404 (2002).

[9] S. L. Braunstein, C. M. Caves, *Wringing out better Bell inequalities*, Ann. Phys. **202**, 22 (1990).

[10] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, *Bell nonlocality*, Rev. Mod. Phys. **86**, 419 (2014).

[11] M. B. Plenio, *Logarithmic negativity: a full entanglement monotone that is not convex*, Phys. Rev. Lett. **95**, 090503 (2005).

[12] R. G. Gallager, *Low density parity check codes*, IRE Trans. Inf. Theory **8**, 21 (1962).

[13] A. E. Lita, A. J. Miller, S. W. Nam, *Counting near-infrared single-photons with 95% efficiency*, Opt. Express **16**, 3032 (2008).

IL MANDATARIO
Ing. Giancarlo Penza
(Albo iscr. n. 1335 B)

Ing. Giancarlo Penza
(Albo iscr. n. 1335 B)

RIVENDICAZIONI

1. Metodo per generare una chiave crittografica per la crittografia/decrittografia di dati, comprendente i passi di:

a) produrre, ad un primo dispositivo opto-elettronico quantistico (10) per mezzo di una prima sorgente ottica (11), un primo stato di luce entangled a due modalità e produrre, ad un secondo dispositivo opto-elettronico quantistico (20) per mezzo di una seconda sorgente ottica (21), un secondo stato di luce entangled a due modalità, in cui il primo stato di luce entangled a due modalità include un primo fascio segnale (a_1) ed un primo fascio idler (a_2) e in cui il secondo stato di luce entangled a due modalità include un secondo fascio segnale (b_1) ed un secondo fascio idler (b_2);

b) inviare il primo fascio idler (a_2) ed il secondo fascio idler (*b2*) ad un'autorità centrale remota (30);

c) all'autorità centrale (30), interferire il primo fascio idler (a_2) con il secondo fascio idler (b_2) su un divisore di fascio (31) e misurare da questo un primo numero di fotoni (*k*) e un secondo numero di fotoni (*S-k*) che passa attraverso il divisore di fascio (31);

d) trasmettere il primo numero di fotoni (*k*) e il secondo numero di fotoni (*S-k*) dall'autorità centrale (30) al primo dispositivo opto-elettronico quantistico (10) e al secondo dispositivo optoelettronico quantistico (20), in modo che il primo fascio segnale (a_1) e il secondo fascio segnale (b_1) condividono uno stato entangled di luce parametrizzato dal primo numero di fotoni (*k*) e da un secondo numero di fotoni (*S-k*);

e) al primo dispositivo optoelettronico quantistico (10), interferire su un primo divisore di fascio variabile (14) lo stato condiviso del primo fascio segnale (a_1) con un primo stato coerente di detta prima sorgente ottica e misurare da questo un primo numero di fotoni trasmessi e/o riflessi;

f) al secondo dispositivo optoelettronico quantistico (20), interferire su un secondo divisore di fascio variabile (24) lo stato condiviso del secondo fascio segnale (b_1) con un secondo stato coerente di detta seconda sorgente ottica e misurare da questo un secondo numero di fotoni trasmessi

e/o riflessi;

g) ripetere il passo e) per una pluralità di differenti riflettività del primo divisore di fascio e/o una pluralità di ampiezze/fasi differenti del primo stato coerente, generando da questo una prima pluralità di misurazioni;

h) ripetere il passo f) per una pluralità di differenti riflettività del secondo divisore di fascio e/o una pluralità di ampiezze/fasi differenti del secondo stato coerente, generando da questo una seconda pluralità di misurazioni;

i) generare, al primo dispositivo opto-elettronico quantistico, una chiave crittografica in funzione di una prima porzione della prima pluralità di misurazioni e generare, al secondo dispositivo opto-elettronico quantistico, una chiave crittografica in funzione di una prima porzione della seconda pluralità di misurazioni;

j) effettuare un test di entanglement della chiave crittografica in funzione di una seconda porzione della prima pluralità di misurazioni e di una seconda porzione della seconda pluralità di misurazioni, in cui la seconda porzione della prima pluralità di misurazioni è differente dalla prima porzione della prima pluralità di misurazioni e in cui la seconda porzione della seconda pluralità di misurazioni è differente dalla prima porzione della seconda pluralità di misurazioni.

2. Metodo secondo la rivendicazione 1, in cui il passo i) comprende ulteriormente:

i1) correggere un qualunque errore di bit della chiave crittografica generata al primo dispositivo opto-elettronico quantistico e/o correggere un qualunque errore di bit della chiave crittografica generata al secondo dispositivo opto-elettronico quantistico;

i2) eseguire un hashing sulla chiave crittografica corretta del primo dispositivo opto-elettronico quantistico e sulla chiave crittografica corretta del secondo dispositivo opto-elettronico quantistico.

3. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui nei passi h) e i) la pluralità di differenti riflettività e/o la pluralità di differenti ampiezze/fasi sono scelte casualmente e sono differenti.

4. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui il primo stato di luce entangled a due modalità e il secondo stato di luce entangled multi-fotone sono stati di luce squeezed vacuum.

5. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui la misurazione nei passi e) e f) è effettuata prima della misurazione nel passo c).

6. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui nel passo c) la misurazione del primo/secondo numero di fotoni include uno tra un rivelatore a risoluzione di numero di fotoni, uno o più rivelatori a singolo fotone (32, 33), fotodiodi a valanga, o una loro combinazione.

7. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui nei passi e) e f) la misurazione del primo/secondo numero di fotoni trasmessi e/o riflessi include uno tra un rivelatore a risoluzione di numero di fotoni, uno o più rivelatori a singolo fotone (15, 16, 25, 26), fotodiodi a valanga, o una loro combinazione.

8. Supporto di memorizzazione non transitorio leggibile da un elaboratore elettronico comprendente istruzioni che, quando eseguite da almeno un elaboratore elettronico, inducono l'elaboratore elettronico ad eseguire i passi del metodo secondo le rivendicazioni da 1 a 7.

9. Sistema opto-elettronico quantistico per generare una chiave crittografica per la crittografia/decrittografia di dati, il sistema comprendente un primo dispositivo opto-elettronico quantistico (10), un secondo dispositivo opto-elettronico quantistico (20) e un dispositivo opto-elettronico quantistico remoto (30),

il primo dispositivo opto-elettronico quantistico comprendente una prima sorgente ottica (11), un primo divisore di fascio (14), un primo rivelatore di fotoni (15) e/o un secondo rivelatore di fotoni (16),

il secondo dispositivo opto-elettronico quantistico comprendente una seconda sorgente ottica (21), un secondo divisore di fascio (24), un terzo rivelatore di fotoni (25) e/o un quarto rivelatore di fotoni (26),

il dispositivo opto-elettronico quantistico remoto (30) comprendente un

terzo divisore di fascio (31), un quinto rivelatore di fotoni (32) e un sesto rivelatore di fotoni (33),

in cui il primo dispositivo opto-elettronico quantistico è configurato per:

- produrre, per mezzo della prima sorgente ottica (11), un primo stato di luce entangled a due modalità, in cui il primo stato di luce entangled a due modalità comprende un primo fascio segnale (a_1) e un primo fascio idler (a_2);
- inviare il primo fascio idler (a_2) al dispositivo opto-elettronico quantistico remoto (30);
- interferire, sul primo divisore di fascio variabile (14), uno stato condiviso del primo fascio segnale (a_1) con un primo stato coerente della prima sorgente ottica e misurare da questo un primo numero di fotoni trasmessi e/o riflessi;
- ripetere detta interferenza per una pluralità di riflettività differenti del primo divisore di fascio e/o una pluralità di ampiezze/fasi differenti del primo stato coerente e generare da questo una prima pluralità di misurazioni;
- generare una chiave crittografica in funzione di una prima porzione della prima pluralità di misurazioni;
- effettuare un test di entanglement della chiave crittografica in funzione di una seconda porzione della prima pluralità di misurazioni, in cui la seconda porzione della prima pluralità di misurazioni è differente dalla prima porzione della prima pluralità di misurazioni;

in cui il secondo dispositivo opto-elettronico quantistico è configurato per:

- produrre, per mezzo di una seconda sorgente ottica (21), un secondo stato di luce entangled a due modalità, in cui il secondo stato di luce entangled a due modalità comprende un secondo fascio segnale (b_1) ed un secondo fascio idler (b_2);
- inviare il secondo fascio idler (*b2*) al dispositivo opto-elettronico quantistico remoto (30);
- interferire, sul secondo divisore di fascio variabile (24), uno stato condiviso del secondo fascio segnale (b_1) con un secondo stato coerente

della seconda sorgente ottica e misurare da questo un secondo numero di fotoni trasmessi e/o riflessi;

- ripetere detta interferenza per una pluralità di riflettività differenti del secondo divisore di fascio e/o una pluralità di ampiezze/fasi differenti del secondo stato coerente e generare da questo una seconda pluralità di misurazioni;
- generare una chiave crittografica in funzione di una prima porzione della seconda pluralità di misurazioni;
- effettuare il test di entanglement della chiave crittografica in funzione di una seconda porzione della seconda pluralità di misurazioni, in cui la seconda porzione della seconda pluralità di misurazioni è differente dalla prima porzione della seconda pluralità di misurazioni;

ed in cui il dispositivo opto-elettronico remoto (30) è configurato per:

- interferire il primo fascio idler (a_2) con il secondo fascio idler (b_2) sul divisore di fascio (31) e misurare da questo un primo numero di fotoni (*k*) ed un secondo numero di fotoni (*S*-*k*) che passa attraverso il divisore di fascio (31);
- trasmettere il primo numero di fotoni (*k*) ed il secondo numero di fotoni (*S*-*k*) al primo dispositivo opto-elettronico quantistico e al secondo dispositivo opto-elettronico quantistico, in modo che il primo fascio segnale (a_1) e il secondo fascio segnale (b_1) condividono uno stato entangled di luce parametrizzato dal primo numero di fotoni (*k*) e da un secondo numero di fotoni (*S*-*k*).

