Tecniche di Progettazione Automatica **Anno Acc. 1995-96**
PROF. ALFREDO DE SANTIS

CRITTOGRAFIA QUANTISTICA

a cura di Rosario Cretella e Gerardo Gioiella *31 maggio 1996*

Indice

1 Introduzione

La crittografia quantistica nasce dal connubio fra meccanica quantistica e crittologia. L'impiego in campo crittografico della meccanica quantistica consente risultati impossibili da conseguire con la sola matematica. 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. Pertanto chi spia un canale di comunicazione quantistico vi provoca inevitabilmente una perturbazione che mette in allarme gli utenti legittimi. La crittografia quantistica sfrutta questo fenomeno per consentire a due utenti che mai si sono incontrati e che non condividano a priori informazioni segrete di comunicare in assoluta segretezza sotto il naso del nemico.

Questi concetti furono introdotti per la prima volta nel 1970 da Stephen J. Wiesner in un articolo intitolato *Conjugate Coding.* In tale articolo Wiesner spiegava, almeno in linea di principio, come la fisica dei quanti potesse essere impiegata per ottenere due compiti inaccessibili alla fisica classica. Uno era quello di produrre banconote che non potessero essere contraffatte, l'altro era uno schema per combinare due messaggi classici in un unica trasmissione quantistica dalla quale il destinatario potesse ricavare uno o l'altro dei messaggi, ma non entrambi. Più tardi, nel 1979, Bennet e Brassard utilizzarono i concetti esposti da Weisner per realizzare un sistema quantistico in sostituzione della crittografia a chiave pubblica tramite il quale due utenti potevano comunicare in tutta riservatezza, e con sicurezza assoluta salvo violazione delle leggi fisiche accertate.

Negli ultimi anni sono stati sviluppati altri protocolli basati sulla crittografia quantistica e in questa trattazione oltre ai crittosistemi quantistici a chiave pubblica tratteremo un protocollo di *bit commitment* quantistico e un protocollo, pure quantistico, per effettuare *l'oblivious transfer* senza limitazioni computazionali. L'implementazione di questi tre protocolli richiede l'esistenza di due canali di trasmissione, uno dei quali è pubblico e l'altro quantistico. Supponiamo che il canale pubblico possa essere soggetto ad ascolto passivo (ascolto e memorizzazione in data-base delle informazioni da parte di un nemico), ma non all'alterazione dell'informazione. Invece il canale quantistico può essere soggetto a intercettazione e alterazione dei dati ma non in maniera passiva poiché un eventuale intercettazione da parte di un nemico viene subito rilevata dai leggittimi proprietari del canale.

Uno svantaggio di questo approcio è che le trasmissioni quantistiche sono necessariamente molto deboli e non possono essere amplificate. Inoltre la crittografia quantistica non può fornire la firma digitale ne tanto meno risolvere dispute davanti al giudice.

2 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. Normalmente un fascio di luce è non polarizzato e tali sono anche i fotoni che lo compongono. Se un fotone o un insieme di essi (raggio luminoso) attraversa un filtro Polaroid (avente proprietà di lasciar passare luce polarizzata solo nella direzione del suo asse), otterremo un fotone polarizzato nella stessa direzione dell'asse del filtro (vedi Figura 1).

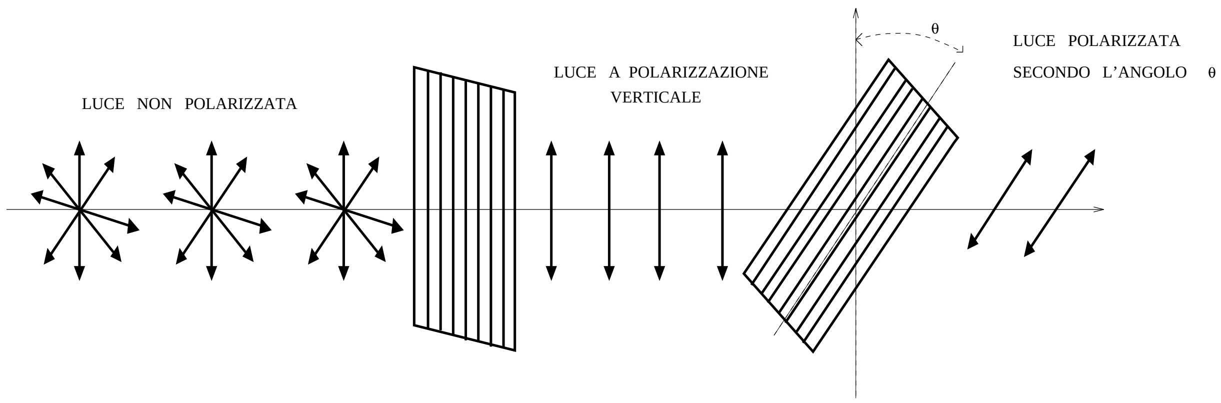

Figura 1: polarizzazione di un raggio di luce

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, 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, vericale, 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 (vedi Figura 2). 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 o 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 gradi, che però possono essere identificati con sicurezza mediante un identico dispositivo ruotato di 45 gradi rispetto all'orientazione originale. Ovviamente l'apparecchio così ruotato, a sua volta, non può distinguere i fotoni verticali da quelli orizzontali.

