UNIVERSITÀ DEGLI STUDI DI PERUGIA
FACOLTÀ DI SCIENZE MATEMATICHE,
FISICHE E NATURALI

Corso di Laurea in Informatica

Crittografia Quantistica

PROFESSORE
Prof. Stefano Bistarelli

STUDENTI
Davide D'Arenzo, 246841
Riccardo Minciarelli, 251107

Anno Accademico 2010/2011

SOMMARIO

INTRODUZIONE

Crittografia quantistica, l'insieme di due grandi argomenti di ricerca; la crittografia, sempre più di utilizzo comune per celare informazioni sensibili e certificare l'indubbia provenienza di un messaggio; e la meccanica dei quanti o fisica quantistica, una dottrina che prova a spiegare tutti i fenomeni microscopici rivoluzionando la fisica classica [GRTR02].

Nel corso del XX secolo il mondo è venuto a conoscenza di alcune proprietà fondamentali della materia elementare, come ad esempio la capacità di un atomo di cambiare il suo stato dal momento in cui viene effettuata una particolare osservazione su di esso, oppure, la capacità di un fotone di attraversare un particolare percorso in base alla polarizzazione che viene imposta ad esso.

Il nostro lavoro è stato quello di studiare, capire e discutere di un sistema che tramite un protocollo prestabilito di crittografia quantistica, il BB84, generi una comunicazione sicura tra due vertici di trasmissione: il destinatario ed il mittente. Una comunicazione di questo tipo è in grado di rilevare intrusioni ed interrompere lo scambio di messaggi fra le due parti che ne compongono il sistema. In altre parole la comunicazione fra i mandanti non potrà mai avvenire se sul canale di comunicazione quantistico è avvenuta un intrusione che sarà sempre rilevata.

Ma perché è rilevata l'intrusione? Perché l'intruso genererebbe una quantità di errori sulla stringa di dati che in definitiva impedirebbe la generazione di una chiave comune. Quindi, dal momento in cui mittente e destinatario si aspettano di avere i medesimi risultati delle misure di polarizzazione e di posizione dei bit, risulterà chiaro che una violazione di sicurezza altererà lo stato dello spin e di conseguenza il confronto delle due misure produrrà un risultato nullo. Oggi sistemi del genere costano centinaia di migliaia di dollari, invece il prototipo studiato, indicato per terminali ATM, transazioni *online* etc., è compatto, a basso costo e si compone di due parti *hardware* proprietarie, il trasmettitore ed il ricevitore, che comunicano tramite l'invio e la ricezione di fotoni opportunamente polarizzati.

Il funzionamento del protocollo BB84 è semplice:

1. In trasmissione vengono scelti casualmente una sequenza di bit di 1 e 0, che vengono trasformati in fotoni applicando per ciascuno di essi una delle possibili polarizzazioni, nel nostro caso 0°, +45°, -45°, 90°, che successivamente saranno spedite al destinatario legittimo.

2. Una volta ricevuti i dati trasmessi, in ricezione si sceglieranno casualmente delle misure di polarizzazione che saranno attribuite a ciascun bit ricevuto, memorizzandole poi in una struttura dati.

3. A questo punto, su canale classico, il legittimo destinatario spedirà al mittente la sua sequenza di polarizzazione ma non le misure ottenute in ricezione, ed il mittente non dovrà fare altro che generare un pacchetto TCP/IP, indicandogli le posizioni corrette di misurazione. In questo modo le due parti condivideranno una chiave sicuramente segreta.

Dal punto di vista *software*, il sistema lavora su due calcolatori differenti: nel primo è presente un generatore di numeri pseudo casuali molto robusto, il *Blum Blum Shub* [BBSS86], che future ricerche potranno sostituire con sistemi *hardware* di generazione assolutamente casuale.

La crittografia quantistica fornisce un modo per generare materiale segreto condiviso in modo sicuro. Un segreto condiviso può essere utilizzato in tre modi: per proteggere l'algoritmo QKD (*Quantum Key Distribution*) in modo da generare altri segreti condivisi, per identificarsi ad altri, ed agire come chiave crittografica per crittografare messaggi. I segreti condivisi di solito vengono cancellati una volta usati.

La segretezza della generazione è salvaguardata dal codificare l'informazione su stati quantistici non ortogonali che un intercettatore non può misurare senza generare disturbo. I protocolli QKD sono progettati in modo da individuare questi disturbi e quindi avvertire della presenza dell'intercettatore. QKD è in linea di principio sicuro contro un attacco che utilizza la tecnologia reale o teorica, e gli sperimentatori hanno come sfida lo sviluppo di sistemi reali che corrispondano a questo ideale.

CAPITOLO 1 – Crittografia classica: origini, debolezze e trasformazione

Per migliaia di anni, re, regine e generali hanno avuto bisogno di comunicazioni efficienti per governare i loro Paesi e comandare i loro eserciti. Nel contempo, essi compresero quali conseguenze avrebbe avuto la caduta dei loro messaggi in mani ostili: informazioni preziose sarebbero state a disposizione delle nazioni rivali e degli eserciti nemici.

Fu il pericolo dell'intercettazione da parte degli avversari a promuovere lo sviluppo di codici e cifre, tecniche di alterazione del messaggio destinate a renderlo comprensibile solo alle persone autorizzate. Il bisogno di segretezza ha indotto le nazioni a creare dipartimenti di crittografia, il cui compito era garantire la sicurezza delle comunicazioni, escogitando e impiegando i migliori sistemi di scrittura segreta. Nello stesso tempo, i decrittatori hanno tentato di far breccia in quei sistemi e carpire i dati che custodivano.

