Crittografia Quantistica

Dario Sangiovanni, Luca Del Basso, Enrico Gasperoni

9 giugno 2005

Parte prima

a cura di Dario Sangiovanni

1 Il limite della crittografia classica

Lo scopo della crittografia è quello di proteggere l'informazione da eventuali attacchi e la crittografia classica punta al raggiungimento di tale scopo tramite algoritmi matematici con alta complessità crittoanalitica come ad esempio un problema NP Completo. Per risolvere un tale problema è necessario fare moltissimi calcoli quindi è evidente che il raggiungimento della soluzione del problema è legato a due fattori tra loro complementari, il tempo e la potenza di calcolo del crittoanalista.Il punto di forza del livello di sicurezza degli algoritmi attuali si basa proprio su questi due fattori.

Facciamo l'esempio di DES e 3DES. Nel luglio del 1998 è stata progettata una macchina multiprocessore in grado di rompere l'algoritmo DES in 5 giorni,un tempo accettabile e innocuo per alcuni sistemi per i quali l'occultamento dell'informazione è utile per un tempo limitato, ma inaccettabile per altri e per questo appunto sono nate delle varianti di DES. 3DES è teoricamente rompibile anch'esso ma ha un costo temporale di gran lunga maggiore quindi è ancora un ottimo algoritmo di cifratura.

Le considerazione fatte finora hanno un senso se presupponiamo che il fattore computazionale[1] sia costante o che comunque possa variare in un intorno abbastanza ristretto ed è logico presupporlo tale alla luce delle attuali possibilità tecnologiche. Ma, teoricamente, se disponessimo di potenza di calcolo illimitata romperemmo qualsiasi algoritmo di cifratura in un tempo irrisorio confrontato a quello delle stime attuali.

Nel 1982 un fisico americano, Richard Feynman, pensò di sfruttare un particolare fenomeno della fisica quantistica per creare una macchina in grado di effettuare calcoli in parallelo invece che in serie, come gli attuali computer, e quindi in grado teoricamente di trasformare un problema N-P completo in un problema di complessità P. Questa macchina venne chiamata appunto computer quantistico.[2]

Ora è chiaro che una macchina con una tale potenza, se fosse realizzata, sarebbe in grado di elidere la sicurezza di qualsiasi informazione protetta dagli attuali algoritmi di cifratura; diventa necessario quindi trovare una nuova tecnica per proteggere l'informazione e sopratutto per fronteggiare una tale tecnologia.

[1] per fattore computazionale si intende la quantità di tempo e la capacità di calcolo

[2] il computer quantistico verrà trattato in dettaglio nella parte terza

2 La nascita della crittografia quantistica

Per ovviare il problema venutosi a creare con l'avvento del computer quantistico si cercò di trovare una soluzione che sfruttasse la natura stessa della comunicazione e si ipotizzò un approccio fisico più che matematico. La soluzione fu trovata nella stessa meccanica quantistica causa principale del problema.

Uno degli aspetti principali della crittografia è il canale di comunicazione.[3] Sul canale classico è possibile che si inserisca un nemico tra mittente e destinatario del messaggio e che intercetti tutto il contenuto del messaggio crittato senza che nessuna delle due parti si accorga della sua presenza. Naturalmente questo aspetto prima non rappresentava un pericolo perchè comunque il nemico doveva decrittare il messaggio intercettato dal canale in un tempo utile ai suoi scopi, ma adesso bisognava impedire qualsiasi tipo di intercettazione.

Viene realizzato allo scopo un canale di comunicazione quantistico sul quale non è possibile effettuare un'osservazione senza essere scoperti. La realizzazione di tale canale fu guidata da uno dei principi fondamentali della meccanica quantistica chiamato ***Principio Di Indeterminzione di Heisenberg***,[4]. Nel 1927 il fisico tedesco Werner Heisenberg scoprì che la natura probabilistica delle leggi della meccanica quantistica poneva grossi limiti al nostro grado di conoscenza di un sistema atomico.

Normalmente ci si aspetta che lo stato di una microparticella in movimento[5] sia caratterizzato completamente ricorrendo a due parametri : velocità e posizione. Heisenberg postulò invece, che a un certo livello queste quantità sarebbero dovute rimanere sempre indefinite. Tale limitazione prese il nome di Principio di Indeterminazione. Questo principio afferma che *maggiore è l'accuratezza nel determinare la posizione di un particella, minore è la precisione con la quale si può accertarne la velocità e viceversa.*[6] Da questo principio si evince anche che non è possibile misurare contemporaneamente velocità e posizione di una microparticella senza modificare irrimediabilmente lo stato in cui essa si trova.