10. Sistema opto-elettronico quantistico secondo la rivendicazione 9, in cui il primo dispositivo opto-elettronico quantistico è configurato per:

- correggere un qualunque errore di bit della chiave crittografica generata;
- eseguire hashing sulla chiave crittografica corretta;

e in cui il secondo dispositivo optoelettronico quantistico è configurato per:

- correggere un qualunque errore di bit della chiave crittografica generata;

- eseguire hashing sulla chiave crittografica corretta.

IL MANDATARIO
Ing. Giancarlo Penza
(Albo iscr. n. 1335 B)

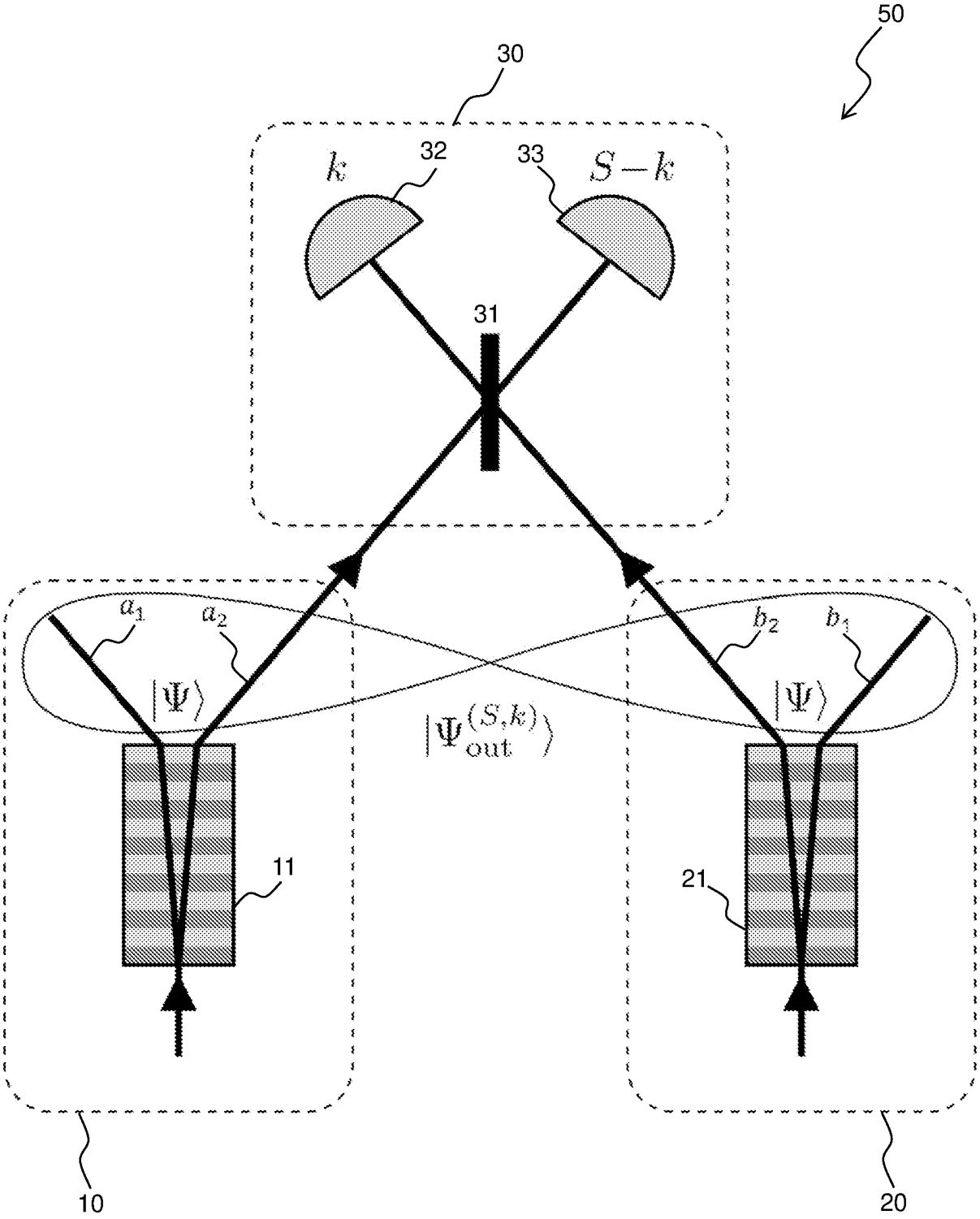
50
30
32
33
k
$S-k$
31
a_1
a_2
b_2
b_1
$|\Psi\rangle$
$|\Psi\rangle$
$|\Psi_{\text{out}}^{(S,k)}\rangle$
11
21
10
20