Crittografi e decrittatori sono cercatori di significati, alchimisti votati alla trasmutazione di astruse serie di segni in parole dotate di senso. La storia dei codici è la storia dell'antica, secolare battaglia tra inventori e solutori di scritture segrete; una corsa agli armamenti intellettuali il cui impatto sulle vicende umane è stato profondo [SSCD01].

D'Altra parte, il naturale desiderio di riservatezza dei cittadini e la crescente domanda di crittografia si scontrano con le esigenze della legalità e della sicurezza nazionale. Se la prima guerra mondiale è stata definita la guerra dei chimici, a causa dell'impiego senza precedenti dei gas tossici, e la seconda, la guerra dei fisici, perché ha visto per la prima volta l'impiego bellico dell'energia atomica, il terzo conflitto mondiale potrebbe essere la guerra dei matematici.

Facendo un passo in avanti, vediamo come nel nostro millennio molti algoritmi di crittografia e protocolli e applicazioni di sicurezza della rete sono stati specificati come standard. I più importanti di questi sono gli standard Internet, definiti in vari documenti RFC (*Request for Comments*) e FIPS (*Federal Information Processing Standards*) emessi dal NIST (*National Istitute of Standard Technology*) [WSCR06].

Questi algoritmi fanno parte dello studio sulla crittologia che, per l'appunto, è lo studio delle tecniche per garantire la segretezza e/o l'autenticità dell'informazione.

La crittografia si può scindere in due grandi branche: la crittografia simmetrica o convenzionale e la crittografia asimmetrica o a chiave pubblica (Vedere anche [WDFK88]). Vedremo più avanti alcuni degli algoritmi più utilizzati attualmente nel nostro millennio e come quest'ultimi non sono sufficienti a predisporre una comunicazione sicura e dunque, di conseguenza, come sia assolutamente necessaria l'applicazione radicale della crittografia quantistica.

Fondamentalmente la crittografia simmetrica è un tipo di sistema crittografico nel quale sia la crittografia che la decrittografia sono eseguite utilizzando la medesima chiave. Questa chiave è utilizzata opportunamente per trasformare il testo in chiaro in testo cifrato e viceversa. Attualmente l'algoritmo più utilizzato che effettui questo tipo di procedure è l'AES (*Advanced Encryption Standard*), che è un algoritmo di cifratura a blocchi progettato per sostituire il DES (*Data Encryption Standard*) nelle applicazioni commerciali. Utilizza una dimensione di blocco di 128 bit e una chiave di lunghezza 128, 192 o 256 bit. Ciascuna delle sue fasi consiste in quattro funzioni separate: sostituzione di byte, permutazioni, operazioni aritmetiche su un campo finito e XOR con una chiave [WSCR06-1].

Questo standard è stato pubblicato dal NIST nel 2001, indice proprio della sua struttura complessa paragonato ad un algoritmo di cifratura asimmetrico come RSA (*Rivest – Shamir – Adleman*). In *Tabella 1.1* sono specificati i criteri di valutazione del NIST relativi allo standard AES.

Oggi, AES non è più un algoritmo di cifratura sicuro [*RIF. X1*]. Gli attacchi del *RIF. X1* riescono a ricavare la chiave di crittografia sfruttando la collisione dei blocchi interni, "calcolati" come *hash*, che è scatenata da un *injection* locale di stringhe che successivamente vengono corrette generando però dei molteplici disturbi.

Altri attacchi, al giorno d'oggi, si trovano per algoritmi quali DES, e persino RSA che, essendo un algoritmo di cifratura a chiave pubblica, dovrebbe garantire una sicurezza ottimale per la difficoltà di fattorizzazione. Purtroppo attualmente non è così. Il problema più grave è stato trovato il 13 maggio 2008 da L. Bello e pubblicato da *Debian O.S.*, riscontrando una vulnerabilità in un pacchetto del *software OpenSSL*, il motore che gestisce le connessioni sicure in rete per il protocollo *HTTPS*.

La falla era nel generatore di stringhe pseudo casuali che invece di mescolare i dati *random* con il *seed*, miscelava un valore non casuale che era rispettivo al valore ID del numero di processi nel sistema, per un massimo di 32768 valori, numero estremamente limitato da utilizzare come *range* del PRNG (*Pseudo Random Number Generator*), che è il motore centrale, che permette la randomizzazione dei numeri. Questo ha impedito la normale regolarizzazione della casualità nell'algoritmo che di fatto è diventato del tutto deterministico, con la conseguenza che tutte le chiavi SSL e SSH generate dal sistema sono a questo punto calcolabili, scavalcando il problema della fattorizzazione dei grandi numeri [TTBP09].

Il principale algoritmo che quindi ha sofferto di questo problema è proprio RSA, considerato sicuro fino alla data considerata in partenza.

RSA sfrutta sì, l'impossibilità (per ora) di fattorizzare i grandi numeri primi ma, quando deve essere applicato ad una trasmissione che necessita di un PRNG, si incorre sempre nel rischio che quest'ultimo come visto, sia o vulnerabile o troppo deterministico. Tant'è che in merito a questo problema sono state distribuite delle *blacklist* che utilizzate opportunamente permettono la violazione della chiave privata, all'interno dei sistemi che ancora oggi utilizzano gli algoritmi descritti in precedenza. Per risolvere questo problema è ovviamente necessario creare degli ambienti *chroot* congiunti all'utilizzo di *passphrase* per impedire gli attacchi a "*forza bruta*" e cambiando la porta d'ascolto del demone SSHD (*Secure Shell Daemon*), che è praticamente un componente del protocollo SSH (*Secure Shell*), che permette alla connessione di rimanere aperta e disponibile in rete. Tutto ciò ha un costo elevato che invece con l'avvento della meccanica quantistica può essere semplicemente risolto in un passo.

