CRITTOGRAFIA QUANTISTICA

Overview

Verso la metà degli anni '80 un fisico inglese, David Deutsch, durante una conferenza sulla fisica quantistica, ebbe l'idea di creare un calcolatore quantistico. Questa e' una idea rivoluzionaria, in quanto i calcolatori tradizionali si comportano secondo le leggi della fisica classica, e quindi con le limitazioni che noi tutti conosciamo. Ma un calcolatore quantistico avrebbe una potenza di calcolo teoricamente infinita, tale da poter invertire un algoritmo a fattorizzazione, come l'RSA, pressoché istantaneamente, rendendo quindi assolutamente inutili i sistemi di crittografia algoritmica. La spiegazione del funzionamento di un calcolatore quantistico e' cosa assai complessa, e non e' detto che si possa realizzare in pratica, almeno in tempi brevi, ma anche solo l'ipotesi di una sua futura realizzazione pone dei seri interrogativi sull'utilizzo della crittografia algoritmica, specialmente per quei documenti che devono rimanere riservati per un periodo di tempo abbastanza lungo. Quindi, alla luce di questo fatto, si impone un radicale cambiamento di strategia nella crittografia attuale: non basta più aumentare la lunghezza delle chiavi per rendere sicuro un documento per i prossimi anni (sempre nell'ipotesi di avvento del calcolatore quantistico) ma bisogna ricorrere a qualcosa di completamente nuovo.

Introduzione

Il principale punto debole di ogni comunicazione cifrata, secondo la fisica classica, è che un intercettatore (negli esempi seguenti, "Eva") che abbia accesso al canale può sempre trascrivere il testo cifrato che viene inviato sul canale stesso. Siccome l'operazione di intercettazione può essere passiva, cioè senza emissione di energia da parte di Eva, l'*eavesdropping* è sempre ammissibile secondo la crittografia classica.

La storia della crittologia è caratterizzata dalla continua lotta fra coloro che hanno il compito di proteggere l'informazione operando trasformazioni sul messaggio originale (crittografi) e coloro che invece lavorano per scoprire o modificare il messaggio originale (crittoanalisti). Con l'avvento della crittografia quantistica la disputa tra algoritmo e crittanalisi si risolverà in favore dei crittografi, grazie alla natura intrinseca della tecnologia basata sulla fisica degli stati quantistici, che la rende teoricamente impossibile da violare e persino da intercettare.

Le leggi della fisica quantistica, applicate alla trasmissione sicura, garantiscono invece che anche l'operazione di intercettazione può essere rilevata dalle parti attive sul canale. Questo dà a tutti gli schemi di crittografia quantistica la garanzia di perfetta sicurezza, e la certezza di non-intercettazione rappresenta il salto in avanti fondamentale di queste nuove tecnologie rispetto a diversi millenni di crittografia classica.

Questi sistemi quantistici sfruttano il principio di indeterminazione di Heisenberg secondo il quale la misurazione di un sistema quantistico in genere lo perturba e fornisce un'informazione incompleta sul suo stato precedente alla misurazione.

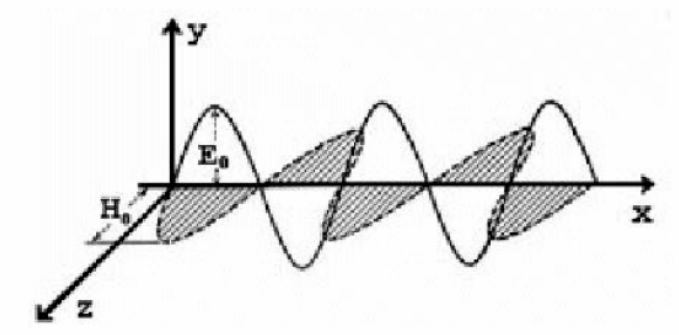
La crittografia quantistica si utilizza convenzionalmente per scambiare fra "Alice" e "Bob" le chiavi private e non il messaggio. Il messaggio verrà crittato successivamente attraverso l'algoritmo One Time Pad. In questo senso si dice che la crittografia quantistica si utilizza nella distribuzione delle chiavi. La Quantum Key Distribution (QKD) permette a due soggetti (negli esempi Alice e Bob) di ottenere chiavi sicure attraverso l'invio di fotoni su un "canale quantistico". Nello schema fondamentale di Crittografia Quantistica, l'informazione associata al singolo fotone risiede nella sua polarizzazione: il fotone viene inviato con una precisa polarizzazione, che corrisponde in uno schema prestabilito ad una cifra binaria (0 e 1).

Le leggi della fisica impediscono ad un terzo soggetto di acquisire informazione sullo stato di un fotone senza disturbarlo, ovvero modificarlo irreparabilmente. Come si vedrà in seguito, è praticamente impossibile intercettare con profitto (ovvero, senza essere scoperti) uno scambio di chiavi su un canale

quantistico senza essere a conoscenza degli schemi di polarizzazione adottati. Inoltre ogni tentativo di intercettazione può essere rilevato da Alice e Bob, con una semplice verifica che rivelerà un apparente incremento di errori di trasmissione.