Ora pensiamo al canale quantistico.Se attraverso questo canale passassero microparticelle e un potenziale nemico cercasse di intercettarle dovrebbe compiere un'osservazione e quindi modificherebbe lo stato della comunicazione facendosi scoprire.[7]

[3] il mezzo tramite il quale l'informazione crittata viene scambiata

[4] Heisenberg, Werner (Würzburg 1901 - Monaco 1976)fisico tedesco. Fu uno dei più grandi fisici teorici e fornì il suo contributo più rilevante alla teoria della struttura atomica

[5] consideriamo ad esempio un elettrone in rotazione attorno al nucleo

[6] Occorre sottolineare però che le limitazioni in parola, non derivano solo dall'invasiva interazione del mondo macroscopico sul mondo microscopico, ma sono proprietà intrinseche (ontologiche) della materia. In nessun senso si può ritenere che una microparticella possieda in un dato istante una posizione e una velocità

[7] questo concetto verrà chiarito nella seconda parte con la spiegazione del protocollo di

Ora ragioniamo sulla comunicazione; affinchè questa mantenga i punti di forza trattati è necessario comunicare tramite microparticelle così da sfruttare il Principio Di Heisenberg. La microparticella che viene utilizzata è il **fotone**.

3 La natura fisica del fotone

Tutto cominciò con la scoperta di uno studente di fisica di nome Max Planck, il quale scoprì nel 1900 che le radiazioni emesse da un corpo caldo non sono emesse in modo continuo ma in pacchetti, ovvero in **quanti**. Fino a Planck si credeva che le radiazioni fossero un fenomeno costante e frazionabile a piacere, come una normale grandezza numerica, dopo Planck si dovette tener conto che l'energia[8] non viene emessa costantemente ma quantizzata in pacchetti.

In sostanza l'energia non è solamente un onda che si propaga in modo continuo e in tutte le direzioni (emanazione continua), l'energia viene emanata a proiettili, ovvero in quanti predefiniti dello stesso valore (emanazione discreta).Per usare un altro esempio, il quanto assomiglia al vagone di un treno, dove il treno rappresenta la quantità di energia complessiva e ciascun vagone il quanto costante in cui è suddivisa e sotto la cui grandezza non può essere ulteriormente considerabile.La costante di Planck esprime il valore fisso e non frazionabile in cui l'energia di una radiazione è divisa. L'onda della radiazione si esprime in frequenza, maggiore è la frequenza[9] maggiore è l'energia racchiusa in un quanto.

L'energia, in sostanza, cambia in quantità, ma per essere emessa viene racchiusa sempre nel medesimo quanto, della stessa dimensione.[10]

Una prima conseguenza della formulazione della teoria dei quanti fu la scoperta che la luce, oltre a comportarsi come onda , e quindi essere soggetta a fenomeni di sovrapposizione e rifrazione,[11] si comporta anche come particella.

Ora come abbiamo visto l'energia di un quanto dipende dalla frequenza dell'onda dalla quale viene generato e visto che la luce è una parte dello spettro di tutte le onde elettromagnetiche[12] il quanto che essa trasporta avrà un energia limitata. Tale quanto prende il nome di fotone.

C'è inoltre un altro aspetto da sottolineare: la luce è un onda elettromagnetica e sappiamo dalle leggi di Maxwell che è composta da una componente elettrica e una magnetica in fase e perpendicolari fra loro. Queste

trasmissione

[8] la radiazione

[9] più corta è la lunghezza dell'onda

[10] relativamente all'esempio precedente, non importa quante persone vi siano in un vagone, il vagone resterà sempre della stessa lunghezza

[11] come le onde del mare

[12] spettro di Plank

componenti hanno direzioni casuali nella luce naturale che viene chiamata per questo luce **non polarizzata**.

4 Rappresentazione del bit

Arrivati a questo punto sappiamo che un canale quantistico[13] può dirsi tale se attraverso esso viaggiano microparticelle, in particolare nel nostro caso fotoni. Nasce ora però un altro problema,come rappresentiamo un bit?

Sappiamo che i fotoni hanno polarizzazione casuale, ma se potessimo decidere noi che polarizzazione deve avere un determinato fotone potremmo anche decidere una determinata rappresentazione del bit.[14] Naturalmente possiamo farlo e lo decidiamo usando un **filtro Polaroid**.

Un filtro Polaroid non fa altro che ripolarizzare un certo numero di fotoni secondo il proprio asse. Ad esempio ammettiamo di posizionare l'asse del filtro in verticale e di puntargli contro una torcia,la luce che attraversa il filtro[15] sarà composta soltanto da fotoni con polarizzazione verticale.[16]

Il numero di fotoni che attraversano un filtro Polaroid non è casuale ma determito da una legge probabilistica detta *Legge di Malus*

$$I = I_0 cos^2 \alpha$$

La legge dice che l'intensità di un fascio di luce che attraversa un Polaroid è uguale all'intensità massima del fascio di luce per il coseno al quadrato dell'angolo tra l'asse del filtro e l'asse di polarizzazione del fascio. Ad esempio se un fotone arriva con polarizzazione sfasata di 90 gradi sicuramente non passerà il filtro mentre se fosse sfasato di 45 gradi avrebbe il 50% di possibilità di passare il filtro o di non passarlo

Bene ora che sappiamo come caratterizzare in modo univoco un fotone è necessario anche studiare le proprietà di ricezione di un fotone da parte di un particolare oggetto, il **cristallo di calcite**.