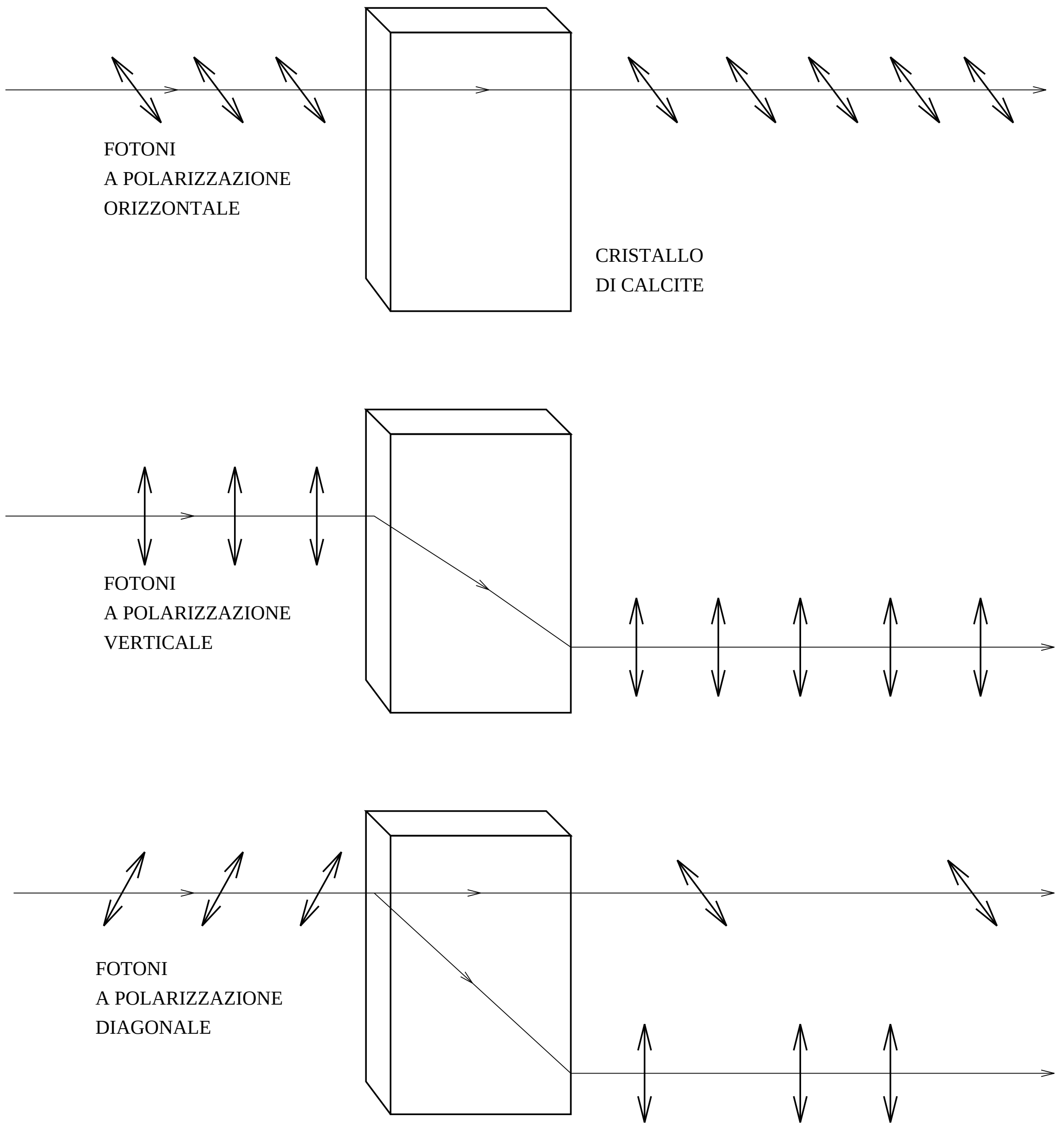

Figura 2: cristallo di calcite attraversato da fotoni

Formalmente la meccanica quantistica rappresenta lo stato interno di un sistema quantistico (ad esempio la polarizzazione di un fotone) come un vettore di lunghezza unitaria in uno spazio lineare sul campo dei numeri complessi, lo spazio di Hilbert. Le dimensioni di tale spazio dipendono dal sistema quantistico ed ogni misura fisica che può essere effettuata sul sistema corrisponde alla risoluzione del suo spazio di Hilbert in sottospazi ortogonali, uno per ogni possibile esito della misura.

Nel nostro caso, lo spazio di Hilbert per un singolo fotone polarizzato è 2-dimensionale, così che lo stato di un fotone può essere completamente descritto come una combinazione lineare dei due vettori $r_1 \equiv (1,0)$ e $r_2 \equiv (0,1)$, rappresentanti rispettivamente le polarizzazioni orizzontale e verticale. In particolare un fotone polarizzato ad un angolo α con l'orizzontale è descritto dallo stato del vettore $(\cos\alpha, \sin\alpha)$. I due vettori ortogonali r_1 e r_2 costituiscono la base rettilinea e semplificano la risoluzione dello spazio di Hilbert a due dimensioni in due sottospazi ortogonali ad una dimensione. In generale ogni coppia di stati di polarizzazione ortonormali e linearmente indipendenti tra loro, attraverso una combinazione lineare dei quali è possibile esprimere la polarizzazione di ogni fotone, sarà riferita come una base. Una base alternativa per lo spazio di Hilbert è, quella diagonale, determinata dai vettori $d_1 \equiv (\gamma, \gamma)$ e $d_2 \equiv (\gamma, -\gamma)$ dove $\gamma = \sqrt{2}/2$. In questa base d_1 rappresenta un fotone a 45 gradi e d_2 un fotone a 135 gradi. Wiesner definisce due basi (quali quella rettilinea e quella diagonale) essere coniugate se ogni vettore di una base ha una proiezione di uguale lunghezza su tutti i vettori dell'altra base. Ciò significa che un sistema preparato in uno stato specifico di una base si comporterà in maniera interamente randomizzata e perderà tutta l'informazione memorizzata in esso quando sarà soggetto a misure corrispondenti ad una base coniugata alla sua. A causa della natura complessa dei suoi coefficienti, lo spazio di Hilbert 2-dimensionale ammette anche una terza base coniugata ad entrambe le basi rettilinea e diagonale ed è quella circolare, data dai vettori $c_1 \equiv(\gamma,\gamma i)$ e $c_2 \equiv(\gamma i,\gamma)$ dove $i = \sqrt{-1}$. Queste basi sono dette anche basi canoniche e nel seguito saranno sufficienti solo quella rettilinea e quella diagonale per i nostri scopi. Inoltre ci sarà utile per le misurazioni anche un'altra base, detta base Breidbart, la quale è angolata a 22.5 gradi con l'orizzontale, esattamente a metà tra la base rettilinea e quella diagonale e, quindi, dalla definizione, non coniugata alle precedenti.

In alcuni casi, utilizzeremo la notazione di Dirac per denotare lo stato di un fotone. Per stato di un fotone si intende l'insieme di tutte le caratteristiche descriventi un fotone, quali energia cinetica, velocità, momento, polarizzazione, componenti di spin ed altro ancora. In particolare, di queste caratteristiche, prenderemo in considerazione solo la polarizzazione e le componenti di spin. Se $\binom{u}{v}$ è lo stato di un fotone nello spazio di Hilbert (dato in termini delle sue componenti rispetto a qualche base), lo denoteremo con $|\phi\rangle=\binom{u}{v}$.

$\langle\phi| = (u^*, v^*)$ denoterà il complesso coniugato trasposto, mentre $\langle\phi_1|\phi_2\rangle = (u_1^*,v_1^*)\binom{u_2}{v_2} = u_1^*u_2 + v_1^*v_2$ è il prodotto scalare. Utilizzando tale formalismo la base rettilinea verrà anche denotata con $+ = (|\leftrightarrow\rangle, |\updownarrow\rangle)$ quella diagonale con $\times = (|\nearrow\rangle,|\searrow\rangle)$.

Un ulteriore risultato della fisica quantistica indica che quando una misura è effettuata su un fotone nello stato $|\phi\rangle$, ogni esito può occorrere con probabilità data dal quadrato della lunghezza della proiezione di $|\phi\rangle$ nel corrispondente sottospazio. Come risultato della misura, lo stato originale $|\phi\rangle$ è cancellato e replicato dal vettore proiezione (rinormalizzato a lunghezza unitaria) corrispondente all'esito osservato. In altri termini, ciò significa che se un fotone ϕ polarizzato è soggetto ad una misura di polarizzazione lungo l'asse θ, esso si comporta come un fotone θ-polarizzato con probabilità $\cos^2(\phi-\theta)$ (quindi, se $\phi = \theta$ la probabilità di essere un fotone θ-polarizzato è 1 mentre quella di essere un fotone $\theta + 90°$-polarizzato è 0) e come un fotone $\theta+90°$-polarizzato con probabilità complementare $\sin^2(\phi-\theta)$ (e quindi, se $\phi = \theta+90°$, si comporta come un fotone $(\theta+90°)$-polarizzato con probabilità 1 e come un fotone θ-polarizzato con probabilità 0).

Infine notiamo che se $\phi = \theta + 45°$ e, quindi, se stiamo misurando la polarizzazione diagonale di un fotone inviato con polarizzazione rettilinea (o viceversa), il risultato sarà totalmente casuale, cioè il fotone si comporterà con probabilità $\cos^2(45°) = 1/2$ come un fotone a polarizzazione orizzontale (diagonale a 45 gradi) e con probabilità $\sin^2(45°)=1/2$ come un fotone a polarizzazione verticale (diagonale a 135 gradi). Quindi, tutta l'informazione memorizzata nel fotone sarà totalmente persa, come avevamo predetto.

Da un punto di vista pratico si possono trasmettere bit d'informazione utilizzando fotoni opportunamente polarizzati a 0, 45, 90 o 135 gradi, in modo tale che ogni fotone contenga un bit d'informazione. La polarizzazione del fotone trasmesso sarà determinata dal valore del bit da rappresentare (0, 1) e dalla base di conversione utilizzata (rettilinea, diagonale). Un possibile schema è il seguente :

R	D	Bit
$\leftrightarrow$	$\nearrow$	0
$\updownarrow$	$\searrow$	1

Tabella 1: R base rettilinea - D base diagonale

Quindi un utente che voglia trasmettere il bit 1, sceglie una base per rappresentare quel bit (es. R rettilinea) e manda sul canale quantistico il fotone rappresentante quel bit, ossia un fotone con polarizzazione $\updownarrow$. Colui che riceve può misurare il fotone e quindi identificare il bit, solo se conosce la base con cui esso è stato convertito. Se la base di conversione non è nota occorre sceglierla a caso fra R e D ottenendo così una risposta giusta con probabilità 1/2 e una risposta sbagliata con eguale probabilità.