Canale quantistico e proprietà fisiche dei fotoni

La meccanica quantistica diversamente dalla meccanica classica considera un fascio di luce composto da quantità discrete di energia chiamate fotoni. I fotoni, data la natura ondulatoria della luce, hanno un proprio angolo di polarizzazione, che è definito come l'angolo formato dal piano in cui essi oscillano con l'asse di propagazione degli stessi fotoni. L'angolo di propagazione è un numero θ compreso fra 0° e 180°: non ci sono infatti distinzioni fra un fotone polarizzato a θ ed uno polarizzato a θ +180°.

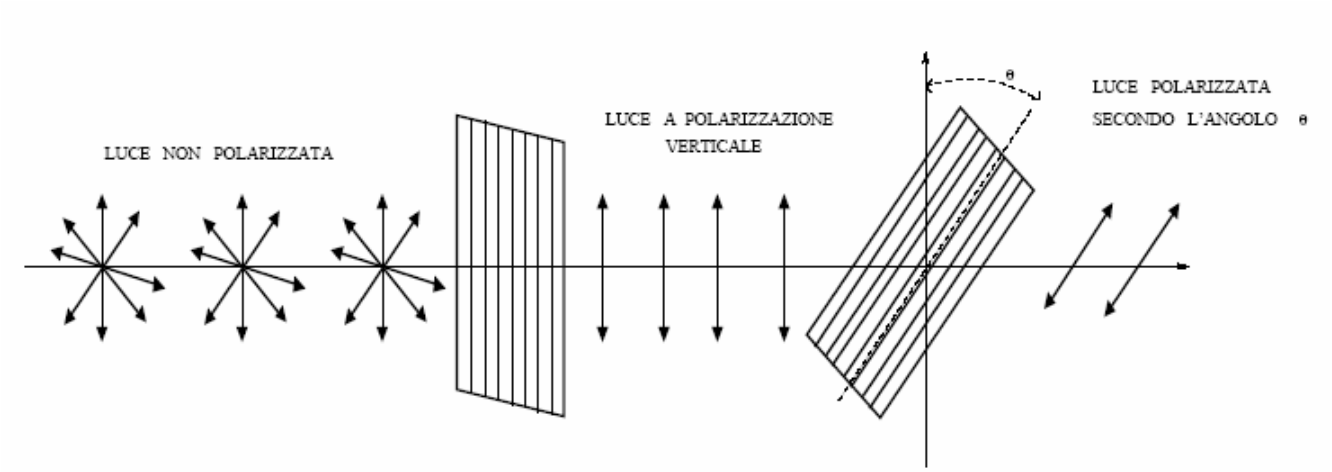


I fotoni provengono da una sorgente di luce con una polarizzazione arbitraria (sono possibili tutte le polarizzazioni). Per far assumere una particolare polarizzazione ad un fotone si utilizza un filtro polarizzatore, che ha la seguente proprietà: le particelle a valle del filtro sono necessariamente polarizzate secondo un determinato angolo. Se questo angolo è θ, allora il filtro si caratterizzerà per essere un θ-filter. Se si fa in modo che un filtro polarizzatore, opportunamente ruotato, permetta il passaggio di fotoni polarizzati con un angolo θ voluto, allora tutti gli altri fotoni che hanno polarizzazioni diverse da θ vengono fermati, oppure oltrepassano il filtro con polarizzazione θ (assumono la polarizzazione θ). Le leggi della meccanica quantistica ci dicono che un fotone a monte del filtro polarizzato con un angolo φ oltrepassa un θ-filter con probabilità:

$$p_\theta(\phi) = \cos^2(\phi - \theta)$$

emergendo ovviamente con polarizzazione θ. La probabilità che lo stesso fotone sia invece "respinto" dal filtro è naturalmente:

$$1 - p_\theta(\phi) = \sin^2(\phi - \theta)$$



Nel seguito utilizzeremo raggi luminosi composti approssimativamente da un solo fotone polarizzato. Un fotone può assumere una qualsiasi polarizzazione ma per i nostri scopi utilizziamo solo fotoni polarizzati a 0°, 45°, 90° e 135° gradi. Il canale quantistico è composto da:

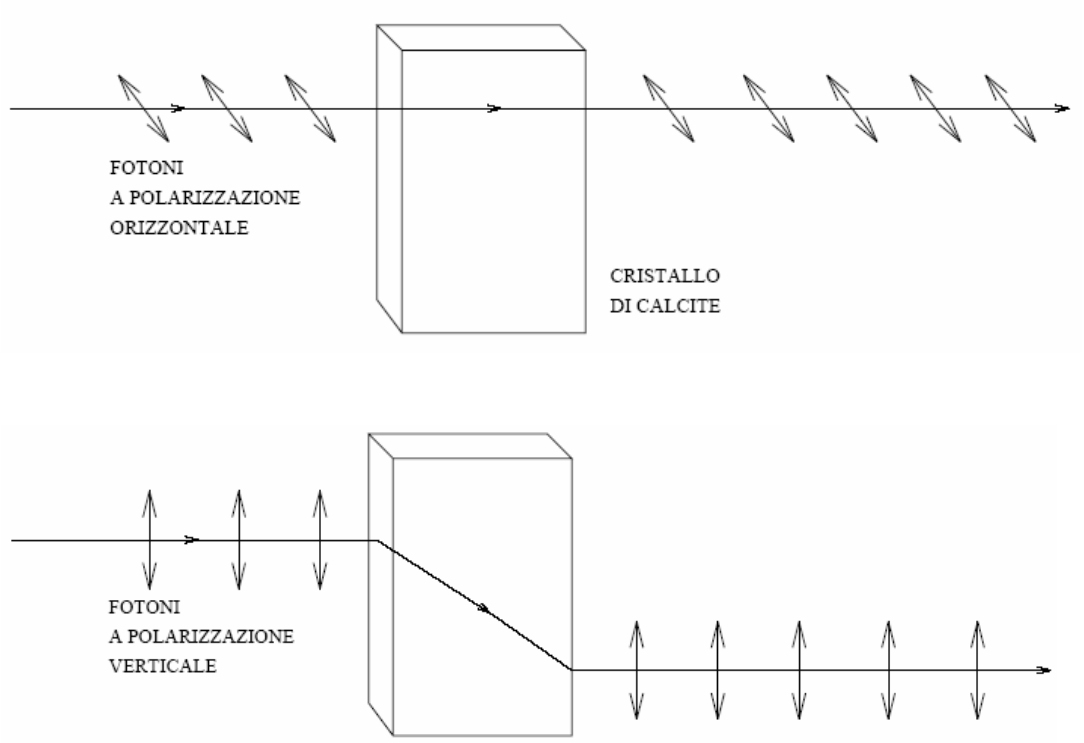
- un dispositivo ottico di emissione capace di produrre fotoni polarizzati in una delle quattro configurazioni possibili (orizzontale, verticale, diagonale a 45 gradi e diagonale a 135 gradi.
- un cavo (es. fibra ottica) su cui viaggiano i fotoni.
- un dispositivo che permetta all'utente destinatario di misurare la polarizzazione dei fotoni.

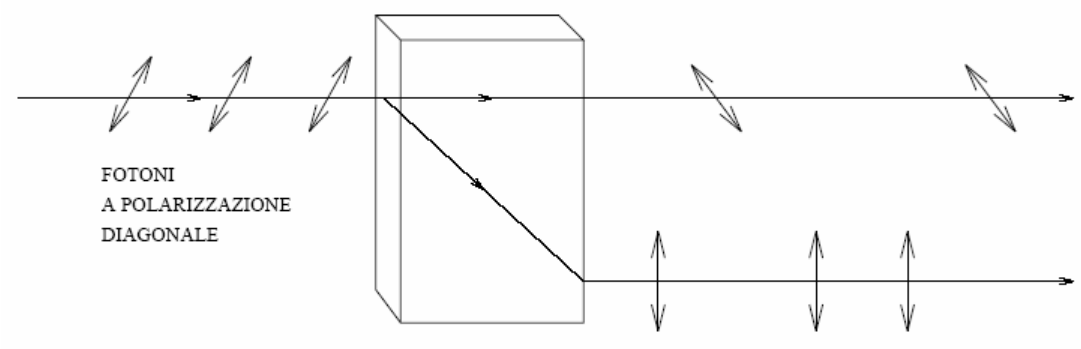
Per misurare la polarizzazione di un fotone è possibile usare un cristallo di calcite che invia i fotoni a seconda della loro polarizzazione lungo una delle due possibili direzioni. Quando un fotone incontra un cristallo di calcite si può comportare in due modi a secondo della sua polarizzazione rispetto al cristallo:

- può attraversarlo in linea retta ed emergerne polarizzato perpendicolarmente rispetto al asse ottico del cristallo.
- può essere traslato ed emergerne polarizzato lungo l'asse stesso.

Se entrando nel cristallo il fotone è già polarizzato in una di queste due direzioni non subisce modifiche di polarizzazione ma viene avviato in modo deterministico lungo il cammino diretto o lungo quello traslato. Se invece nel cristallo entra un fotone polarizzato secondo qualche direzione intermedia esso può seguire a seconda dei casi l'uno o l'altro dei due cammini e quindi venire opportunamente

ripolarizzato perdendo la polarizzazione d'origine. Un comportamento del tutto casuale si ha quando la polarizzazione è intermedia fra queste due direzioni cioè a 45° e 135° gradi: in questo caso la probabilità che il fotone segua l'uno o l'altro cammino è la stessa. In tal modo si perde la memoria della polarizzazione originaria sulla quale il fotone non rivela nulla. Supponiamo che un determinato individuo sia informato in anticipo che un certo fotone è polarizzato secondo una delle due direzioni "rettilinee", verticale o orizzontale, ma che non sappia quale sia la polarizzazione specifica. Può stabilire con sicurezza questa direzione inviando il fotone in un dispositivo consistente in un cristallo di calcite orientato verticalmente e due rilevatori capaci di registrare i fotoni. Questo dispositivo non consente di distinguere fotoni la cui direzione di polarizzazione sia 45° o 135° che però possono essere identificati con sicurezza mediante un identico dispositivo ruotato di 45° gradi rispetto all'orientazione originale. Ovviamente l'apparecchio cosi, ruotato a sua volta non può distinguere i fotoni verticali da quelli orizzontali.