Altri attacchi possibili per RSA sono il MITM (*Man in the Middle,* attacco utilizzato per la prima volta da *K.D. Mitnick*, che gli consentì di frapporsi fra due computer che già avevano iniziato una connessione) e l'utilizzo di alcune conoscenze che si hanno sul testo cifrato scelto in corrispondenza al testo in chiaro noto, che permetterebbero di risalire alla chiave privata [DBTR08].

Il MITM invece permetterebbe all'*attacker* di cambiare la chiave pubblica inserita nel documento, inserendo la propria. Certo la comunicazione verrebbe interrotta vista l'impossibilità poi di decodifica da almeno una delle due parti in comunicazione, ma la sicurezza risulterebbe comunque violata. Ma questa è tutta un'altra storia!

Arrivati a questo punto, è chiaro il perché si è avuta la necessità di creare una forma di crittografia che garantisca un livello di sicurezza ideale e robusto anche contro gli attacchi dei super computer.

Sicurezza generale
Non esiste alcun attacco noto alla sicurezza di *Rijndael*. *Rijndael* utilizza delle *S-Box* come componenti non lineari. *Rijndael* sembra avere un margine di sicurezza adeguato, ma ha ricevuto qualche critica che suggeriva che la sua struttura matematica potrebbe essere soggetta ad attacchi.
Implementazioni software
Rijndael svolge molto bene le operazioni di crittografia e decrittografia in un'ampia varietà di piattaforme fra cui piattaforme a 8 e 64 bit e DSP. Tuttavia vi è una riduzione delle prestazioni quando aumentano le dimensioni delle chiavi dato il maggior numero di fasi che devono essere eseguite.
Ambienti con spazio limitato
In generale *Rijndael* è molto adatto ad ambienti con spazio limitato dove vengono implementate la crittografia e la decrittografia, ma non entrambe. Ha ridottissimi requisiti in termini di RAM e ROM.
Implementazioni *Hardware*
Rijndael è il più efficiente rispetto a tutti gli altri finalisti per le modalità con *feedback* e secondo per le modalità senza *feedback*.
Attacchi alle implementazioni
Le operazioni utilizzate da *Rijndael* sono tra le più facili da difendere dagli attacchi a controllo dell'energia e del tempo.
Crittografia e decrittografia
Le funzioni di crittografia e decrittografia *Rijndael* sono differenti. Uno studio della FPGA indica che l'implementazione combinata della crittografia e della decrittografia richiede circa il 60% di spazio in più rispetto all'implementazione della sola crittografia.
Agilità della chiave
Rijndael supporta il calcolo in tempo reale della sottochiave di crittografia.
Altri elementi di versatilità e flessibilità
Rijndael supporta blocchi e chiavi di 128, 192 e 256 bit in qualsiasi combinazione. In linea di principio la struttura di *Rijndael* può impiegare blocchi e chiavi di qualsiasi dimensione (ma multipli di 32 bit) e anche variazioni del numero delle fasi.
Potenzialità in termini di parallelismo delle istruzioni
Rijndael ha eccellenti potenzialità per sfruttare il parallelismo nella crittografia di un singolo blocco.

Tabella 1.1 – Valutazione finale del NIST relativa all'algoritmo *Rijndael* (2 ottobre 2000) [WSCR06-3]

CAPITOLO 2 – Crittografia quantistica

Quando trattiamo di crittografia quantistica è meglio specificare che è più giusto definire quest'ultima come *Quantum Key Distribution* (QKD), grazie alla quale si ha la capacità di trasmettere informazioni sicure tramite una chiave sicura. Dunque la QKD non è utilizzata per cifrare e proteggere le informazioni, né per trasferire informazioni crittografate e nemmeno per archiviare in modo sicuro dati importanti: i protocolli di QKD sono esclusivamente utilizzati per generare e distribuire chiavi segrete che poi possono essere utilizzate insieme ad altri algoritmi di crittografia classica. Dunque è chiaro che la crittografia quantistica è utilizzata, in seconda istanza, in correlazione alla crittografia classica [FGPA06].

Soffermiamoci a questo punto sul come la chiave deve essere generata da questo tipo di sistema. Generalmente nella crittografia classica si ha la necessità, con alcuni algoritmi, di utilizzare dei generatori pseudo casuali di dati, abbastanza robusti, che consentono in secondo luogo di generare la chiave privata che tecnicamente dovrebbe essere puramente casuale e di lunghezza appropriata, ma che in realtà può essere ricavata con l'ausilio di algoritmi deterministici che "simulano" il comportamento di un generatore pseudo casuale di numeri. Per risolvere questo problema di conseguenza si possono adottare due misure di sicurezza:

1. I due interlocutori devono scambiarsi la chiave "fisicamente", in altre parole vedendosi di persona.

2. I due interlocutori devono adottare delle tecniche di crittografia asimmetrica basandosi sulla generazione di chiavi pubbliche (*RSA, Diffie-Hellmann etc.*).