3 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 è ottenuto in modo tale che essi, da successive conversazioni su un canale ordinario non quantistico possano dire, con alta probabilità, se la trasmissione quantistica è stata disturbata nel transito da un eventuale origliatore. Se la trasmissione quantistica non è 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 finchè riportano un successo. Benchè 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.

3.1 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, Eve. Un bit è rappresentato da un fotone polarizzato come illustrato in Tabella 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 origliatore 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.	$\nearrow$	$\updownarrow$	$\searrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\searrow$	$\nearrow$	$\updownarrow$	$\searrow$	$\nearrow$	$\nearrow$	$\updownarrow$
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

Tabella 2: Esempio di una trasmmissione

Descrizione :

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

È 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 $\log k$ parità supplementari di sottoblocchi, finchè l'errore è trovato e corretto. Per evitare di fornire troppa informazione ad Eve 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, finchè 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 l blocchi, la probabilità di non scoprire l'esistenza di tali errori è $1/l$ e il costo per questa strategia è di l bit (perché ne perdiamo uno per blocco).

È 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 l iterazioni è $(1/2)^l$ che è molto minore di $1/l$, per l grande, e comporta la perdita di ugualmente l 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 Eve 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 Eve 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. Definiamo innanzitutto un bit deterministico di informazione su x il valore $e(x)$ di un'arbitraria funzione $e : \{0,1\}^n \to \{0,1\}$. Bit di parità sono bit deterministici; bit di informazione di Shannon non lo sono. É possibile dimostrare che se la conoscenza di Eve circa x non è più di l bit deterministici, una funzione hash, scelta pubblicamente e casualmente da un'appropriata classe di funzioni $h : \{0,1\}^n \to \{0,1\}^{(n-l-s)}$, mapperà x in una stringa $h(x)$ per la quale l'informazione attesa da Eve è minore di $2^{-s} \ln 2$ bit, dove $s > 0$ è un arbitrario parametro di sicurezza. Questa tecnica è applicabile per Alice e Bob perché i bit di parità sono un caso speciale di bit deterministici. Inoltre per poter scegliere una tale funzione di contrazione, non è neppure necessario che le due parti sappiano quali informazioni parziali possa avere l'origliatore sull'input. In particolare basta definire ciascun bit dell'output come la parità di un sottoinsieme indipendente ed aleatorio, concordato pubblicamente, dei bit di input.

3.2 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 inoltre 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 Eve potrebbe seguire.

3.2.1 Intercettare/Rimandare

In tale stategia, Eve intercetta alcuni impulsi luminosi e li legge nella base da lei scelta. Per ogni impulso, con probabilità approssimativamente μ, i detector perfettamente efficienti di Eve riescono a percepire un fotone. Quando questo avviene, Eve 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 Eve indovina l'esatta polarizzazione con probabilità 1/2. In [1], e ne daremo un cenno in seguito, è dimostrato che almeno il 25% degli impulsi intercettati o rispediti da Eve 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 Eve 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 Eve attraverso tale strategia.

3.2.2 Divisione del raggio

Tale attacco si basa sul fatto che gli impulsi trasmessi non sono, in genere, a singoli fotoni. Per portare questo attacco, Eve 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, Eve potrebbe depositare la sua frazione d'impulso finchè le corrette basi non sono state annunciate nella discussione pubblica (memorizzazione d'impulso). Quando ciò verrà fatto, Eve misurerà i suoi impulsi in queste basi. Con probabilità approssimativamente $f\mu$, Eve riuscirà a percepire un fotone ed otterrà, quindi, i bit di Alice per quell'impulso. Benchè 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 Eve 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. Riguardo a tale attacco, è dimostrato in [1], che se la trasmissione quantistica consiste di N impulsi con successo, Alice e Bob possono stimare che Eve ha appreso meno di $N\mu + 5(\sqrt{N\mu(1-\mu)}$ bit, dove il secondo termine è la deviazione standard.

3.2.3 Note addizionali

In conclusione, la frazione della stringa di Alice lasciata ad Eve in entrambe le strategie di origliamento, è limitata superiormente da $\rho = \mu + (4/\sqrt{2})p$, dove μ è l'intensità dell'impulso a monte del canale e p è la percentuale di bit d'errore. Tale formula viene fuori dal fatto che Eve può apprendere una frazione approssimativamente μ (assumendo f=1) dei bit attraverso la deviazione del raggio, ed un numero di effettivi bit non più grande di una frazione $(4/\sqrt{2})$ attraverso l'intercettare/rimandare. A causa della possibile correlazione tra queste due specie d'informazione (intercettare/rimandare un impulso diviso), la totale informazione ottenuta da Eve, sarà minore della somma di questi due termini. La stima su ρ assume che Eve possa ritardare le misure fin quando non vengono annunciate le corrette basi (se ciò non venisse fatto il primo termine della formula decrementerebbe da μ a $\mu/\sqrt{2}$) e, cosa ancora più importante, che tutti gli errori di trasmissione, che Alice e Bob scoprono, risultino dall'intercettare/rimandare. Ora, se N è il numero di impulsi con successo, Alice e Bob possono stimare il numero di bit lasciati passare ad Eve come $l = N\rho + 5\sqrt{N\mu(1-\mu) + (4+2\sqrt{2})p}$ dove il primo termine rappresenta l'attesa informazione di Eve ed il secondo termine è la deviazione standard. I due termini sotto radice rappresentano il contributo della varianza dell'informazione di Eve tenendo conto del numero di impulsi splittati a fissato μ e il numero di bit effettivamente sottratti da Eve attraverso l'intercettare/rimandare. Prendiamo la radice quadrata della somma e non la somma delle radici quadrate (cioè addizioniamo le varianze piuttosto che le deviazioni standard), perché la probabilità di successo dell'attacco a divisione del raggio è indipendente dalla probabilità di successo dell'intercettare/rimandare, considerando solo gli impulsi con successo. Vediamo anche di dare l'idea di base delle dimostrazioni precedenti. Essa consiste nel descrivere un arbitrario stato di polarizzazione come un punto $Q = (X,Y,Z)$ su una sfera unitaria $X^2+Y^2+Z^2=1$, detta sfera di Poincarè. I parametri X,Y,Z rappresentano rispettivamente le componenti rettilinee, diagonali e circolari dello stato Q. Se un fotone nello stato Q è misurato nelle basi $(P,-P)$ (dove P è ugualmente del tipo (X,Y,Z), cioè un punto sulla sfera) esso si comporta come se si trovasse nello stato P con probabilità $\cos^2(\alpha/2) = (1+cos\alpha)/2$, dove α è l'angolo tra P e Q visto dal centro della sfera di Poincarè, e come se fosse nello stato $-P$ con probabilità complementare $\sin^2(\alpha/2) = (1-cos\alpha)/2$. Osserviamo che tali probabilità sono diverse, come espressioni, da $\cos^2(\phi-\theta)$ e $\sin^2(\phi-\theta)$ ma sono concettualmente le stesse in quanto ugualmente abbiamo informazione deterministica solo quando $Q = \pm P$, nel qual caso $\alpha/2$ è o 0 gradi o 90 gradi. Attraverso semplici considerazioni si giunge ad espressioni probabilistiche che si riferiscono a probabilità di errore di Eve e di Bob che raggiungono il loro valore minimo rispettivamente a 0.15 ed 1/4. Come conseguenza di ciò possiamo dedurre che l'origliatore non può effettuare nessuna misura sui fotoni che sono in transito da Alice a Bob, che produca più di 1/2 previsto bit d'informazione sulla loro polarizzazione (0 bit quando non indovina la base, 1 bit altrimenti, per cui in media 1/2). Inoltre ogni misura che produce $s \leq 1/2$ di previsto bit d'informazione, ha probabilità almeno $s/2$ di indurre una discrepanza quando i dati di Alice e Bob sono confrontati, assumendo che i fotoni siano misurati nella corretta base da Bob. Gli altri risultati e stime sulle deviazioni standard possono essere ottenuti attraverso la nozione di Big Brother. Assumiamo la presenza di un qualcuno a cui è data una moneta truccata ed una non truccata (la cui truccatura è sotto il suo controllo), che accede immediatamente a tutte le basi usate da Alice e che ha l'abilità di guardare ad ogni bit di Alice e apprendere i suoi valori in maniera affidabile, se egli sceglie di farlo. Ogni volta che Eve decide di misurare un impulso, il Big Brother interviene e la supplisce con una lettura simulata che è statisticamente indistinguibile dalla lettura che Eve avrebbe ottenuto senza la sua presenza. Il punto chiave è che il Big Brother non sempre ha bisogno di vedere i bit di Alice per supplire Eve: qualche volta può uscirsene lanciando una moneta. Senza scendere troppo nei dettagli delle dimostrazioni (che sono simili sia per l'intercettare/rimandare che per la divisione del raggio), accade che, nel caso in cui Eve sceglie la base Breidbart per le sue misurazioni, ogni volta che seleziona un impulso per l'intercettamento, il Big Brother lancia una moneta truccata e con probabilità $1/\sqrt{2}$ guarda i bit di Alice e li dà ad Eve; altrimenti egli lancia una moneta non truccata e dà il suo esito ad Eve. Nel caso in cui Eve scelga una base arbitraria (diversa da quella Breidbart) avente componenti X,Y,Z, il Big Brother guarda ai bit di Alice con probabilità X o Y (a seconda che la loro base sia rettilinea o diagonale) e li fornisce ad Eve; altrimenti le fornisce un lancio di moneta non truccata. Semplici considerazioni probabilistiche fanno giungere al termine $(4/\sqrt{2})t$, dove t è l'osservato numeri di errori. Denotando poi con l il numero di bit di informazione lasciati al Big Brother, sotto l'assunzione che Eve abbia usato le basi Breidbart per tutti gli intercettamenti, e con k il non noto numero di impulsi soggetti ad intercettato/rimandato, si verifica che t è una Binomiale $(k,1/4)$ ed l una Binomiale $(k,1/\sqrt{2})$, da cui seguono banalmente le stime sulle deviazioni standard.