Nella seguente tabella è riportata la probabilità con cui un fotone appartenente ai quattro tipi considerati riesce a superare quattro diversi filtri di polarizzazione.

	0^0-filter	90^0-filter	45^0-filter	135^0-filter
0^0 ↔	1	0	$\frac{1}{2}$	$\frac{1}{2}$
90^0 ↕	0	1	$\frac{1}{2}$	$\frac{1}{2}$
45^0 ↗	$\frac{1}{2}$	$\frac{1}{2}$	1	0
135^0 ↘	$\frac{1}{2}$	$\frac{1}{2}$	0	1

Distribuzione quantistica a chiave pubblica

Lo scopo di una distribuzione quantistica a chiave pubblica è di utilizzare il canale quantistico per fare in modo che due interlocutori, i quali inizialmente non condividono informazioni segrete, possano accordarsi su un insieme di bit casuali. Questo e ottenuto in modo tale the essi, da successive conversazioni su un canale ordinario non quantistico possano dire, con alta probabilità, se la trasmissione quantistica e stata disturbata nel transito da un eventuale origliatore. Se la trasmissione quantistica. non e stata disturbata gli utilizzatori possono sicuramente utilizzare questi bit segreti condivisi come una chiave segreta, per cifrare le comunicazioni successive. D'altra parte, se la trasmissione è stata disturbata, gli utilizzatori scartano i bit ottenuti e provano ancora. Così essi rinviano ogni significativa comunicazione finché riportano un successo. Benché l'origliatore possa intercettare la comunicazione tra gli interlocutori, inserendosi sul canale, egli non può ingannarli facendogli credere che hanno avuto successo quando in effetti non l'hanno avuto.

Il protocollo

Vediamo più in dettaglio come due interlocutori. Alice e Bob. possono effettuare una distribuzione a chiave pubblica su un canale quantistico. Assumiamo la presenza di un origliatore, Eva. Un bit è rappresentato da. un fotone polarizzato come illustrato in Tabella 1.

R	D	Bit
↔	↗	0
↕	↘	1

Facciamo infine l'ipotesi. che ogni impulso contenga esattamente un fotone.
Il protocollo è il seguente:

1. Alice sceglie una stringa casuale di bit ed una sequenza casuale di basi di polarizzazione (rettilinea, o diagonale) e manda a Bob una, sequenza di fotoni, ognuno rappresentante un bit della stringa, nella base scelta.

2. Bob sceglie casualmente per ogni fotone mandatogli da Alice (e indipendentemente dalle scelte fatte da Alice, perché queste scelte non sono note a Bob a questo punto del protocollo) se misurare la polarizzazione rettilinea o diagonale e interpreta ogni risultato come 0 o 1, a

seconda dell'esito della corrispondente misura. Come abbiamo più volte ripetuto, una risposta casuale è prodotta e tutta l'informazione è persa quando si tenta di misurare la polarizzazione rettilinea di un fotone diagonale o viceversa. Così Bob ottiene dati significativi solo dal 50% dei fotoni che ha misurato (quelli per i quali ha indovinato la corretta base di polarizzazione) supponendo che non vi siano state alterazioni dovute ad origliamento.

3. Bob annuncia pubblicamente le basi con cui ha analizzato i fotoni.

4. Alice comunica a Bob. pubblicamente, se per ciascun fotone che egli ha ricevuto ha eseguito il tipo giusto di misurazione. Si scartano tutte le posizioni dei bit per le quali Bob ha eseguito un tipo di misurazione sbagliato o per le quali non è stato rilevato alcun fotone. Ciò può capitare quando un origliatone li ha intercettati e non ne ha rimandato altri, o quando questi ha effettuato una divisione del raggio e ne ha presi per sè alcuni. o perché sono stati persi durante il transito, o, infine, perché non sono stati deviati correttamente verso i fotomoltiplicatori che, di conseguenza. non li hanno rilevati. Infatti osserviamo anche che i fotomoltiplicatori non hanno un'efficienza quantistica del 100%.

5. Alice e Bob, per verificare se le loro risultanti stringhe di bit sono identiche confrontano pubblicamente un sottoinsieme casuale dei bit correttamente ricevuti da Bob, cioè con la base esatta. Se tutti i fotoni (o quasi) concordano, Alice e Bob possono concludere che la trasmissione quantistica. è stata. libera da significativi origliamenti, per cui i rimanenti bit segreti possono costituire la chiave. Se invece vi è stato un notevole origliamento, la trasmissione è scartata e si riprova con un nuovo gruppo di fotoni.