Nel primo caso è pressoché scontato che la chiave è scambiata in maniera sicura, ma nonostante il secondo ci suggerisca una percentuale di segretezza maggiore (vista la difficoltà di calcolo per violare un algoritmo di crittografia asimmetrica senza la conoscenza della chiave), non è detto che un futuro calcolatore più veloce non possa fattorizzare in maniera estremamente veloce le chiavi interne elaborate dallo stesso algoritmo che formano poi la chiave pubblica[HBPQ04]. Come non è detto che in futuro non si riesca a dimostrare e trovare matematicamente un modo per fattorizzare i logaritmi discreti usati nella maggior parte degli algoritmi che effettuano crittografia asimmetrica: ad esempio attraverso computer quantistici

La forza della crittografia quantistica è proprio la capacità di utilizzare degli stati fisici del fotone che consentono di rilevare l'intrusione grazie ad un'aumentata percentuale di errore sul canale quantistico. Questa forma di trasmissione non ha bisogno né di utilizzare generatori di dati, poiché è sufficiente la casualità del fotone nel cambiare il suo *spin* che ne determina lo stato di polarizzazione, né di cifrare le informazioni. Tolte le due cause principali di violazione della comunicazione è garantita, dunque, la capacità di rilevamento dell'*intruder*, quindi i problemi di sicurezza sono risolti.

Esaminando invece i pro e i contro di questa forma di comunicazione possiamo trovare utili caratteristiche nella *tabella 2.1*[HBPQ04-1].

Fondamentalmente la QKD è utile se:

1. Il fine giustifica i costi .

2. E' strettamente necessario garantire l'inviolabilità della comunicazione, per esempio quella militare o industriale evitando quindi i diversi tipi di spionaggio.

3. Si vuole adottare una forma di sistema in grado di garantire sicurezza e segretezza virtualmente al cento per cento.

Notiamo che la QKD si basa su alcune proprietà delle particelle elementari le cui azioni e movimenti sono regolati dalle leggi universali della meccanica dei quanti. Fondamentalmente per far sì che due interlocutori colloquino in maniera sicura sulla rete abbiamo bisogno che questi si trovino su un canale quantistico che spesso è bi-direzionale e che abbiano a disposizione un canale ordinario classico su cui autenticarsi. Sul primo si trasmetteranno dunque i fotoni che formeranno fasci di luce e più in generale onde elettromagnetiche. Questi fotoni polarizzati, ovvero che assumono un certo stato, saranno in grado di essere letti e rilevati da due dispositivi, in altre parole abbiamo a disposizione un trasmettitore quantistico ed un ricevitore quantistico.

Vale la pena dare un'occhiata più da vicino agli elementi che governano questa nostra ricerca; i fotoni sono privi di massa, ciò significa che le leggi della fisica classica si scostano notevolmente dai comportamenti che hanno questo genere di particelle, in particolare ci basiamo su alcune leggi della meccanica dei quanti secondo le quali:

1. Non possiamo prevedere con certezza quale sarà il risultato di un esperimento, ma conosceremo solo le statistiche dei risultati che obbligano a ripetere l'esperimento più volte.

2. Non è possibile creare una "fotocopiatrice" di stati quantici, ossia non si può duplicare uno stato quantico sconosciuto.

D'altro canto ulteriori leggi affermano che ogni misurazione effettuata sullo stato del sistema ne altera lo stesso. Inoltre non è possibile misurare un fotone in stato di polarizzazione orizzontale - verticale simultaneamente ad un secondo fotone in stato diagonale.

Analizzando meglio quest'ultimo punto è chiaro che se un sistema di misurazione è atto a rilevare solo ed esclusivamente misure orizzontali e verticali ed il fotone si trova in una delle due condizioni, per principio la misurazione non altererà nessuno dei due stati del fotone, viceversa lo stato, verrà alterato se il sistema di misurazione è predisposto al rilevamento degli stati non ortogonali a quelli in uso (in altre parole se misuriamo in base diagonale commetteremo un errore del 50% sulla misurazione, modificando lo *spin* del fotone stesso) [GCGU03].

Infatti, la polarizzazione è una proprietà del fotone legata al suo momento angolare, che può essere immaginata come la relazione che c'è fra l'asse di una particella e la sua velocità di rotazione intorno allo stesso. Un esempio è visibile in *Figura 2.1*, che descrive come un fascio di fotoni viene polarizzato cambiando asse e come viene assorbito se passa attraverso filtri ortogonali.

Il protocollo *Bennet - Brassard* 1984 (BB84) è stato il primo a sfruttare queste proprietà dei fotoni per realizzare il primo sistema QKD. La sua implementazione è di norma molto semplice poiché si basa proprio su quei principi che, a differenza della loro semplice applicazione, sono estremamente complessi da dimostrare. In pratica in questo sistema vengono scelti quattro stati di polarizzazione (ovvero rispettivamente verticale / orizzontale e sinistra / destra diagonalmente, per l'appunto le basi) e si misurano sul canale di trasmissione [GCGU03].

Questo significa che se scegliamo il sistema di misura non compatibile incorreremo nell'errore visto in precedenza. Ad ogni stato è assegnato un valore in bit ed in questo modo è possibile trasmettersi il messaggio stesso (chiave) sul canale, poiché verrà a formarsi in via definitiva una stringa di uno e zero [HBPF04].