3.3 Considerazioni finali

E' interessante notare che se anzichè massimizzare la sua informazione sulla chiave, Eve volesse massimizzare la sua (molto piccola) possibilità di indovinare l'intera chiave correttamente, la sua strategia ottimale sarebbe quella di effettuare tutte le misure nella base Breidbart. I risultati di tali misure, infatti, come abbiamo più volte ripetuto, si accordano con i bit di Alice con probabilità $p = (2+\sqrt{2})/4 \simeq 85\%$, e la provvista informazione di Shannon è pari a $1-p\log p+(1-p)\log(1-p) \simeq 0.399$ bit rispetto al 1/2 bit di attesa informazione deterministica provvista da una misura in base canonica. E' intuitivo anche che questa maggiore informazione probabilistica richiede, ad Alice e Bob, di gettare via maggiore informazione sulla trasmissione quantistica durante l'amplificazione della riservatezza. L'assunzione che facciamo sul canale quantistico, vale a dire che i messaggi pubblici non possano essere corrotti nel transito da Eve, è fondamentale perché è chiaro che ella, altrimenti, potrebbe porsi tra Alice e Bob ed impersonare ognuno di essi all'altro. Come risultato, Eve finirebbe con l'avere una stringa condivisa con Bob ed una con Alice. Questo inconveniente può essere risolto nella pratica o usando un canale pubblico non disturbabile con interferenze, o uno schema di autenticazione dell'informazione di Wegman-Carter. Nell'ultimo caso, tuttavia, Alice e Bob necessitano di avere a priori un modesto ammontare di informazione segreta condivisa che possa servire come chiave di autenticazione per i loro messaggi. Tale chiave viene utilizzata per produrre un'etichetta dipendente dal messaggio (di lunghezza arbitraria) e ciò è fatto in modo tale che Eve (ignorante di questa piccola chiave) ha solo una trascurabile probabilità di essere sicura di generare ogni altra valida coppia messaggio-etichetta (ciò sarà vero anche se Eve avesse un'illimitata potenza computazionale). L'etichetta così fornita evidenzia che il messaggio è legittimo e non è stato generato o alterato da Eve. I bit costituenti la chiave, tuttavia, sono gradualmente esauriti nello schema di Wegman-Carter e non possono essere riutilizzati senza compromettere la sicurezza incondizionata del sistema. Comunque ogni successiva istanza del protocollo fornisce Alice e Bob di un volume sostanzialmente grande di nuova informazione chiave, parte della quale può essere usata per sostituire i bit di autenticazione persi. Quindi, in tal caso, il protocollo implementerebbe l'espansione di chiave piuttosto che la distribuzione di chiave.

4 Oblivious Transfer

Nell'oblivious transfer(OT), ed in particolare nell'1 out of 2 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.

4.1 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 $d = 10^{-5}$ 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 (vedremo che devono essere tali da produrre particolari condizioni), 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. Osserviamo in particolare che a dovrebbe essere posto normalmente a $1 - e^{-(q\mu+2d)} \approx q\mu$, la probabilità di Poisson di rilevare 1 o più fotoni (o anche conteggi oscuri) in un impulso di intensità μ, mentre ε dovrebbe normalmente essere posto a $d/a \approx d/q\mu$. La scelta di Alice di μ è guidata dalla necessità di porre simultaneamente a alto abbastanza ed ε basso abbastanza da fare in modo che le ricezioni di Bob siano meno rumorose e più efficienti. Mostreremo in seguito che un OT sicuro può essere ottenuto quando $H(2\varepsilon) < \frac{1}{2} - \frac{(1-e^{-\mu}-\mu e^{-\mu})}{2a}$, dove H è la funzione entropia.

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 ($\frac{2N}{a} \cdot a = 2N$, 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 nè 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 (o quasi niente, se ha misurato più di N bit nelle corrette basi) 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 $\hat{c}$ la conoscenza di Bob (cioè Bob conosce $x_{\hat{c}}$).

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

8. Se $c = \hat{c}$, 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 o 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. Per garantire la sicurezza dell'OT, possiamo enunciare il seguente teorema:

Teorema 4.1 *Sia Δ il dato che Bob ottiene dal protocollo. Almeno una tra $H(b_0|\Delta, b_1)$ e $H(b_1|\Delta, b_0)$ è esponenzialmente chiusa (in N) ad 1. Senza riguardo di cosa accade, Alice non apprende niente.*

In pratica questo significa che Bob o conosce b_0 o conosce b_1 ma non può conoscere entrambi, altrimenti entrambe le entropie varrebbero 0. Il resto del capitolo costituisce la dimostrazione di questo teorema.

4.2 Ulteriori considerazioni sul protocollo

Per consentire ad un onesto Bob di ricevere il bit correttamente e per prevenire un'ingannevole Bob dall'apprendere qualcosa circa entrambi i bit, è necessario utilizzare due strumenti fondamentali: *codici concatenati* ed *amplificazione della riservatezza.* Quest'ultima è stata già abbondantemente descritta nel capitolo 3, per cui ne daremo solo un breve cenno, mentre ci soffermeremo con più attenzione sui codici.