Fig. 1

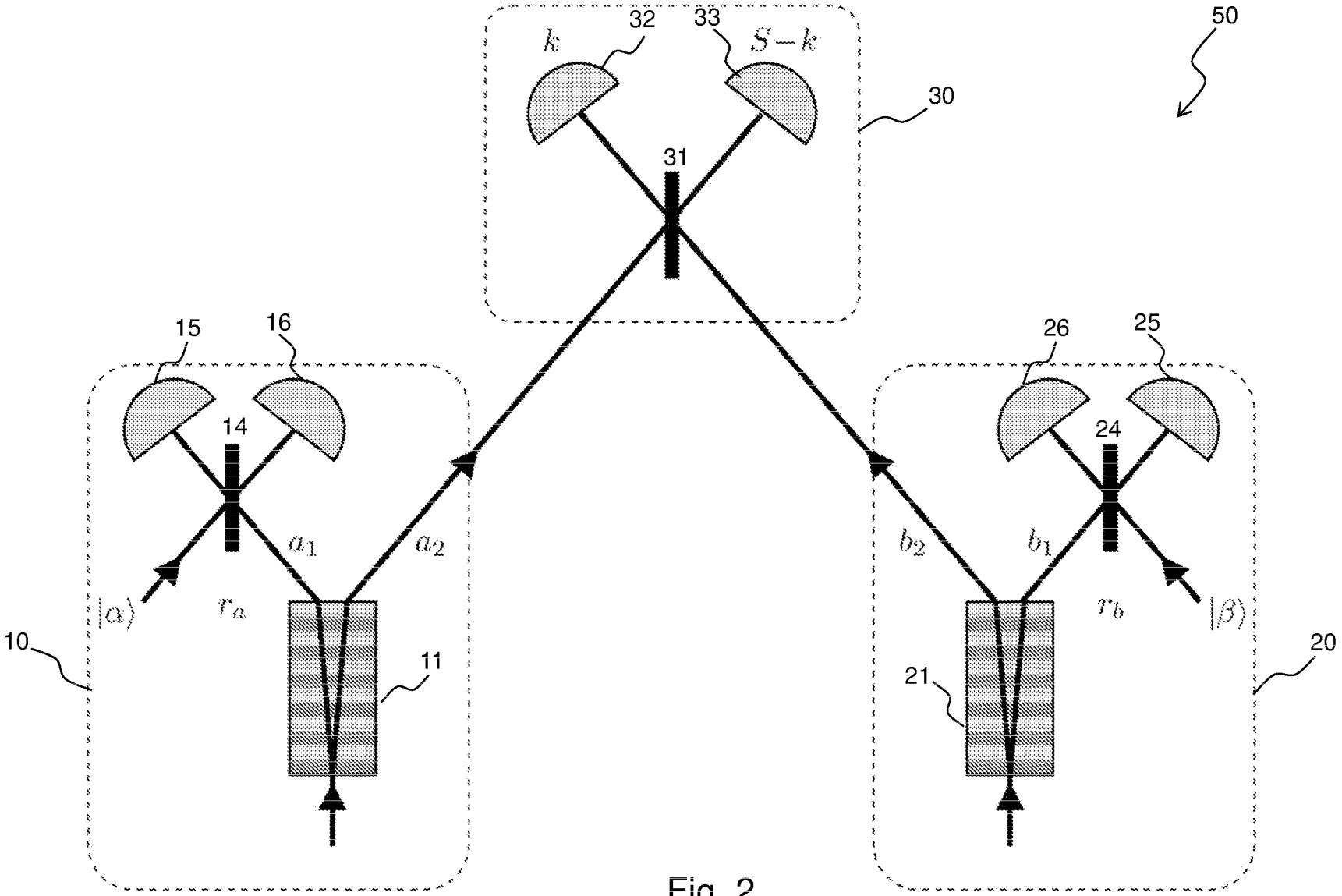
50
30
32
33
k
$S-k$
31
15
16
14
26
25
24
a_1
a_2
b_2
b_1
$|\alpha\rangle$
r_a
r_b
$|\beta\rangle$
10
11
21
20

Fig. 2