Vediamo in maniera chiara i passi di questo protocollo ponendo l'esempio più classico della crittografia; due interlocutori Alice e Bob vogliono trasmettersi una chiave sicura:

1. Alice sceglie a caso uno dei quattro stati di polarizzazione ed invia a Bob il fotone corrispondente su canale quantistico, registra poi la sua scelta senza riferirla a nessuno.

2. Bob sceglie a caso (indipendentemente da Alice), una delle due basi di polarizzazione e misura il fotone ricevuto in quella base. Memorizza quindi la base che ha scelto e il risultato ottenuto dalla misurazione, ma non lo comunica.

3. Questi due punti vengono ripetuti più volte fino ad ottenere una chiave sufficientemente lunga in base a ciò che deve essere trasmesso sul canale classico.

4. A questo punto, sul canale classico, Bob trasmette ad Alice le misurazioni che lui aveva scelto per ogni singolo fotone, ma solo le misure di polarizzazione scelte da lui stesso e non il risultato ottenuto riferendoci ai bit.

5. Per ogni fotone Alice replica un pacchetto a Bob specificandogli se quest'ultimo è stato misurato correttamente o meno e gli impone di cancellare tutti i risultati che si trovano in posizione scorretta. Ciò che rimane è la chiave [*Figura 2.2*].

[B3SS92] Dopo i passaggi [1] e [2] statisticamente Bob ha una chiave che è errata nel 25% dei casi. Cioè è dovuto al fatto che il sistema di misurazione di Bob statisticamente nel 50% dei casi ha una incompatibilità con il fotone trasmesso da Alice.

Queste percentuali di errore troppo alte fanno sì che successivamente Alice e Bob debbano necessariamente utilizzare il canale classico per comunicarsi parzialmente alcuni dei risultati ottenuti, secondo i punti [4] e [5]. Prendiamo ora in considerazione l'attacco più semplice che l'*intruder* E (Eva) può fare, ovvero intercettare e rispedire i dati sul canale quantistico.

L'*attacker* è posizionato esattamente al centro della comunicazione e riceve tutti i fotoni che gli interlocutori si trasmettono. Ma la fisica ed il protocollo BB84 non permettono la riuscita dell'operazione.

Basandoci sull'asserzione che non è possibile fare una fotocopia esatta di uno stato quantistico sconosciuto, l'unica cosa che l'*intruder* può fare è misurare i fotoni inviati da Alice, come Bob avrebbe fatto. Ma come Bob avrebbe avuto il 50% di errori sulla chiave, anche l'intruder incappa in questo genere di risultati. Ciò nonostante l'intruso può inviare a sua volta dei fotoni a Bob ma che a loro volta verranno misurati con un margine di errore del 50% in base alle leggi della meccanica quantistica: ciò significa che l'*intruder* avrà introdotto un ulteriore 25% di errore sulla corrispondenza della comunicazione che a conti fatti produrrà una correlazione delle chiavi fra Alice e Bob pressoché nulla [DLQA04].

Una contromisura dell'intruso potrebbe essere il cercare di ridurre quanto più possibile gli errori sul canale, ma ciò significherebbe misurare solo parte della comunicazione fra i due legittimi interlocutori per cui, di conseguenza, l'*attacker* non conoscerebbe l'intera chiave. In altre parole meno percentuale di errore è introdotta sul canale, meno informazioni sulla chiave può acquisire l'intrusore.

Per rilevare la presenza di un intruso sul canale, se la comunicazione fosse perfetta, cosa impossibile con qualsiasi strumento, ad Alice e Bob basterebbe rilevare la minima presenza di un errore nella chiave. Ciò che attualmente possiamo fare è predisporre di un *set random* di bit e confrontarli in maniera esplicita sul canale classico.

Ovviamente queste stringhe dovranno essere scartate dalla chiave ed essere inutilizzate in futuro. Se si trovano errori allora vi è stata un intrusione, ma questo solo in teoria. Quello che in realtà avviene è che l'*intruder* comporta sempre un aumento della percentuale di errore sul canale che comprova la non corrispondenza della chiave.

Altre brevi considerazioni vanno però fatte per quanto riguarda il problema dell'errore sul canale.

Come abbiamo visto non c'è modo in effetti di certificare la presenza di un intruso, ma soltanto la possibilità di impedire che la comunicazione avvenga se è rilevata una quantità di errore sufficiente a bloccare la trasmissione.

In futuro si potrà pensare di applicare degli algoritmi che permettano di correggere gli errori sperimentali e quindi in primo luogo di ridurre quasi a zero la possibilità che l'*intruder* abbia anche la benché minima informazione sulla chiave, ed in secondo luogo ottimizzare il protocollo usato. Se tuttavia questo non fosse sufficiente a ridurre a zero la capacità dell'*intruder* a reperire informazioni sulla chiave, bisognerebbe implementare un ulteriore passo al protocollo che introdurrebbe una sorta di "*principio della minima conoscenza*"; vale a dire che se è rilevata una percentuale di errore oltre una certa soglia limite, o deve crescere in maniera evidente la lunghezza della chiave oppure la comunicazione deve essere interrotta.

Generalmente la quantità di errori deve essere inferiore dell'11% per generare una chiave sicura.