4.2.1 Codici concatenati

Il principale problema che riveste il nostro protocollo riguarda la necessità di fornire Bob di informazione attraverso la quale egli possa correggere la piccola percentuale d'errore dei suoi buoni impulsi (dovuti a conteggi oscuri ed a rumori inevitabili), con ragionevole sforzo di decodifica e con probabilità d'errore residua esponenzialmente piccola (in N), ed allo stesso tempo, prevenire Bob (eccetto con probabilità di successo esponenzialmente piccola) dal correggere tutti gli errori nel suo cattivo insieme, anche con sforzo di decodifica illimitato. Un codice concatenato, combinazione cioè di un codice RS ed un codice binario lineare casuale di dimensione esponenzialmente più piccola del primo, è un'appropriata scelta per tali scopi. Tali codici offrono probabilità d'errore residuo esponenzialmente piccola, mentre permettono all'informazione di essere trasmessa efficientemente attraverso un rumoroso canale binario simmetrico ad un tasso $R(\varepsilon) \leq 1$ - $H(2\varepsilon)$. La loro decodifica può essere compiuta in maniera efficiente dall'algoritmo di Berlekamp, per i codici RS, e da una ricerca di forza bruta, per il codice lineare (tale ricerca, come è ben noto, richiede tempo esponenziale nella dimensione del codice, ma ciò è comunque efficiente poiché tale codice è scelto di dimensione esponenzialmente più piccola di quella di un codice RS). Il nostro uso di un codice a correzione d'errore è non standard, nel senso che, invece di mandare una parola codice nel rumoroso canale quantistico, Alice manda una parola casuale. Inoltre, per permettere efficienti decodifiche a Bob, Alice gli manda anche la corrispondente sindrome su un canale senza rumore. Si verifica che ciò non altera lo sforzo di decodifica di Bob. Il fatto che questi codici prevengono Bob dal correggere gli errori nel suo cattivo insieme, anche con sforzo di decodifica illimitato, è più complicato da dimostrare. Vedremo, tuttavia, che qualsiasi sia l'insieme di basi (canoniche e non) che Bob usa al passo 3 per ottenere i suoi dati e qualsiasi sia la partizione che egli sceglie al passo 5, l'informazione addizionale provvista a lui da Alice non gli assicura di correggere gli errori in entrambi gli insiemi o anche ottenere informazione su più di uno dei bit di Alice (eccetto con probabilità esponenzialmente piccola).

4.2.2 Amplificazione della riservatezza

Avendo già discusso di tale argomento, ci limiteremo ad enunciare in particolare una proprietà che ci sarà utile nelle dimostrazioni successive. Denotando con x una stringa di lunghezza N, è dimostrabile che se Bob conosce una proporzione $\gamma < 1 - H(2\varepsilon)$ dei bit di x prima di ricevere la sindrome, e se abbastanza bit di controllo sono provvisti per correggere una proporzione ε di errori, allora la probabilità che Bob conosce ogni cosa circa la parità di un sottoinsieme casuale dei bit di x rimane arbitrariamente piccola ($2^{-s}/\ln 2$ con $s \geq 0$ un arbitrario parametro di sicurezza), supposto che x risulti sufficientemente lungo. Nel nostro caso, x sarebbe la stringa relativa al cattivo insieme di Bob, sulla quale egli conosce poco o niente.

4.3 Analisi dei vari attacchi

I motivi per cui Alice e Bob sono tentati ad ingannare sono, evidentemente, per Alice, cercare di apprendere la scelta di Bob, per Bob, cercare di apprendere entrambi i bit mandati da Alice. Vedremo come nessun attacco sia in grado di raggiungere questi obiettivi, nonostante che Alice e Bob possano disporre di un'illimitata potenza computazionale.

4.3.1 Attacchi di Alice

Notiamo, innanzitutto, che Alice potrebbe ingannare al passo 8 dando a Bob il complemento di quello che egli vorrebbe. In questo caso, tuttavia, non possiamo parlare di vero e proprio inganno, in quanto comunque un OT verrebbe eseguito, anche se il bit trasferito non sarà quello voluto. Per determinare, o almeno dare un'indicazione, circa il valore di c (sul quale Bob non rivela niente fino al passo 7), Alice potrebbe rifiutarsi di mandare una delle due sindromi al passo 6. Il punto è che Bob non avrebbe modo di scoprire tale comportamento se Alice manda il rifiuto per il suo cattivo insieme. Quindi, se Bob reclama, Alice apprende che ciò è dovuto al fatto che ella ha scelto di mandare il rifiuto per l'insieme buono. Questo inganno, tuttavia, potrebbe non dare frutti in quanto Bob potrebbe scoprire Alice nell'atto dell'ingannare, prima che ella abbia una possibilità di apprendere qualcosa : la scelta c di Bob, infatti, non è usata nel protocollo fino al passo 7 e, quindi, dopo che Alice manda le sue sindromi. Se, invece, Bob non reclama, Alice può dedurre di aver mandato il rifiuto per il cattivo insieme. Ciò è più serio perché in questo caso il protocollo potrebbe continuare ed Alice potrebbe apprendere la scelta c di Bob, in quanto, avendo mandato una sola sindrome, saprebbe il bit $x_{\hat{c}}$ che Bob conosce e, quindi, in relazione a quanto Bob le chiede, anche il bit b_c che egli ha appreso. D'altra parte, Bob non sarebbe conscio di questa perdita. C'è, tuttavia, un'uscita molto semplice per Bob: farsi mandare comunque entrambe le sindromi da Alice, altrimenti chiude la bocca.

4.3.2 Attacchi di Bob

Dal punto di vista di Bob, invece, sono disponibili molte strategie ingannevoli per tentare di creare due buoni insiemi al passo 5, o almeno due insiemi che gli facciano apprendere qualcosa su entrambi i bit di Alice. Ci concentreremo su strategie *simmetriche*, cioè strategie ingannevoli che favoriscono entrambi gli insiemi formati da Bob.

Attacco standard

Consideriamo prima il semplice caso in cui Bob non inganna al passo 3. In tal caso, la strategia simmetrica di Bob sarebbe quella di selezionare circa $N/2$ buoni bit (e così $N/2$ cattivi bit) in ogni insieme, cioè, in altri termini, Bob conoscerebbe solo metà dei bit in ogni insieme. Tuttavia, quanto più il numero di bit di parità mandati da Alice al passo 6, per ogni insieme, è minore di $N/2$ (per bit di parità, in questo caso, si intendono quelli generati dalla sindrome), tanto meno di N bit di parità, circa ogni insieme, è la conoscenza di Bob. Applicando l'amplificazione della riservatezza si può concludere che l'informazione attesa da Bob sulle parità di entrambi i sottoinsiemi casuali scelti da Alice al passo 6 è piccola. Numericamente questo significa che tale attacco è futile se $H(2\varepsilon) < 1/2$, cioè se $\varepsilon < 5.501\%$.

Attacco Breidbart

Un ovvio modo nel quale Bob può ingannare è misurare, al passo 3, gli impulsi di Alice nella base Breidbart. In questo caso sappiamo che Bob ottiene ogni bit di Alice con probabilità, $\beta \approx 0.85$ producendo 0.399 bit d'informazione di Shannon. Analizziamo, in particolare il seguente scenario:

- assumiamo che il canale quantistico sia libero da errori (ciò rende solo Bob più potente).
- Alice manda a Bob una stringa $b = b_1, b_2, \ldots. b_N$

- Bob la riceve come $b' = b'_1, b'_2, ...b'_N$ attraverso un canale binario simmetrico il quale trasmette i bit correttamente con probabilità β (dalla misura Breidbart).
- Alice rivela la sindrome $S_b = Hb^T$ a Bob dove H è la matrice $k \times N$ di controllo di parità del codice lineare considerato (k è la lunghezza della sindrome)
- Alice prende un sottoinsieme casuale I di 1,2,......,N e lo annuncia a Bob
- Bob vuole approssimare $z = \bigoplus_{i \in I} b_i$.