Il cristallo di calcite ha la proprietà di distinguere in modo univoco due fotoni con polarizzazioni sfasate di 90 gradi fra loro alla condizione che una delle due sia parallela all'asse del cristallo stesso. Ad esempio un cristallo di calcite posizionato a 0 gradi sarà in grado di distingure al 100% solo fotoni polarizzati a 0 e 90 gradi e non a 45 gradi per esempio. Se volessimo distingere quello a 45 gradi dovremmo appunto ruotare il cristallo di 45 gradi.

[13] nel nostro caso si intende in particolare la fibra ottica come canale quantistico

[14] questo aspetto sarà più chiaro nella prossima parte

[15] detta **luce polarizzata**

[16] in particolare solo quei fotoni la cui componente del campo elettrico è parallela all'asse del filtro

Parte seconda

a cura di Luca Del Basso

5 Il Quantum Key Distribution

Come possiamo sfruttare i principi della meccanica quantistica in ambito crittografico? Il principio di indeterminazione di Heisenberg afferma sostanzialmente che non è possibile effettuare un processo di misurazione senza perturbare il fenomeno in questione. Tramite questo principio possiamo costruire un canale quantistico di comunicazione ed essere sicuri, almeno in teoria, che nessuno sia in grado di intercettare la comunicazione senza essere scoperto? Come possiamo costruire un canale quantistico? Come codifichiamo le informazioni su questo canale? Come possiamo rilevare la presenza di un eventuale intruso sulla linea di comunicazione?

Per rispondere a queste domande bisogna venire a conoscenza del primo e principale protocollo della Crittografia Quantistica o meglio detto Quantum Key Distribution (QKD), il protocollo **BB84**. BB84 fu ideato da Bennet e Brassard nel 1984 e consente lo scambio di una chiave, detta *sifted key*, in maniera sicura tra due utenti, da utilizzare poi per cifrare le comunicazioni. Lo scopo di una distribuzione quantistica a chiave pubblica è di utilizzare un canale quantistico per fare in modo che due interlocutori, saranno in grado di scambiarsi su un canale non protetto una chiave casuale di lunghezza arbitraria in completa sicurezza, con la certezza che ogni tentativo di intercettazione verrebbe rilevato inequivocabilmente. La crittografia quantistica, a differenza di quella classica, basa la sua sicurezza sulle leggi della fisica piuttosto che su congetture sulla difficoltà di certe operazioni matematiche.

6 Il protocollo BB84

Entriamo nel dettaglio descrivendo il protocollo ormai noto come BB84. Due interlocutori Alice e Bob, dispongono di due canali di comunicazione: uno quantistico ed uno convenzionale, e che siano possibili intercettazioni passive su questi canali da parte di un origliatore che chiameremo Eve. Le informazioni che Alice scambia con Bob sul canale quantistico sono singoli fotoni ad una determinata polarizzazione: Ogni bit 0,1 puo essere trasmesso sul canale quantistico in forma di fotoni oppurtunatamente polarizzati. Assumiamo che i fotoni vengano polarizzati in 4 forme diverse a 0-90 gradi[17] o 45-135 gradi,[18] in modo tale che ogni fotone contenga un bit di informazione, La polarizzazione del fotone trasmesso sarà determinata dal valore del bit da rappresentare (0,1) e dalla base di conversione utilizzata (vedi fig.1).

[17] orizzontale e verticale

[18] diagonale, anti-diagonale

R	D	Bit
↔	↗	0
↕	↘	1

Figura 1: Rappresentazione dei bit con base rettilinea e base diagonale

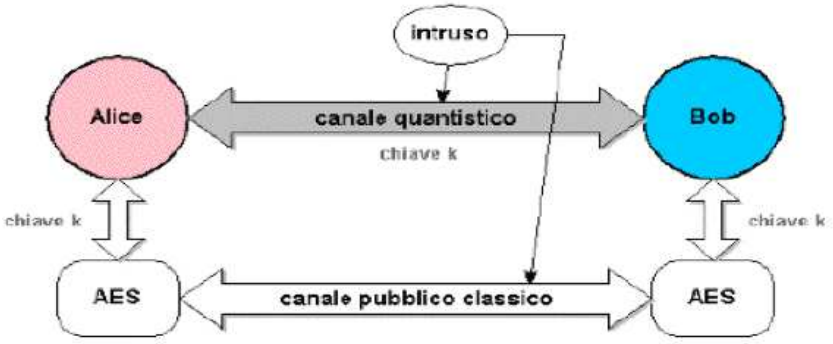

Figura 2: Schema della comunicazione tra Alice e Bob

Queste polarizzazioni (vettori) sono suddivise in due basi, **Rettilinea** + e **Diagonale** x, non ortogonali tra loro: ciò significa che, per il Principio di Indeterminazione, non è possibile misurare contemporaneamente se la polarizzazione è diagonale o rettilinea, perchè nel momento in cui misuri il fotone in una base, lo modifichi in modo permanente.