PRO	CONTRO
La sicurezza è matematicamente provata e basata su leggi fisiche	Richiede linea ed *Hardware* dedicato
La sicurezza è costruita su principi di base che non cambieranno nel futuro	Attualmente è molto costoso
La sicurezza sarà inviolabile anche con l'avvento dei *Quantum Computer*	E' una scienza ancora molto giovane ed in fase di sviluppo
Può essere usato insieme al *One-Time-Pad* che è matematicamente sicuro	Attualmente lavora solo su brevi distanze (max. 100-150Km)
Per chiavi troppo lunghe la potenza di calcolo cresce esponenzialmente ma soltanto per problemi tecnici	

Tabella 2.1 – QKD *pro & contro*

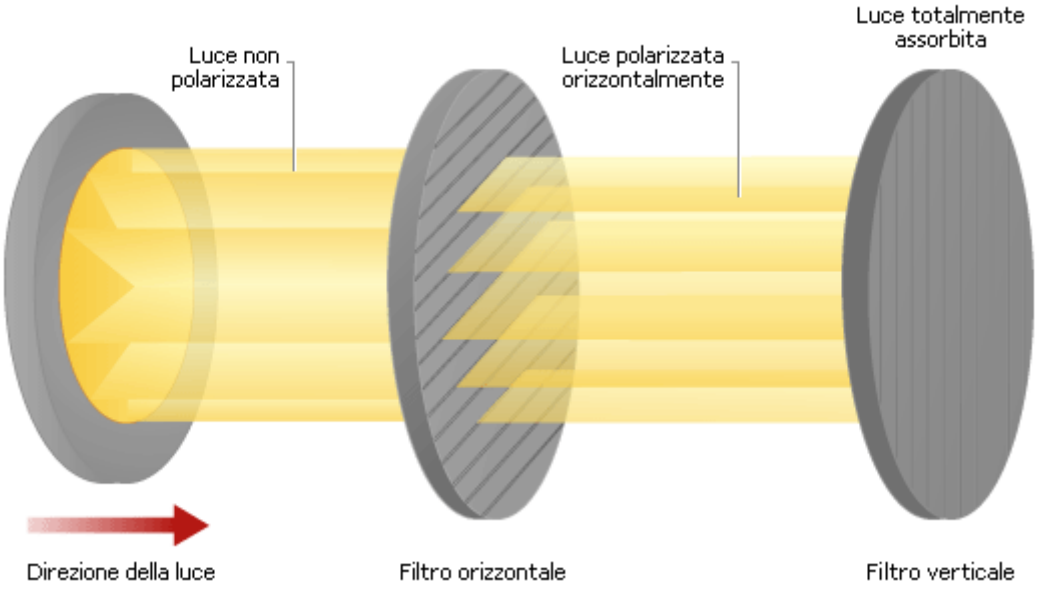

Figura 2.1 – Effetti della polarizzazione sulla luce. L'ultimo filtro ha una polarizzazione verticale. Dunque come si può vedere due stati ortogonali si annullano a vicenda. Se invece ruotassimo di 45° l'ultimo filtro si avrebbe un assorbimento della luce pari al 50%.

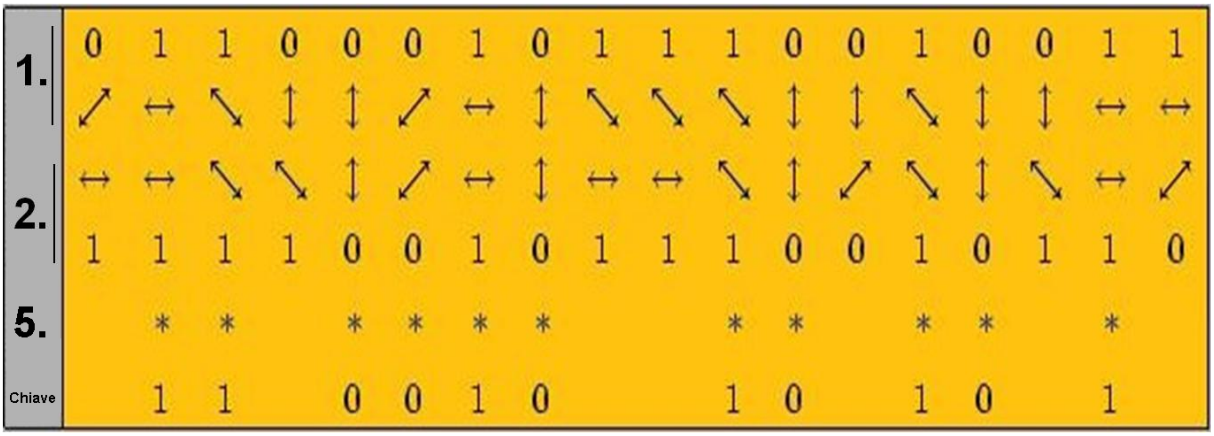

Figura 2.2 – Dimostrazione di come si ottiene la chiave sicura dal protocollo BB84.

CAPITOLO 3 – De artis statu

Trattando la meccanica dei quanti dal 1989 si pensò ad apparecchiature, in grado di sfruttare la fisica del fotone che, in qualche modo, riuscissero ad offrire delle garanzie sulla sicurezza di alcuni dispositivi come gli PRNG, per la sostituzione dei numeri pseudo casuali con i numeri puramente casuali negli algoritmi di crittografia e garanzie per una comunicazione sicura nella *global network*.

Proprio in questo periodo nei laboratori *T. J Watson* si cominciarono a sperimentare i primi protocolli per lo scambio delle chiavi e l'IBM riuscì a creare il primo canale quantistico lungo circa trenta centimetri. Il protocollo scelto per questo tipo di comunicazione era il BB84 che tuttavia, visti gli scarsi fondi a disposizione del laboratorio, non riusciva ad essere elaborato in maniera ottimale, poiché, l'apparecchiatura costruita era rudimentale e poco elaborata per una corretta gestione del protocollo stesso, anche se lo scambio della chiave privata riuscì perfettamente, nonostante il sistema girasse su un unico computer.