E' dimostrabile che se $k \leq 3N/5$, eccetto con probabilità esponenzialmente piccola, Bob avrà un numero esponenziale di candidati ugualmente probabili da cui scegliere la stringa originale b di Alice. Quindi, l'amplificazione della riservatezza può essere applicata per concludere che la sua informazione su z è piccola. Per contro, ogni valore di k più grande di $N/2$ (che è comunque compreso nell'insieme di valori) avrebbe permesso a Bob di indovinare z con buona probabilità, se la sua informazione fosse stata ottenuta dall'uso di misure in basi canoniche (nel qual caso Bob conoscerebbe metà dei bit di b esattamente e non avrebbe nessuna informazione sull'altra metà). Questo ci permette di dedurre che, per tale protocollo,*nessuna misura può essere migliore di una misura legittima nelle basi canoniche* (questo perché anche con lunghezze più piccole delle sindromi, $N/2$ contro 3N/5, riusciamo comunque ad indovinare z con buona probabilità, per cui le misure nelle basi canoniche sono più potenti). L'idea della dimostrazione del risultato precedente è abbastanza semplice. Denotato con D il numero di errori nei dati di Bob, viene prima trovato un limite inferiore al numero delle parole a distanza di Hamming D da b'. Tra queste parole vengono poi selezionate quelle che hanno la stessa sindrome di b, poiché queste sono i soli candidati per b nella scelta di Bob. Denotato con $N_D(x, y)$ il numero di parole con sindrome y a distanza D da una fissata parola w con sindrome x, viene mostrato che $N_D(S_{b'}, S_b) \geq 2^{-r}\ \frac{\binom{N}{D}}{2^k}$ con probabilità almeno $1 - 2^{-r}$ per ogni parametro di sicurezza $r > 0$, dove $\binom{N}{D}$ è il numero di parole di Hamming a distanza D da b' e 2^k è il numero di sindromi. Infine, sfruttando la limitazione inferiore già trovata per $\binom{N}{D}$ si verifica che $N_D(S_{b'}, S_b)$ è esponenzialmente grande in N $(2^{-r} \forall r > 0$), tranne che con probabilità esponenzialmente piccola in N, se $k \leq 3N/5$. Di conseguenza, poiché vi è un numero di candidati esponenzialmente grande da cui Bob può risalire a b, si ricava che l'informazione disponibile a Bob è molto piccola, se $k \leq 3N/5$.

Divisione del raggio

Un altro modo mediante il quale Bob può ingannare, riguarda ancora il passo 3. Richiamiamo che gli impulsi mandati da Alice non sono a singoli fotoni ma contengono μ fotoni, con μ significativamente più piccolo di 1. Più precisamente ogni impulso dovrebbe contenere un numero di fotoni che segue una distribuzione di Poisson con media μ. In particolare c'è una probabilità $\xi = 1 - e^{-\mu} - \mu e^{-\mu} \approx \mu^2/2$ che un impulso sia a conteggio multiplo, cioè contenga 2 o più fotoni. In questo caso, Bob lo potrebbe separare in due fotoni misurandoli in due diverse basi canoniche (rettilinea e diagonale). Dopo aver ascoltato la corretta base da Alice al passo 4, Bob saprebbe quale misura è stata rilevante e cosìapprenderebbe i bit di Alice con certezza. Ricordiamo che con a abbiamo indicato l'efficienza del conteggio di Bob e che il numero di impulsi mandati da Alice è $M = T/a$, dove $T = 2N$ è il numero di impulsi che Bob riceve. Consideriamo, ora, il caso in cui i fotomoltiplicatori di Bob siano perfetti. Un tale Bob può ottenere i bit di Alice con certezza per l'intero insieme $M\xi = T\xi/a$

di impulsi a conteggi multipli (numero di bit che Alice manda per la probabilità che questi impulsi siano a conteggio multiplo). Assumendo che $\xi < a$, altrimenti Alice abortirebbe il protocollo al passo 1, Bob conoscerebbe circa $T\xi/a$ bit dalla divisione del raggio e circa metà dei rimanenti$(1 - \xi/a) \cdot T$ bit da un comportamento *onesto* (leggendo gli impulsi nelle basi canoniche) per un totale di γT bit dove $\gamma = 1/2 + \xi/2a$. Questa quantità è $1 + \xi/a$ volte più grande del T/2 che egli avrebbe ottenuo onestamente. In questo caso la strategia simmetrica di inganno consisterebbe nel dividere i $T = 2N$ bit in due insiemi di dimensione N, così che egli conoscerebbe una proporzione γ dei bit in ogni insieme. L'analisi, a questo punto, è simile a quella condotta per l'attacco standard tranne per il fatto che Bob conosce una più grande frazione di bit di qualsiasi insieme scelto da Alice. Quindi questo inganno sarebbe contrastato se $H(2\varepsilon) < 1 - \gamma = 1/2 - \xi/2a$. Questo completa la dimostrazione formale del principale teorema, sotto la ragionevole assunzione che Bob debba misurare ogni impulso prima che arrivi il successivo, altrimenti perde l'opportunità di misurarlo. Il protocollo risulta, in definitiva, sicuro anche contro inganni che richiedono un'illimitata potenza computazionale, perché il passo 1 assicura che $H(2\varepsilon) < 1/2 - \xi/2a$ e quindi anche minore di 1/2 (il che lo rende sicuro dall'attacco standard; per renderlo sicuro anche dall'attacco Breidbart basta prendere $k \leq 3N/5$, il che non toglie che un onesto Bob non possa apprendere b_c , in quanto valori di k più grandi di $N/2$ sono compresi in tale range).

Memorizzazione d'impulso

Invece di misurare gli impulsi al passo 3, Bob potrebbe semplicemente supporre di farlo, mentre, in effetti, memorizza tutti gli impulsi in una linea senza perdita di ritardo. Dopo che Alice ha annunciato le basi inviate al passo 4, egli potrebbe misurarli nelle basi corrette, che ora conosce, usando detector perfettamente efficienti. In definitiva, Bob riuscirebbe a costruire due buoni insiemi, apprendendo, di conseguenza, sia b_0 che b_1 . Per portare tale attacco, è chiaro che Bob debba essere capace di mantenere gli impulsi polarizzati per un tempo arbitrariamente lungo (perché Alice può sospettare che Bob stia tentando un tale attacco e, quindi, attendere prima del passo 4) e che debba avere un perfetto (o quasi) fotorilevamento per le misurazioni successive. Tuttavia, anche questo non sarebbe sufficiente. La difficoltà aggiuntiva di Bob è che egli deve dire ad Alice in anticipo, al passo 3, quali impulsi egli sostiene di aver misurato. Anche se fornissimo Bob della tecnologia necessaria per sferrare tale attacco (notiamo che attualmente non è possibile conservare fotoni per più di una piccola frazione di secondo), ci sarebbe un riparo concettualmente semplice al protocollo. Prima di tutto Alice manderebbe $3N/a$ impulsi al passo 2, permettendo a $3N$ di loro di essere con successo, se Bob è onesto. Quindi, prima del passo 4, Bob userebbe uno schema di *bit commitment* (si veda il prossimo capitolo) per impegnarsi non solo ad ognuna delle basi usate per le sue misure con successo, ma anche ai bit così ottenuti. Ancora prima del passo 4, Alice selezionerebbe un sottoinsieme casuale di N successi riportati e direbbe a Bob di aprire i suoi *impegni* per questi. Questo permette ad Alice di testare che gli impegni di Bob sono corretti (soggetti ad una percentuale di errore ε) quando la sua base impegnata è corretta, e che i suoi impegni sono non correlati ai corretti bit, quando la sua base è errata. Questo prova ad Alice che Bob non solo misura gli impulsi prima del passo 4, ma anche che egli non li misura nelle basi non canoniche (come la base Breidbart).

Misure coerenti

Abbiamo limitato Bob nel misurare gli impulsi uno alla volta e combinato i risultati classici di queste misure con le informazioni successivamente ottenute da Alice. Il formalismo della meccanica quantistica permette una più generale specie di misura, attualmente impossibile da realizzare. Tale misura tratta l'intera sequenza di M impulsi mandati al passo 2, come un singolo sistema quantistico a 2^M stati, permettendo ad esso di interagire coerentemente con un sistema quantistico intermediario di complessità confrontabile, mantenendo la fase di coerenza del sistema intermediario per un tempo arbitrariamente lungo e, quindi, finalmente, misurando il sistema intermediario in un modo dipendente dall'informazione provvista da Alice al passo 4. Alla luce di quanto detto, evitare questo attacco è semplice. Il riparo, infatti, che abbiamo mostrato per la memorizzazione d'impulsi, può essere applicato anche a tale attacco, anche perché lo schema di bit commitment che vedremo risulta sicuro contro ogni specie di attacco.