Quindi un utente che voglia trasmettere il bit 1, sceglie una base per rappresentare quel bit e manda sul canale quantistico il fotone rappresentante quel bit, ossia un fotone di polarizzazione verticale.[19]

Vediamo ora i singoli passaggi per realizzare una comunicazione segreta. Come è stato anticipato utilizziamo il canale quantistico per lo scambio di una chiave segreta k (di bit casuali). Questa chiave k, se non intercettata, verrà utilizzata come chiave di un sistema di cifratura con algoritmo simmetrico (ad esempio AES) per lo scambio dei dati cifrati su di un normale canale pubblico di comunicazione (ad esempio Internet).

Alice e Bob sono collegati tra loro tramite una fibra ottica. Alice ha a disposizione un dispositivo di emissione di fotoni polarizzati (nelle 4 polarizzazioni sopra citate) e Bob ha a disposizione un dispositivo per rilevare i fotoni emessi da Alice.

1. Alice sceglie casualmente, con una probabilità del 50%, n basi di polarizzazione x e +, e successivamente genera, sempre casualmente, n

[19] Ovviamente il bit 1 poteva essere rappresentato anche da un fotone polarizzato a 135 gradi con base diagonale

fotoni codificati in 0 o 1 nelle basi corrispondenti. Invia questi fotoni a Bob

2. Per ogni fotone ricevuto, Bob sceglie casualmente[20] una delle due basi di polarizzazione x o + e misura la polarizzazione del fotone[21] e intrepreta ogni risultato come 0 o 1 a seconda dell'esito della corrispondente misura.

   Se le basi scelte per identificare il singolo bit di informazione sono le stesse, l'identificazione avverrà correttamente, mentre se è sbagliata Bob otterrà comunque un valore nella base scelta[22] perdendo però le informazioni del fotone originario.

   Cerchiamo di spiegare meglio quest'ultimo punto. Prendiamo per esempio un rivelatore di polarizzazione; Bob decide di controllare la polarizzazione di fotoni che vengono creati da Alice. L'utilizzo di un filtro a base rettilinea + consente di avere due possibilità: il fotone viene rilevato con polarizzazione verticale, oppure il fotone è rilevato con polarizzazione orizzontale in modo certo. Se la particella che Bob sta analizzando era stata spedita utilizzando proprio la base + la misura che ha effettuato è corretta e rispecchia le informazioni di Alice, ma se invece era stato spedito con base diagonale x il fotone supererà comunque il filtro rettilineao +, ma avrà una polarizzazione casuale e che non ha nulla a che vedere con quella con cui era stato spedito

3. Raggiunto un numero adeguato di questi scambi, Alice smette di spedire fotoni. Come abbiamo già detto 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[23] supponendo che non vi siano state alterazioni dovute ad origliamento. Bob, allora, annuncia pubblicamente sul canale convenzionale la lista delle basi da lui utilizzate per misurare i fotoni, ma non cosa ha misurato.

4. Alice comunica pubblicamente a Bob, se per ogni fotone che egli ha ricevuto ha eseguito il tipo giusto di misurazione, ma non cosa ha spedito. Con queste informazioni tutti e due possono determinare i bit che sono stati inviati correttamente, confrontando le basi identiche, cosicchè le altre possono essere scartate per mantenere le polarizzazioni per le quali hanno utllizzato la stessa base. Se, mediamente, si ottiene il 50% dei bit corrispondenti vorrà dire che nessun intruso ha

[20] e indipendentemente dalle scelte fatte da Alice perchè queste scelte non sono note a Bob a questo punto del protocollo

[21] in questo modo Bob ha una probabilità del 50% di indovinare la codifica binaria di Alice

[22] se è quella rettilinea, otterrà un fotone con polarizzazione o verticale od orizzontale

[23] quelli per i quali ha indovinato la corretta base di polarizzazione

intercettato il messsaggio e quindi questi bit possono essere utilizzati come chiave segreta (k). Se la percentuale d'errore è diversa, tipicamente con un incremento del 25% d'errore, la trasmissione della chiave dovrà essere rieseguita tornando al punto 1. Ciò può capitare quando un origliatore li ha intercettati e non ne ha rimandato altri, o perchè sono stati persi durante il transito, o, infine perchè non sono stati deviati correttamente verso i fotomoltiplicatori che, di conseguenza, non li hanno rilevati. Infatti osserviamo anche che, i fotomoltiplicatori non hanno una efficienza quantistica del 100%

5. Alice e Bob, per verificare se le loro risultanti stringhe di bit sono identiche confrontano pubblicamente un sottoinsieme casuale di 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 una chiave identica da entrambe le parti e sicuramente segreta, e che quindi potrà essere utilizzata per cifrare i messaggi

Se Eve ha in qualche modo intercettato i fotoni nel loro tragitto tra Alice e Bob, grazie alle leggi della Meccanica Quantistica ed alla particolare preparazione delle quattro polarizzazioni e delle due misure possibili, li ha per forza modificati. Infatti come abbiamo detto, le fotocopiatrici perfette non esistono in Meccanica Quantistica. Se Eve ha intercettato e modificato dei fotoni, le misure di Bob avranno degli errori rispetto alle polarizzazioni inviate da Alice. Quindi, in teoria, se la sifted key di Bob è diversa da quella di Alice, vuol dire che Eve ha intercettato i fotoni e che la chiave non è sicura poichè Eve è a conoscenza di almeno parte di essa.