Successivamente verso la fine del 2001 quattro ricercatori dell'università di Ginevra fondarono una società, l'*IdQuantique*, che introdusse sul mercato i primi prototipi commerciali di sistemi che fornivano la distribuzione delle chiavi sfruttando il fotone e la sua meccanica. Dopo questa grande, riuscita, manovra di potenziamento tecnologico, l'*IdQuantique* si accorse che questi dispositivi potevano essere utilizzati anche per il rilevamento del singolo fotone (SPAD, *Single Photon Avalanche Diode*) e per la generazione di numeri puramente casuali [*Figura 6.1*].

Attualmente esistono QKD dell'*IdQuantique* che sfruttano il BB84 per lo scambio sicuro della chiave e AES 256bit per la crittazione vera e propria della stessa. Inoltre, la distanza raggiunta da questi dispositivi va dagli 80 chilometri per "*Cerberis*" ai 100 chilometri per "*Clavis*" e "*Vectis*" [*Figura 6.2*]. Altre aziende come la *BBN Technologies*, *Toshiba*, *NEC*, *Corning* sono comunque attive nel settore. La prima in questione ha sviluppato una piccola rete di crittografia quantistica in collaborazione con alcuni enti pubblici statunitensi.

Comunque sia, di recente sono state aperte nuove strade abbastanza interessanti per questa tecnologia. Già nel 2000 i progressi tecnologici compiuti nel campo avevano permesso ai ricercatori dei laboratori di Los Alamos di trasmettere una chiave su una distanza pari a un chilometro e mezzo, sfruttando però non la fibra ottica, ma un canale che avrebbe rappresentato una vera e propria svolta in questo campo: l'aria [FSSQ08-1].

Nel 2004 questo traguardo fu segnato da alcuni ricercatori di una società privata collegata al Ministero della difesa britannico, che ripeterono l'esperimento via aria, sulle montagne di Zugspitze nel sud della Germania, a una distanza di oltre 23 chilometri. Nonostante l'esperimento fu compiuto a oltre 3000 metri di altitudine e in piena notte, questo ha evidenziato la possibilità di creare satelliti artificiali in grado di trasmettere chiavi quantistiche per una distanza che varia dai 500 ai 1000 chilometri, satelliti che ruoterebbero attorno all'orbita terrestre. Successivamente, l'università di Padova, in collaborazione con l'ASI (*Agenzia Spaziale Italiana*) e con l'università di Vienna, ha testato per la prima volta il canale satellitare per la trasmissione dei singoli fotoni, caratterizzando e trasmettendo le problematiche e le accortezze che devono essere prese in considerazione per questo tipo di canale.

Questo progetto, chiamato *QSpace*, è stato il primo a permettere lo scambio di una chiave, tra un satellite e una stazione ottica a terra quella di ASI-MLRO (*Matera Laser Ranging Observatory*), Matera [*Figura 6.3 e Figura 6.4*]. L'idea è stata quella di simulare una sorgente di singoli fotoni a bordo del satellite, sfruttando la retro – riflessione di un debole impulso *laser* da un *corner – cube* (strumento ottico che ha la proprietà di riflettere un fascio luminoso incidente sulla superficie frontale esattamente verso la direzione di provenienza, formato da tre superfici ortogonali fra loro che determinano uno spigolo di cubo) di un satellite per il *laser – ranging*, che in pratica rileva in modalità spettroscopica la presenza di radiazioni *laser*, scegliendo i parametri in modo da avere meno di un fotone per impulso nel canale del satellite a terra [FSSQ08-1].

Successivamente tramite operazioni di filtraggio spaziale, temporale e in frequenza, la presenza del fotone è stata rivelata, nonostante un fortissimo rumore di fondo.

La riuscita di questo esperimento ha dato la possibilità di rompere numerose barriere sulla lunghezza che la meccanica dei quanti ci impone, tanto da permettere al gruppo di Padova in collaborazione con l'università di Vienna, di attuare un nuovo progetto chiamato QIPS finanziato dall'ESA (*European Space Agency*) che stabilirà la fattibilità a medio e lungo termine della comunicazione quantistica dalla terra allo spazio e viceversa. Sistemi del genere sono di interesse sia per grandi *network* di telecomunicazioni, sia per enti governativi o militari, come per esempio il Ministero della difesa.

Ancora, andando avanti con il tempo, nel 2004, è stato dato il via a un importante progetto europeo riguardante la crittografia quantistica, il SECOQC (*Secure Communication based on Quantum Cryptography*) [RASE07] che ha promesso di sviluppare un protocollo commerciale di crittografia quantistica in un massimo di quattro anni. Invece, il 28 giugno 2008, l'ETSI (*European Telecommunications Standard Institute*), ha sviluppato un piano per l'installazione e la resa operativa del QISG (*Industry Specification Group for quantum standards*). Questo nuovo gruppo nasce con lo scopo di portare la crittografia quantistica fuori dagli ambienti sperimentali universitari, introducendola nel mondo reale. Questo perché in qualche modo bisogna avanzare nella ricerca in questo settore. In particolare si intraprenderanno strade per lo sviluppo degli obiettivi di sicurezza che la crittografia quantistica dovrà rispettare, e la tecnologia dovrà poi essere standardizzata per il mercato *home – client*.