5 Bit commitment

Prima di mostrare il protocollo e di analizzare i vari attacchi, è opportuno definire in cosa consiste il bit commitment. Supponiamo che una parte, Alice, abbia un bit x in mente, con il quale vorrebbe essere impegnata nei confronti di un'altra parte, Bob. Alice desidera, attraverso una procedura *commit(x)*, assicurare Bob che ella ha in mente un dato bit e che non può cambiarlo. D'altra parte, Bob, avendo a disposizione solo questa prova, non é capace di dire quale è il valore di x. In seguito, Alice può rivelare, attraverso una procedura *unveil(x)*, il valore di x e provare a Bob che il pezzo di prova mandato prima, realmente corrisponde a quel bit. Notiamo che schemi di bit commitment classici (nei quali il pezzo di prova di Alice è infomazione classica, quale una stringa di bit) non sono sicuri contro un'illimitata potenza computazionale. Lo schema quantistico che presenteremo, invece, è fornito di una prima, completa, dimostrazione che nessun partecipante al protocollo possa imbrogliare, eccetto con probabilità arbitrariamente piccola, in accordo alle leggi della fisica quantistica. Ciò consente anche di completare la dimostrazione sulla sicurezza dell'OT quantistico presentato nella sezione precedente.

5.1 Il protocollo

Forniamo, innanzitutto, alcuni formalismi matematici che ci saranno utili nel seguito. Sia γ^p la variabile casuale che assume il valore binario 0 con probabilità p e 1 con probabilità $1-p$. Se $p = 1/2$ ometteremo l'apice 1/2. Denotiamo con $[]_i$ la funzione selezione tale che $[a_0, a_1, ..., a_n]_i = a_i$. Sia $x \otimes y$ il prodotto scalare booleano, cioè se x_i,y_i sono gli i-esimi bit di x e y, avremo:

$$x \otimes y = \bigoplus_{i=1}^{n} x_i \wedge y_i.$$

Sia, infine, ε un limite superiore alla percentuale d'errore del canale quantistico, cioè la probabilità che un fotone $|\leftrightarrow\rangle$ polarizzato venga rilevato come $|\updownarrow\rangle$. Desciviamo, inizialmente, il protocollo *commit(x)* utilizzato da Alice per impegnarsi ad un bit x nei confronti di Bob.

commit(x)

1. Bob sceglie una matrice booleana M come una matrice generatrice di un codice binario lineare (n,k,d) C, tale che $d/n > 10\varepsilon$ e $k/n = 0.52$ e la annuncia ad Alice.
2. Alice sceglie una stringa casuale a n bit $r \leftarrow (\gamma_1, \gamma_2, ..., \gamma_n)$ e la annuncia a Bob.
3. Alice sceglie una parola codice casuale a n bit $c \leftarrow (\gamma_1, \gamma_2, ..., \gamma_k) \cdot M$ da C, tale che $c \otimes r = x$.

4. Per i=1,...,n

   - Alice sceglie un bit casuale $b_i \leftarrow \gamma$ e definisce la sua base di trasmissione $(\varphi_i, {\varphi_i}^\perp) \leftarrow [+, \times]_{b_i}$ (cioè se $b_i = 0$ la base dell'i-esimo fotone mandato sarà rettilinea; se $b_i = 1$ sarà diagonale questo per la funzione di selezione).
   - Alice manda a Bob un fotone π_i con polarizzazione $[\varphi_i, {\varphi_i}^\perp]_{c_i}$ (ciò significa che, supposto $b_i = 0$, se, $c_i = 0$, allora π_i sarà rettilineo orizzontale, altrimenti se $c_i = 1$ sarà rettilineo verticale. Se, invece, $b_i = 1$, π_i , sarà diagonale a 45 gradi se $c_i = 0$ e diagonale a 135 gradi se $c_i = 1$.

5. Per i=1,...,n

   - Bob sceglie un bit casuale ${b'}_i \leftarrow \gamma$ e misura il fotone π_i nella base $(\vartheta_i, \vartheta_i^\perp) \leftarrow [+, \times]_{{b'}_i}$
   - Bob pone ${c'}_i \leftarrow \{ \begin{array}{l} 0 \quad se \quad \pi_i \quad è \quad visto \quad come \quad \vartheta_i \\ 1 \quad se \quad \pi_i \quad è \quad visto \quad come \quad \vartheta_i^\perp \end{array}$

     (se, per esempio ${b'}_i = 0$ e quindi, la base è rettilinea $\vartheta_i \equiv$ orizzontale e ${\vartheta_i}^\perp \equiv$ verticale, per cui ${c'}_i$ varrà 0 o 1 a seconda dell'esito della misura).

Siano c', b e b' i vettori $c' = ({c'}_1, {c'}_2, ..., {c'}_n)$, $b = (b_1, b_2, ..., b_n)$ e $b' = ({b'}_1, {b'}_2, ..., {b'}_n)$. Alice tiene x, c e b segreti finché (e se) le rivelazioni hanno luogo, mentre Bob tiene c' e b' segreti per sempre. Notiamo anche che il vettore casuale r è fornito a Bob in chiaro, mentre la parola codice casuale c è mandata attraverso il canale quantistico, codificandola mediante fotoni polarizzati nelle basi scelte casualmente. Poichè Bob non conosce in quali basi i fotoni sono polarizzati, egli li misura in basi scelte casualmente. Quando sceglie la base corretta (${b'}_i = b_i$), il che avviene con probabilità 1/2, egli ottiene il corretto bit (${c'}_i = c_i$), eccetto con probabilità d'errore al più ε. Dall'altro lato, quando sceglie la base errata (${b'}_i \neq b_i$), il suo bit non è correlato con il bit di Alice, tuttavia, ${c'}_i = c_i$ ugualmente con probabilità 1/2 (in quanto anche se sbaglia la base, comunque puó ottenere 0 o 1 con probabilità 1/2, per il principio di indeterminazione). Quindi, la lettura di Bob della parola c di Alice è corretta su approssimativamente il 75% dei bit (100% nel primo caso e 50% nel secondo, per cui in media 75%). Un ingannevole Bob, come sappiamo, potrebbe ottenere circa l'85% dei bit correttamente, utilizzando la base Breidbart, e dimostreremo che questo è il meglio che possa fare. Notiamo, inoltre, che il codice lineare C è scelto in maniera tale che ci sono esponenzialmente molte parole codice intorno a quella ricevuta da Bob, c', che sono alla stessa distanza di Hamming da quella trasmessa da Alice c. Ciò per evitare che Bob possa risalire più facilmente alla parola c di Alice e, quindi, ad x. Per questo motivo, la distanza minima tra parole codice non dovrebbe essere grande (perché, altrimenti, le parole codice alla stessa distanza da c sarebbero poche da trovare). Il risultato precedente è indispensabile per un corretto protocollo, perché come vedremo nel seguito (teorema 5.4), essendo r scelta casualmente, la conoscenza di r e c' danno a Bob un ammontare di attesa informazione di Shannon esponenzialmente piccola su $x = c \otimes r$. Dall'altro canto , tuttavia, la distanza minima tra parole codice deve essere sufficientemente grande da prevenire Alice nel trovare due differenti parole codice, c^0 e c^1 (insieme con basi mandate possibilmente false) in maniera tale da poter affermare di aver mandato l'una anziché l'altra, così che Bob sarebbe disposto a dare la colpa agli errori di trasmissione per la differenza tra la parola codice mandata da Alice e la sua misura c' (Teorema 5.7). Di conseguenza è necessario bilanciare queste due esigenze, nella scelta della distanza minima del codice C, per prevenire Alice e Bob dall'ingannare, da cui i misteriosi parametri 10ε e 0.52 nel protocollo *commit(x)*. A questo punto, se Alice decide di rivelare il suo impegno x, affinché Bob possa apprendere il corretto valore di x e provare che Alice aveva in mente proprio quel bit, è necessario che entrambi intraprendano il seguente protocollo: *unveil*$((c,b,x),(c',b'))$

1. Alice rivela c,b e x a Bob.

2. Bob pone

$$\delta \leftarrow \sum_{i|b'_i=b_i} \frac{c_i \oplus c'_i}{n/2}$$

3. **if** $(\delta < 1.4\varepsilon)$, $(x = c \otimes r)$ e (c è una parola codice)

   then Bob dà in output *accettato*

   else Bob dà in output *rifiutato*

In effetti, i parametri che Alice rivela al passo 1 potrebbero anche non essere quelli reali. Tuttavia vedremo che la sicurezza del protocollo è garantita dal valore 1.4 ε.