Mostriamo ora un esempio reale di trasmissione quantistica a chiave pubblica fra due ipotetici utenti Alice e Bob i quali inizialmente non condividono nessuna informazione in comune

1a.	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
1b.	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
1c.	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
2a.	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
2b.	1		1		1	0	0	0		1	1	1		0	1
3.	R		D		R	D	D	R		R	D	D		D	R
4a.			OK		OK			OK				OK		OK	OK
4b.			1		1			0				1		0	1
5a.					1									0	
5b.					OK									OK	
5c.			1					0				1			1

Trasmissione quantistica

1a. Bit casuali scelti da Alice

1b. Sequenza di basi scelte da Alice

1c. Fotoni spediti da Alice sul canale quantistico

2a. Base casuale scelta da Bob per interpretare i fotoni

2b. Bit ricevuti da Bob

Discussione pubblica

3. Bob dichiara le basi con cui a misurato i fotoni

4a. Alice dice a Bob quali base erano corrette

4b. Questa informazione è presumibilmente corretta (se non ci sono stati origliamenti)

5a. Bob rivela alcuni bit della chiave scelti casualmente

5b. Alice conferma questi bit

Risultato

5c. Rimanenti bit segreti condivisi

E interessante notare come la probabilità che le risultanti stringhe di Alice e Bob concordino completamente non può essere resa pari ad 1. Possono, infatti, capitare degli errori, dovuti, ad esempio a ripolarizzazioni dei fotoni durante il transito anche in assenza di origliamento.

Se il numero degli errori capitati è relativamente piccolo essi potrebbero essere corretti mediante l'utilizzo di un concordato codice a correzione d'errore generando una sequenza controllata di bit. Questa sequenza può, quindi, essere inviata a, Bob su un canale pubblico. Se il codice ha sufficiente ridondanza, Bob può decodificare univocamente l'informazione disponibile per recuperare, con alta probabilità la stringa di Alice.

L'elementare controllo di qualità, appena descritto, è dispendioso in quanto una porzione significativa di bit deve essere sacrificata per fornire un ragionevole margine di sicurezza che i dati

dei due interlocutori siano identici, anche se gli episodi di spionaggio sono stati poco frequenti e hanno causato pochi errori.

Questo inconveniente può essere risolto da un più sottile protocollo di verifica che sfrutta il confronto di parità di un sottoinsieme casuale di bit scelto pubblicamente.
Il protocollo riconciliativo consta dei seguenti nuovi passi :

5' Alice e Bob permutano la stringa in base ad una permutazione su cui si sono accordati e, quindi, partizionano le loro stringhe permutate in blocchi di dimensione k tali che i singoli blocchi contengono, con bassa probabilità, più di un errore (la dimensione conveniente dei blocchi è 5).

6' Per ogni blocco, Alice e Bob, confrontano la parità. Blocchi con parità concorde sono ritenuti momentaneamente corretti (in quanto potrebbero capitare un numero pari di errori) mentre blocchi con parità discorde vengono sottoposti a ricerca bisettiva, rivelando al limite log2 le parità supplementari di sottoblocchi, finché l'errore è trovato e corretto. Per evitare di fornire troppa informazione ad Eva durante il processo di riconciliazione, Alice e Bob si accordano anche di scartare l'ultimo bit di ogni blocco o sottoblocco, di cui hanno rilevato la parità.

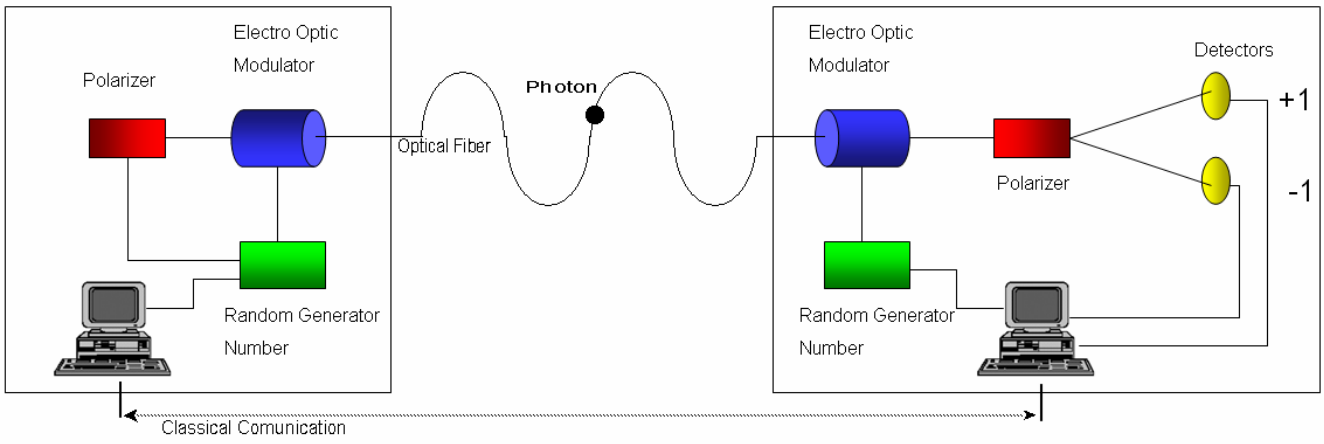
7' Per rimuovere gli errori rimasti (dai blocchi con parità concorde ma con un numero pari di errori), la permutazione casuale e la rivelazione della parità dei blocchi è ripetuta molte più volte, con dimensione dei blocchi incrementata, finché Alice e Bob stimano che al più un piccolo numero di errori rimangono nei dati. Anche tale approccio, tuttavia, è abbastanza dispendioso. Se la dimensione dei blocchi è scelta così che vi siano k blocchi, la probabilità, di non scoprire l'esistenza di tali errori è 1/k e il costo per questa strategia è di k bit (perchè ne perdiamo uno per blocco).