7 Correzione degli errori

È interessante notare come la probabilità che le risultanti stringhe di Alice e Bob concordino completamente non puo 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, oppure fotoni persi o che non sono stati rilevati correttamente. Questi sono i cosiddetti errori sperimentali e sono sempre presenti. Sembrerebbe quindi che siamo giunti ad un punto morto: vi sono sempre errori, ma se ci sono errori vuol dire che Eve ha intercettato la chiave poichè è molto difficile distinguere con sicurezza tra errori sperimentali ed errori dovuti ad Eve.

La soluzione a questo apparente insolubile problema, è in realtà relativamente semplice. Prima di tutto si assume che tutti gli errori siano sempre dovuti a Eve. Poi Alice e Bob debbono applicare alla sifted key due ulteriori fasi del protocollo.

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	OI
4b.			1		1			0				1		0	1
5a.					1									0	
5b.					OK									OK	
5c.			1					0				1			1

Figura 3: Esempio di trasmissione

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

La prima si chiama "Reconciliation" o "Error Correction" e permette ad Alice e Bob di eliminare tutti gli errori nella sifted key di Bob ed al contempo stimare la percentuale di errori trovati. Se questa percentuale è inferiore all'11%, allora si può passare alla fase seguente detta "Privacy Amplification". In questa fase la chiave segreta viene modificata secondo una procedura tale che l'informazione che nel caso Eve ha sulla chiave segreta viene ridotta praticamente a zero.

Questo è possibile perchè se Eve ha introdotto errori solo per al più l'11%, vuol dire che la sua conoscenza della sifted key è sufficientemente ridotta, conosce pochi bit della chiave, e quindi modificando appropriatamente la chiave segreta Alice e Bob possono eliminare i bit a conoscenza di Eve. Queste ultime due fasi possono essere realizzate anche pubblicamente poichè le informazioni scambiate tra Alice e Bob non aiutano Eve a fare lo stesso. Bisogna inoltre notare che in queste due fasi la lunghezza della chiave viene ridotta. A seconda delle procedure utilizzate la chiave segreta finale può anche essere lunga solo 1/8 del numero di fotoni inizialmente inviato da Alice. Una volta in possesso della chiave segreta, e con la garanzia data dalla meccanica quantistica che Eve non ne è a conoscenza, Alice e Bob la possono usare per cifrare un messaggio e scambiarselo. Il motivo per cui la Crittografia Quantistica così formulata non puo' essere usata per scambiarsi direttamente messaggi è che la presenza di Eve viene rilevata solo DOPO aver concluso l'invio dei fotoni, nella fase della Error Correction.

8 L'alternativa

La Crittografia Quantistica è quindi un'alternativa all'uso dei protocolli a Chiave Pubblica, quali ad esempio RSA, per generare e scambiare le chiavi segrete. La differenza principale tra i protocolli a Chiave Pubblica e la Crittografia Quantistica è che quest'ultima non teme attacchi basati sulla potenza di calcolo degli elaboratori o sugli sviluppi di tecniche matematiche che permettono già oggi di rompere sistemi a Chiave Pubblica che adottano chiavi pubbliche/private troppo corte.

Infine, oltre al BB84 altri protocolli sono stati proposti ed implementati, ma in ogni caso le leggi fisiche su cui si basano sono le stesse e le loro logiche sono molto simili a quella del BB84 anche se vengono sfruttate differenti proprietà dei fotoni e/o procedure leggermente diverse.

Parte terza

a cura di Enrico Gasperoni

9 Supporto alla crittoanalisi

L'introduzione della meccanica quantistica nella crittografia è volta principalmente ad identificare un metodo infallibile per trasferire informazioni in modo sicuro, ovvero per fornire al crittologo uno strumento tramite il quale, con opportuni protocolli di comunicazione, si renda fisicamente *impossibile* (e non solo *molto difficle* come accade nella crittografia classica) intercettare e decifrare la comunicazione; le leggi della quantistica, però, forniscono anche nuovi e preziosi strumenti al crittoanalista.

Com'è noto, la sicurezza degli algoritmi di crittografia classica è legata all'elevata complessità computazionale richiesta dagli attacchi crittoanalitici, anche dai più efficienti. Ciò significa che la sicurezza di tali algoritmi è legata al fatto che, nel caso peggiore, il tempo richiesto al crittoanalista per decifrare il messaggio, con l'attuale potenza di calcolo, risulta proibitivo. Quanto appena asserito ha due importanti sfaccettature:

- la sicurezza dell'algoritmo è inversamente proporzionale alla potenza di calcolo disponibile;
- esiste la possibilità, seppur non molto probabile, che l'algoritmo di crittoanalisi riesca qualche volta a decifrare il messaggio in tempo sensibilmente più basso da quello richiesto nel caso peggiore[24].