5.2 Analisi dell'informazione di Bob circa x

Esaminiamo adesso un possibile inganno da parte di Bob. Osserviamo che tutta l'informazione disponibile a Bob circa x gli è data attraverso la trasmissione quantistica di c nel passo 4. Vedremo che anche se Bob effettuasse la misura ottima (in base Breidbart), essendovi molti vettori alla stessa distanza da c, otterrebbe un'informazione esponenzialmente piccola su c. Dimostriamo, innanzitutto, che la base Breidbart costituisce la migliore misura che Bob possa effettuare. Vale a tal proposito il seguente teorema:

Teorema 5.1 *La misura quantistica che massimizza (ingannando) l'informazione di Bob circa x è la misura di ogni fotone π_i nella base $(\vartheta_i, \vartheta_i^{\perp}) = (B, B^{\perp})$.*

L'idea della dimostrazione è molto semplice. Consideriamo un nuovo protocollo $commit'(x)$ che ha come variante, rispetto a *commit(x)* il passo 4:

$4'$ Per i=1,...,n

- Alice sceglie un bit casuale $b_i \leftarrow \gamma^{k^2} = \gamma^{0.85}$
- Alice manda a Bob un fotone π_i con polarizzazione $[|B\rangle, |\, B^{\perp}\rangle]_{c_i \oplus b_i}$.

Ciò che si verifica è che le matrici densità (che, ricordiamo, descrivono la mistura quantistica di stati mandati a Bob) utilizzate per rappresentare uno 0 o un 1 nei passi 4 e 4', coincidono sia per *commit(x)* che per $commit'(x)$. Sfruttando il teorema della fisica quantistica , affermante che *misture con identiche matrici densità non possono essere distinte da ogni misura quantistica*, si deduce che Bob è capace di ottenere la stessa informazione su c (e così su x), sia in *commit(x)* che in $commit'(x)$. Quindi, in altre parole, *commit(x)* e $commit'(x)$ sono equivalenti, e poiché $(|B\rangle, |B^{\perp}\rangle)$ è una base ottima per $commit'(x)$ (in quanto tutti i fotoni mandati in esso sono polarizzati in tale base e, quindi, tutti i bit possono essere ottenuti con certezza a meno di errori dovuti a cause naturali) allora $(|B\rangle, |B^{\perp}\rangle)$ è anche ottima per *commit(x)*. Ciò significa, in particolare, anche ogni più generale misura congiunta su tutti i fotoni insieme (misura coerente) non sarà di nessun vantaggio (ciò completa la dimostrazione sulla sicurezza dell'OT). Malgrado un onesto Bob non effettui la misura ottima, dimostreremo che, anche se lo facesse, otterrebbe poca informazione circa x. Premettiamo, a tal proposito, il seguente lemma:

Lemma 5.2 *Anche se Bob, ingannando, effuttuasse la misura ottima, esiste una costante positiva* $\alpha < 1$ *tale che egli termina con un vettore* c' *a distanza minore di* γn *da* c*, con probabilità al più* α^n *(dove* $\gamma = H^{-1}(1/2) \approx 0.1100279$*, vale a dire il valore di probabilità per cui si ottiene* $H(\gamma) = 1/2$*).*

Teorema 5.3 *Anche se Bob conosce l'esatta distanza di Hamming* $d \leftarrow d_H(c, c')$*, avrebbe molta poca informazione quando* $d > \gamma n$*.*

Usando il fatto che $d > \gamma n$, si perviene alla conclusione che il numero di parole codice a distanza d da c', costituenti l'insieme E, è almeno $\frac{2^{k-n/2-\alpha n}}{\sqrt{n}}$ che è esponenzialmente grande se $k/n > 1/2$, ciò tranne che con probabilità $2^{-\alpha n}$, per ogni $\alpha > 0$ (nell'OT, il fatto che $k > n/2$ ci era stato utile per dimostrare che , per quel protocollo, la misura nella base canonica fosse la migliore possibile). Sfruttando, infine, il seguente lemma:

Lemma 5.4 *Se Bob ha ridotto il valore di c all'insieme E di candidati ugualmente probabili, e se un insieme casuale dei bit di c è scelto, l'atteso ammontare della informazione di Shannon disponibile a Bob circa la parità dei bit in questo sottoinsieme (che in effetti sarebbe x) è minore di* $2/|E| \ln 2$ *bit*

possiamo dedurre che, nel nostro caso, il numero di bit d'informazione che Bob ottiene su x dopo aver osservato c' è meno di $\frac{2\sqrt{n}}{2^{k-n/2-\alpha n} \cdot \ln 2}$, che è esponenzialmente piccolo come $k > n/2 + \alpha n$. In definitiva, se $d/n > \gamma \approx 0.1100279$ ed assumendo il canale senza rumore, cioè con $\varepsilon \leq 1\%$, il che significa che $d/n > 10\varepsilon$, prendendo $\alpha = 0.1$ troviamo che il numero di bit d'informazione è al più $2^{-0.1n}\sqrt{n}/\ln 2$ (quindi molto pochi per n sufficientemente grande), ogni volta che $k/n > 0.51$, anche se Bob conosce l'esatto numero di errori d.

5.3 Note addizionali

Nel protocollo per l'OT viene dimostrato che nessuna misura risulta migliore di quella effettuata nelle basi canoniche. Riguardo al bit commitment, abbiamo, invece, visto che la misura ottima è quella effettuata in base Breidbart. Di conseguenza questi due risultati sembrerebbero essere in antitesi tra loro. Tuttavia, vi sono delle differenze di fondo nei due protocolli che avvalorano il perché valga tale risultato. Nell'OT è necessario un protocollo riconciliativo per poter far sì che la versione mandata e quella ricevuta, almeno per quanto concerne il buon insieme, coincidano. Per cui l'informazione di Bob deve essere per quanto più è possibile affidabile e, quindi, deterministica e non probabilistica, come si otterrebbe utilizzando la base Breidbart. Nello schema di bit commitment, invece, non occorre effettuare alcuna riconciliazione, ma basta indovinare, quanto più è possibile, la parola codice c mandata da Alice. Per questo motivo, in questo caso, l'informazione probabilistica è accettabile e viene dimostrato anche essere la migliore che si possa ottenere.

Riferimenti

[1] C. Bennett, F. Bessette, G. Brassard, L. Salvail e J. Smolin, *Experimental quantum cryptography, Journal of Cryptology* , vol. 5, n.1, pag. 3-28, 1992.

[2] C. Bennett, G. Brassard, C. Crepeau e M. H. Skubiszewska, *Pratical oblivious transfer* in Proceedings of Crypto '91, Lecture Notes in Computer Science, vol. 576, pag. 351-366, 1992.

[3] C. Bennett, G. Brassard e A. Ekert, *Crittografia quantistica*, in Le Scienze, n. 292, pag. 84-93, dicembre 1992.

[4] A. Ekert *Quantum cryptography based on Bell's theorem, Physical Review Letters*, vol. 67, n. 6, 5 agosto 1991.

[5] C. Bennett, G. Brassard e M. David, *Quantum cryptography without Bell's theorem, Physical Review Letters*, 68, n. 5, 3 febbraio 1992.

[6] G. Brassard, C. Crepeau, R. Jozsa e D. Langlois, *A quantum bit commitment scheme provably unbreakable by both parties* In 34th Symp. on Found. of Computer Sci. , pag. 42-52. IEEE, 1993.