E possibile scegliere una strategia, alternativa che risulta. essere più efficiente della precedente:

5" Per ogni iterazione, Alice e Bob confrontano la parità di un sottoinsieme casuale, scelto pubblicamente, delle posizioni dei bit nelle loro rispettive stringhe. Se le stringhe non sono identiche, allora le parità del sottoinsieme casuale saranno in disaccordo con probabilità 1/2. Se un disaccordo è trovato, Alice e Bob intraprendono una ricerca bisettiva. con lo stesso criterio (cioè scegliendo un sottoinsieme casuale delle sottostringhe e così via), per trovare e rimuovere gli errori. Come nel precedente passo. l'ultimo bit di ogni sottoinsieme confrontato è scartato. Per assicurarsi che le stringhe siano veramente identiche. con una trascurabile probabilità di non scoprire i rimanenti errori sarà sufficiente attendere

20 accordi consecutivi. Osserviamo che con questa strategia la probabilità di non scoprire errori dopo k iterazioni è $(1/2)^k$ che è molto minore di $1/k$, per k grande, e comporta la perdita di ugualmente k bit. A questo punto del protocollo. Alice e Bob sono in possesso di una stringa che è quasi certamente condivisa, ma solo parzialmente segreta, in quanto Eva ha, potuto apprendere tutti i bit di parità che essi hanno rivelato, oltre ai bit appresi attraverso le sue misurazioni. Prima di procedere, Alice e Bob devono necessariamente stimare l'intensità dell'origliamento e questo può essere fatto in base al numero di errori che hanno incontrato e corretto, all'intensità dell'impulso originale ed all'efficienza quantistica dei rilevatori di Bob. Se osservano un sensibile origliamento, scartano i loro dati e riprovano la, trasmissione quantistica.

Se Alice e Bob ritengono che Eva abbia. appreso poca informazione, possono proseguire il protocollo estraendo dalla stringa riconciliata una sottostringa più piccola ma quasi certamente segreta, applicando la, tecnica. dell'amplificazione della riservatezza descritta di seguito. Sia x la stringa riconciliata e n la sua. lunghezza. é possibile dimostrare che se la conoscenza, di Eva circa x non è più di k bit , una. funzione hash, scelta. pubblicamente e casualmente da un'appropriata classe di funzioni $h:\{0,1\}^n \rightarrow \{0,1\}^{(n-k-s)}$ mapperà x in una stringa h(x) per la quale l'informazione attesa da Eva è minore di 2^{-s} ln2 bit, dove s >0 è un arbitrario parametro di sicurezza.



Strategie di origliamento

Sia μ il numero atteso di fotoni per impulso luminoso. Se μ è sufficientemente più piccolo di 1, esso è approssimativamente anche la probabilità che un fotone venga percepito all'interno di un impulso da un detector perfettamente efficiente. Diciamo che un impulso è con successo se Bob lo percepisce nella base originale scelta da Alice. In altri termini gli impulsi con successo sono quelli che contribuiscono ad un bit nella trasmissione quantistica. Fatte queste premesse, analizziamo più in dettaglio le varie strategie di origliamento che Eva potrebbe seguire.

Intercettare/Rimandare

In tale strategia, Eva intercetta alcuni impulsi luminosi e li legge nella base da lei scelta. Per ogni impulso i detector perfettamente efficienti di Eva riescono a percepire un fotone. Quando questo avviene. Eva fabbrica e manda a Bob un impulso della stessa polarizzazione da lei percepita, ma anche della stessa intensità, per evitare di essere scoperta da Bob. Naturalmente Eva indovina l'esatta polarizzazione con probabilità 1/2. E' dimostrato che almeno il 25% degli impulsi intercettati o rispediti da Eva produrranno degli errori se successivamente vengono misurati da Bob. Inoltre. se ci sono t errori nella trasmissione quantistica.. Alice e Bob possono stimare che meno di $4t + 5\sqrt{12t}$ dei loro bit sono stati soggetti ad una strategia di intercettato/rimandato e che l'ammontare di informazione lasciata ad Eva non vale più di $(4/\sqrt{2}) + 5\sqrt{(4+2\sqrt{2})t}$ bit della trasmissione quantistica. Quindi Alice e Bob potrebbero tentare di determinare empiricamente la percentuale d'errore attesa in assenza di origliamento e usare la differenza tra la percentuale d'errore predetta, e quella osservata, per stimare l'ammontare di informazione lasciata ad Eva attraverso tale strategia.