Il primo dei due punti sopra elencati, è preso in seria considerazione nell'analisi del livello di sicurezza di un algoritmo e si basa in buona parte su stime del progresso nella tecnologia di miniaturizzazione del silicio, la quale consente la produzione di calcolatori sempre più sofisticati e potenti. Un esempio di queste speculazioni è accessibile nell'analisi dell'algoritmo *serpent*, il quale, quando fu presentato nel concorso indetto dal NIST,[25] risultò essere il più robusto poichè, in base alle stime fatte, avrebbe potuto resistere a circa cinquant'anni di evoluzione della tecnologia del silicio.

Queste stime però si basano sull'ipotesi che i calcolatori futuri, per quanto più potenti di quelli attuali, seguano la stessa logica di questi ultimi. Tale ipotesi è considerata credibile poichè fin'ora, nella relativamente breve storia del computer, non è mai stata contraddetta. Gli attuali calcolatori, infatti, seppur enormemente piú potenti di quelli di cinquant'anni fa, hanno esattamente la stessa logica di calcolo dei loro progenitori, basata su flussi di bit.

[24] Tuttavia, anche il caso medio non è molto incoraggiante, per cui l'elevata complessità è, nella maggior parte dei casi, un deterrente molto efficace.

[25] Il *National Institute of Standard and Technology* (NIST), indisse nella fine degli anni novanta un concorso volto ad identificare un algoritmo che succedesse all'ormai vecchio e non più perfettamente sicuro algoritmo DES. Tale concorso sancì la vittoria dell'algoritmo AES, che risultò il miglior compromesso tra robustezza ed onere computazionale.

L'avvento della quantistica ha aperto nuovi orizzonti nella teoria della logica di calcolo, portando alla progettazione del cosiddetto *computer quantistico*. Tale calcolatore funziona in modo radicalmente diverso da quello tradizionale, consentendo il calcolo in parallelo di una stessa operazione su un insime potenzialmente infinito di dati in ingresso, e ciò gli conferisce una potenza di calcolo enormemente superiore a quella di un calcolatore classico.

Sulla scia dell'entusiasmo generato dalla possibilità di effettuare un numero infinito di calcoli contemporaneamente, si trovano molto spesso fonti che parlano del computer quantistico come di un calcolatore quasi onnipotente, in grado di portare a completamento qualsiasi tipo di algoritmo in un batter d'occhio. Ciò, ovviamente, è tutt'altro che vero.

Riuscire a quantificare il vantaggio introdotto da questo nuovo strumento, è fondamentale per comprendere come questo possa essere sfruttato al meglio dal crittoanalista.

9.1 Potere computazionale del computer quantistico

È noto, dalla teoria della Turing-calcolabilità,[26] che i problemi affrontabili sono divisi in *classi*, in base alla loro complessità, ovvero alla complessità dell algoritmo più efficiente che sia noto risolvere il problema dato. Nonostante esistano diverse classi di complessità, quelle solitamente di maggiore interesse sono le classi P ed NP, che racchiudono rispettivamente i problemi risolvibili in *tempo polinomiale (deterministico)* e quelli risolvibili in *tempo polinomiale non deterministico*. La nozione di determinismo e non determinismo è usata in questo contesto nella sua accezione più generale, che è andata col tempo scemando a causa dell'utilizzo di tali termini in contesti particolari. Normalmente, infatti, ad essi si associa l'idea di "evento certo" e di probabilità, ma tale associazione è solo un particolare punto di vista, legato al senso comune ed alimentato dalla fisica classica.

Nella teoria della calcolabilità, il concetto di *non determinismo* indica l'accadimento *contemporaneo* di più conseguenze scaturite dallo stesso evento; il concetto di *determinismo*, invece, indica l'accadimento di una ed una sola conseguenza in risposta all'evento iniziale. Una computazione deterministica, di fronte ad una situazione in cui possono essere prese diverse strade, ne segue prima una, poi eventualmente le altre, impiegando un tempo pari alla somma dei tempi richiesti dalle singole strade. Una computazione non deterministica, invece, ad ogni possibile scelta segue tutte le strade, portandole avanti in parallelo ed impiegando così un tempo pari a quello richiesto dalla strada più lunga.

Si può pensare quindi ad una computazione deterministica come una

[26] Tale teoria è stata introdotta dal matematico inglese Alan Turing, personaggio che ha molto influenzato il mondo dei calcolatori, e che ne ha sfruttato appieno le potenzialità nel suo importante incarico di crittoanalista di spicco nel team di matematici alleati impegnati nella decrittazione delle trasmissioni tedesche nella seconda guerra mondiale.