Divisione del raggio

Tale attacco si basa sul fatto che gli impulsi trasmessi non sono, in genere, a singoli fotoni. Per portare questo attacco, Eva usa uno specchio parzialmente argentato o un dispositivo equivalente, per deviare a sè una frazione f dell'intensità del raggio iniziale, lasciando passare la rimanente frazione 1-f a Bob. Per evitare perdite di informazione misurando gli impulsi nelle basi sbagliate, Eva potrebbe depositare la sua frazione d'impulso finche le corrette basi non sono state annunciate nella

discussione pubblica. (memorizzazione d'impulso). Quando ciò verrà fatto, Eva misurerà i suoi impulsi in queste basi. Eva riuscirà a percepire un fotone ed otterrà, quindi, i bit di Alice per quell'impulso. Benché tale procedimento in teoria, funzioni, in pratica non lo si può applicare per l'impossibilità tecnica di conservare fotoni per più di una piccola frazione di secondo. Osserviamo che tale attacco non introduce errori, ma fa. ridurre l'intensità dell'impulso che giunge a Bob di un fattore 1-f. Inoltre, se f è piccola, Alice e Bob potrebbero attribuire la riduzione d'intensità a cause naturali, per cui tale attacco non verrebbe rilevato. Osserviamo che se Eva volesse misurare immediatamente i suoi fotoni apprenderebbe una frazione approssimativamente pari a $\mu/2$ della stringa di Alice (prendendo f = 1; 1/2 perché con tale probabilità indovinerebbe la base) se effettuasse misure nelle basi canoniche ed una frazione non più grande di $\mu\sqrt{2}/2$ se utilizzasse la base Breidbart dove $\sqrt{2}/2$ è la probabilità di successo. La soluzione più semplice che Alice e Bob possano trovare a tale attacco è di attendere un tempo arbitrariamente lungo, sufficiente per far sì che gli impulsi si rovinino nel tempo, e solo allora annunciare le basi in cui hanno effettato le misure, ed inoltre utilizzare impulsi molto deboli in maniera tale che il raggio non possa essere diviso significativamente.

Oblivious Transfer

Nell'oblivious transfer (OT), ed in particolare nell'one out of two OT, che è quello che analizzeremo in questa sezione, Alice parte con due messaggi di due bit. di sua scelta. Lo scopo del protocollo è, per Alice, trasmettere i messaggi a Bob in maniera tale che egli possa scegliere di ricevere uno di loro (apprendere il suo valore con probabilità d'errore esponenzialmente piccola) ma non possa ottenere informazioni significative su entrambi, mentre Alice rimane completamente ignorante di quale dei due bit Bob abbia, ricevuto. Vedremo che nessuna parte può ingannare (cioè deviare dal protocollo mentre lo eseguono) in maniera tale da ottenere più informazioni di quelle che sono consentite dal protocollo. Assumiamo che le trasmissioni quantistiche consistano di serie di impulsi molto deboli di luce polarizzata e che l'impulso non possa essere memorizzato per una significativa lunghezza di tempo così che il ricevente risulti costretto a misurare ogni impulso prima che arrivi il successivo altrimenti perde l'opportunità di misurarlo.

Il protocollo

Definiamo innanzitutto con d la percentuale di conteggio oscuro, cioè la probabilità che un detector registri un conteggio durante un lasso di tempo nel quale nessun fotone è incidente su di esso (quindi, è una probabilità d'errore) e con q l'efficienza quantistica. vale a dire la probabilità di registrare un conteggio quando un fotone è incidente sul detector (un tipico fotomoltiplicatore può avere $d = 1\,0^{-5}$ e q = 25%). Siano, ora b_0 e b_1 i bit di Alice e sia, c la scelta di Bob (cioè Bob vuole ottenere b_c).

Il protocollo per l'OT è il seguente:

1. Bob dice ad Alice l'efficienza quantistica q e la percentuale di conteggio oscuro d dei suoi detector. E' necessario adattare il protocollo alle limitazioni fisiche dell'apparato rilevatore di Bob se non si vuole compromettere seriamente la probabilità di successo dello stesso. Se questi valori sono soddisfatti. Alice manda successivamente a Bob l'intensità μ dell'impulso luminoso che vorrà utilizzare, la frazione a di tale impulso che si attende che Bob percepisca, con successo, e la percentuale ε di errore sui bit che sarà disposta a correggere nei dati di Bob, per compensare il suo calcolo oscuro e le altre sorgenti di rumore. Alice decide anche su un parametro di sicurezza N, usato nel seguito, e lo annuncia a Bob. I due, infine, si accordano su un codice binario lineare a correzione d'errore capace di correggere, con

alta. probabilità, parole a N bit trasmesse con probabilità d'errore ε.

2. Alice manda a Bob una sequenza, casuale di *2N/a* impulsi luminosi, di intensità μ nelle quattro polarizzazioni canoniche (rettilinea orizzontale e verticale e diagonale a 45 gradi e a 135 gradi).