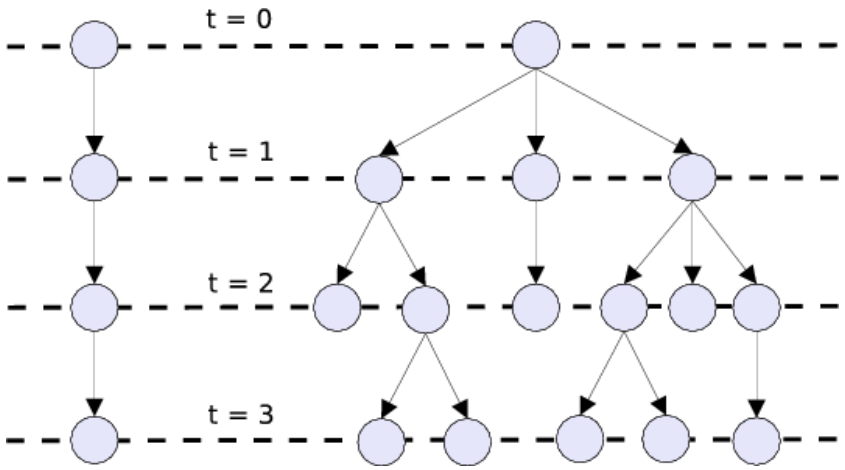

Figura 4: Esempio di computazione deterministica (sinistra) e di computazione non deterministica (destra).

sequenza di operazioni in fila, ognuna con un solo predecessore e con un solo successore. Una computazione non deterministica, invece, è rappresentabile come un albero, il quale, avendo nella radice la prima operazione, ramifica ogni qual volta si presenti una situazione che si presta ad avere diverse possibili conseguenze (vedi fig 4).

Abbreviando la terminologia, si parla di tempo deterministico riferendosi allo scorrere del tempo per una macchina a funzionamento deterministico, mentre si parla di tempo non deterministico per fare riferimento a ciò che accade in una macchina non deterministica. È bene notare che il tempo non deterministico è legato al numero di livelli dell'albero, e non al numero dei suoi nodi, che è in generale esponenziale rispetto ad essi. Ad esempio, un albero binario completo a tre livelli ha sette nodi, e corrisponde ad una computazione che, in tre istanti di tempo, ha eseguito sette operazioni. Allo stesso modo, il tempo deterministico può essere visto come il caso particolare di un albero i cui nodi abbiano al massimo un figlio. Da ciò risulta chiaro che i problemi P sono un sottoinsieme dei problemi NP, poichè una computazione deterministica può essere vista come caso particolare di una computazione non deterministica.

Da queste considerazioni, si evince che emulare una macchina non deterministica con una deterministica consiste essenzialmente nella visita di un albero, la quale richiede tempo lineare rispetto al numero di nodi, ovvero esponenziale rispetto al numero di livelli. È chiaro dunque che un algoritmo NP richiede tempo esponenziale per essere risolto da una macchina deterministica.

Poichè il calcolatore classico è una macchina che lavora in tempo deterministico, i problemi NP hanno sempre rappresentato una sfida difficile da

superare, poichè il tempo richiesto per la loro risoluzione è proibitivo per dimensioni dell'input relativamente poco grandi.

Il calcolatore quantistico, invece, è una macchina che *lavora in tempo non deterministico*, ed è quindi in grado di risolvere problemi NP con la velocità con cui il computer tradizionale risolve problemi P. Tale affermazione ha delle pesanti ripercussioni sul mondo della crittoanalisi, ma, prima di parlare di queste, è necessario sottolineare un fatto teorico importante, che è diretta conseguenza di quanto appena asserito:

- la potenza di calcolo del computer quantistico **è la stessa** quella di un computer tradizionale; ovvero i problemi risolubili da un calcolatore quantistico sono *tutti e soli* i problemi risolubili da un calcolatore normale.

Ciò si riferisce al fatto che per alcuni problemi, noti in letteratura come problemi *indecidibili*, per i quali non esiste un algoritmo risolutore, non si trae alcun vantaggio utilizzando il computer quantistico rispetto a quello tradizionale. La dimostrazione di ciò è immediata considerando che, come accennato precedentemente, la computazione di una macchina non deterministica può essere emulata da una macchina deterministica tramite la visita dell'albero delle "operazioni"; se esistesse dunque una macchina non deterministica in grado di risolvere un problema indecidibile, sarebbe possibile costruire una macchina deterministica in grado di emularla e quindi in grado anch'essa di risolvere il medesimo problema, ma ciò è un assurdo poichè contraddice l'ipotesi di indecidibilità del problema dato.

Ciò nonostante, il computer quantistico è uno strumento di inestimabile valore nella risoluzione dei problemi decidibili che impiegano normalmente una quantità di tempo proibitivo, come i problemi NP.

9.2 Computer quantistico come strumento per il crittoanalista

In base a quanto affermato sul potere computazionale del calcolatore quantistico, appare chiaro che un crittoanalista in possesso di tale strumento sarebbe in grado di portare a termine un attacco di tipo *brute-force* ad un qualsiasi algoritmo crittografico in tempo polinomiale, ovvero in un tempo decisamente irrisorio.

Si potrebbe essere tentati di risolvere questo spiacevole problema creando un algoritmo di crittografia il cui attacco *brute-force* abbia complessità più elevata, ad esempio NEXP[27] invece che NP. In tal modo una macchina non deterministica impiegerebbe comunque tempo esponenziale per portare a

[27] I problemi appartenenti alla classe NEXP sono quelli risolvibili in tempo esponenziale da una macchina non deterministica.

compimento l'attacco, riportando la situazione uguale a quella precedente all'avvento del computer quantistico.

Tale proposito però non tiene conto di un problema fondamentale, insito nella natura delle classi di complessità sopra elencate: i problemi NP sono problemi aventi un albero delle computazioni con un numero di livelli polinomiale rispetto all'input. Se si sapesse a priori qualè un ramo che conduce ad una soluzione, una macchina deterministica che tenti di risolvere il problema potrebbe visitare direttamente quel ramo, impiegando tempo polinomiale. Questo è effettivamente ciò che accade con un calcolatore normale quando si decifra un messaggio di cui si conosce la chiave.

Utilizzare un algoritmo con complessità ad esempio NEXP, implicherebbe che *ogni* ramo dell'albero delle computazioni che conduca ad una soluzione, abbia lunghezza esponenziale rispetto alla dimensione dell'input. Ciò comporta che, per quanto detto, anche decifrare il messaggio conoscendone la chiave richiede un tempo esponenziale, e ciò è chiaramente inaccettabile.

Si può dunque concludere che, in presenza di un computer quantistico **un attacco *brute-force* richiede in ogni caso lo stesso tempo richiesto dalla decifrazione del messaggio avendo a disposizione la chiave di cifratura**.

9.3 Computer quantistico vs. crittografia quantistica

In base a quanto detto nelle prime parti di questo documento, il calcolatore quantistico non offre alcun aiuto al crittoanalista intento a decifrare un messaggio crittato quantisticamente. La vera difficoltà di tale attacco, non è infatti legata a questioni di natura computazionale, bensì all'impossibilità di intercettare il messaggio senza che i veri interlocutori se ne accorgano e decidano quindi di prendere provvedimenti. Và evidenziato infatti che, oltre alle difficoltà prodotte da un'evidente introduzione di un tasso di errore nella comunicazione, il tentativo di intercettazione del messaggio comporta un meccanismo di tipo *store-and-forward*,[28] il quale, considerando la velocità di propagazione dei fotoni nella fibra ottica e l'ordine di grandezza delle distanze coperte, introduce una latenza decisamente sospetta nella comunicazione.

10 Stato attuale dell'arte

La crittografia quantistica è un mondo ancora molto giovane e decisamente complesso, nel quale, nonostante l'enorme interesse suscitato ed il considerevole sforzo di ricerca fin'ora speso, non sono stati riportati risultati eccellenti. La meccanica quantistica, infatti, fornisce con il fotone uno strumento che

[28] ovvero un meccanismo che prevede la lettura del bit in arrivo e la riproduzione di questo in uscita.

necessità di protocolli che ne sfruttino le potenzialità crittologiche, come il BB84 esposto nella parte seconda. Nel tempo sono stati proposti diversi protocolli inerenti anche operazioni diverse dalla distribuzione di una chiave,[29] ma si è poi dimostrato che ognuno di essi presenta delle falle che ne compromettono la sicurezza.

Ad oggi dunque, solo il protocollo BB84 risulta sicuro e quindi solo le applicazioni che possono farne uso traggono benefici dalla crittografia quantistica. Ciò evidenzia come questo campo sia effettivamente ancora tutto da scoprire.

Attualmente si sta iniziando ad esplorare anche una nuova frontiera della comunicazione quantistica, che sfrutta il fenomeno fisico detto *entanglement*. Tale fenomeno, che costituisce tuttora uno dei più grossi misteri della fisica quantistica, consiste nel fatto che più quanti generati sotto particolari condizioni dal decadimento di uno stesso quanto (e per questo denominati *entangled*) godano della seguente proprietà: la modifica dello stato di un quanto comporta lo stesso cambiamento di stato per tutti i quanti *entangled* rispetto ad esso. Ciò significa che avendo due fotoni entangled, ogni modifica apportata allo stato di uno si riflette immediatamente sullo stato dell'altro, indipendentemente dalla distanza a cui questi si trovano. Si può facilmente immaginare come questo sorprendente risultato sia potenzialmente la base di un tipo completamente nuovo di comunicazione a distanza; tuttavia, poichè l'entanglement è un fenomeno ancora inspiegato, la sua applicazione per scopi crittografici è vista con molta prudenza poichè non si ha la minima idea di come l'eventuale scoperta del funzionamento di tale fenomeno possa esporre una comunicazione che ne fa uso ad attacchi.

[29] I più noti sono i protocolli *bit-commitment* ed *oblivious-transfer*.