3. Bob decide casualmente, per ogni impulso se misurarlo nella base rettilinea o diagonale e registra le basi e i risultati delle misure in una tavola, ogni volta che (con probabilità approssimativamente a) percepisce un impulso. Quindi Bob riceverà con successo approssimativamente 2N impulsi (2N/a * a cioè 2N/a mandati da Alice, moltiplicato per la frazione a di essi che Bob dovrebbe ricevere). Se egli ne ha ricevuto di più (e ciò può capitare a causa. di conteggi multipli), ignora l'eccesso; se ne ha ricevuto di meno (e ciò può capitare a causa di perdite naturali nel canale quantistico) completa. la tavola. con entrate casuali così da avere esattamente 2N entrate. Bob, infine dice ad Alice i tempi d'arrivo di tutti i 2N impulsi, ma non le basi che ha usato per misurarli ne i risultati delle sue misure (ciò assicura Alice che Bob abbia misurato effettivamente gli impulsi).
4. Alice rivela a Bob le basi che ha usato per mandare ognuno degli impulsi da lui ricevuti.

5. Bob partiziona, i suoi impulsi in due insiemi di N impulsi ciascuno: un *buon* insieme consistente (per quanto è possibile) di impulsi ricevuti nella corretta base, ed un cattivo insieme consistente di impulsi ricevuti nella base errata. Egli dice ad Alice gli indirizzi dei due insiemi ma non le dice qual'è il buono o il cattivo insieme. A questo punto del protocollo Bob condivide con Alice una parola (cioè una stringa a N bit, con un'attesa percentuale d'errore non più grande di ε se ha indovinato per meno di N volte la corretta polarizzazione), corrispondente al suo buon insieme di misure: condivide niente riguardo al suo cattivo insieme di misure, supposto che egli segua fedelmente il protocollo. D'altra parte Alice non sa quale parola condivide con Bob. Vediamo, ora, come Bob possa correggere gli errori occorsi nel suo buon insieme.

6. Usando il concordato codice a correzione d'errore, Alice computa le sindromi delle parole corrispondenti ad ogni suo insieme e le manda a Bob su un canale libero da, errori. Da tali sindromi, Bob è in grado di recuperare la parola originale corrispondente al suo buon insieme, ma non quella corrispondente al suo cattivo insieme (questo per la proprietà. di opportuni codici detti codici concatenati, che sono in effetti quelli scelti per la correzione degli errori).

Inoltre Alice computa un sottoinsieme casuale di parità per ogni insieme e rivela a Bob gli indirizzi definenti tali sottoinsiemi ma non le risultanti parità. A questo punto, Bob conosce una di queste parità. esattamente (quella relativa al suo buon insieme), mentre non conosce niente (o quasi niente) circa l'altra parità. D'altra parte, Alice conosce entrambe le parità, ma non sa quale di queste Bob conosce. Siano x_0 e x_1 questi due bit di parità e sia c* la conoscenza di Bob (cioè Bob conosce x_c).

7. Bob dice ad Alice se c = c* o meno (notiamo che questa è la prima volta c entra in gioco nel protocollo).

8. Se c = c*, Alice manda a Bob $x_0 \oplus b_0$ e $x_1 \oplus b_1$ nell'ordine prescritto (solo ora entrano in gioco b_0 e b_1), altrimenti gli manda $x_0 \oplus b_1$ e $x_1 \oplus b_0$. Da queste informazioni. Bob è in grado di apprendere il suo b_c

Notiamo che, poiché Alice non sa se Bob conosce x_0 e x_1, non può rendersi conto se egli ha appreso b_0 o b_1. D'altra parte. Bob conosce solo x_0 o solo x_1, per cui non può apprendere contemporaneamente b_0 e b_1. Quindi, l'OT è realizzato.

Appendice: Situazione Attuale

In una banca austriaca è stata effettuata una transizione elettronica di denaro usando fotoni "entangled" per creare un codice di comunicazione indecifrabile. Anche se esistono già prodotti commerciali basati sulla crittografia quantistica, nessuno di questi utilizza fotoni correlati per garantire una comunicazione sicura. Il collegamento è stato usato mercoledì 21 aprile per trasferire denaro fra il municipio di Vienna e la Bank Austria Creditanstalt. I fotoni "entangled" (correlati quantisticamente) obbediscono agli strani principi della meccanica quantistica: disturbando lo stato di uno, si disturba automaticamente anche l'altro, non importa a che distanza si trovino. La coppia di fotoni correlati utilizzata era stata generata inviando un laser attraverso un cristallo per dividere singoli fotoni in due. Un fotone di ogni coppia correlata è stato poi inviato dalla banca al municipio attraverso una fibra ottica. Giunti a destinazione, è stato osservato il loro stato di polarizzazione. In questo modo entrambe le estremità del collegamento avevano a disposizione lo stesso dato (un uno oppure uno zero). In questo modo è stato possibile costruire una chiave crittografica con la quale proteggere da terzi la transazione finanziaria.

Bibliografia

C. Bennett, F. Bassette, G. Brassard, L. Salvail e J. Smolin: *Experimental quantum cryptography Journal of Cryptology.*

C. Bennett, G. Brassard, L. Salvail, J. Smolin, C. Crepeau e M. H. Skubiszewska: *Pratical Oblivious Ttransfer.*

C. Bennett, G. Brassard, A. Ekert: *Crittografia quantistica, in Le Scienze n° 192.*