Inoltre si dovrà avere la possibilità di interfacciare queste nuove categorie di prodotto con gli impianti già esistenti. Si pensa addirittura ad una prima e nuova versione di rete "*quantistica*" con computer che lavoreranno il *Qbit* transcodificandoli in bit "*classici*". Si pensa addirittura alla "*quantum internet*", fino a spingersi poi in un progetto chiamato *Quantum Backbone Link Interface* (QBB – LI) sviluppato dalla SECOCQ che permetterebbe la comunicazione fra più nodi della rete come visto in precedenza in questi capitoli.

Tutto sta nello sviluppare sistemi, che sfidano e romperanno gli standard della fisica classica.

Figura 6.1 – Due dispositivi che permettono la generazione di numeri puramente casuali.

Figura 6.2 – Uno dei sistemi che effettuano trasmissione quantistica dell'*IdQuantique*.

Figura 6.3 – Il telescopio di terra che ha “visto” il fotone nella stazione MLRO.

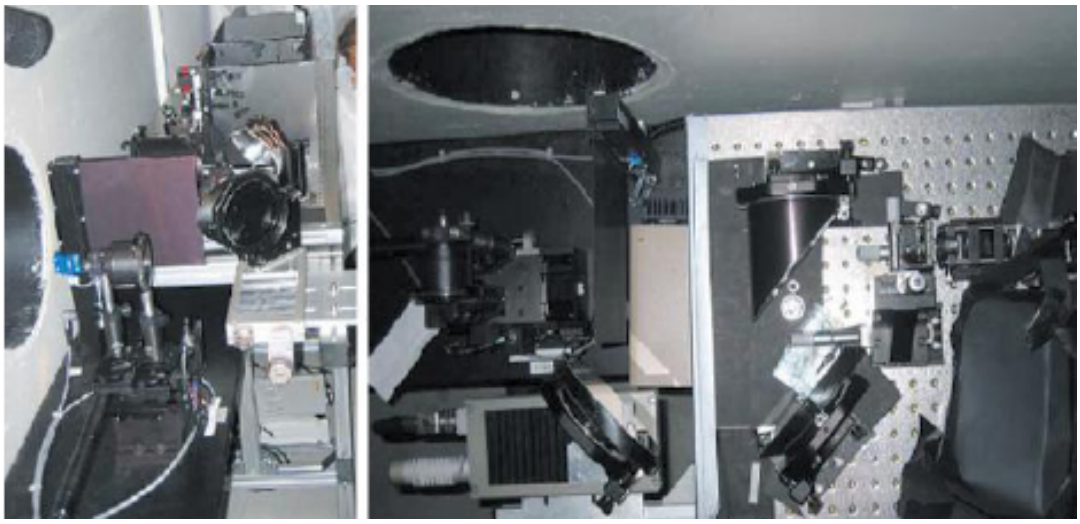

Figura 6.4 – A sinistra il ricevitore ottico del fotone del MLRO e a destra una sezione ottica del progetto *QSpace*.

CONCLUSIONI

Nel corso della storia sono state usate moltissime forme di crittografia per inviare messaggi da parte di governi, eserciti e imprese, facendo affidamento sull'affidabilità di questa tecnologia. Purtroppo, come abbiamo avuto modo di vedere nel corso dei secoli, questi algoritmi cifranti spesso erano vulnerabili a diversi tipi di attacchi, ma oggi la tecnologia quantistica permette in linea di principio di risolvere tutti i problemi incontrati sia dalla crittografia simmetrica che asimmetrica.

Un computer quantistico ha la possibilità di convertire le informazioni binarie in particelle quantistiche fondamentali. Questo ci darà quindi la capacità di risolvere problemi di calcolo che oggi sarebbe impossibile implementare. Inoltre la tecnologia quantistica offre, come visto, la possibilità di generare delle chiavi sicure al cento per cento, riserbando la loro segretezza senza far incorrere nel dubbio che questa possa essere violata, grazie alle prove scientifiche dimostrabili.

Logicamente oggi sistemi del genere devono essere meglio riadattati alle esigenze di una grande rete, poiché abbiamo bisogno di cavi in fibra ottica dedicati e di utilizzare dei ripetitori quantici per allungare le distanze limite dovute al decadimento del fotone.

Diversi ricercatori di tutto il mondo - citiamo alcune località come Los Alamos, Londra, New Mexico - stanno poi sperimentando la trasmissione quantistica attraverso l'aria, piuttosto che su fibra ottica. L'idea è quella di inviare chiavi segrete fino ai satelliti che attualmente circondano il globo.

Altri sviluppi [HBPQ06] sono stati elaborati per aziende interessate quali "Visa International", "NEC", "Toshiba" e per società quali "MagiQ Technologies" a New York e "Id Quantique" a Ginevra che di recente hanno cominciato a vendere prodotti che effettuano crittografia quantistica. Il costo per implementare questi sistemi in una grande azienda è di centinaia di migliaia di dollari e per il momento è limitato ad alcuni *campus* e nelle aree metropolitane, di Durban (Sud Africa), Londra e Madrid, ma la nostra ricerca mira proprio ad abbassare il costo di tali apparecchiature e ridurre i costi che ad ogni modo lievitano per l'assunzione di esperti dell'ITC.

BIBLIOGRAFIA

[B3SS92] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. – Experimental Quantum Cryptography" – Journal of Cryptology, 1992

[BBSS86] Lenore Blum, Manuel Blum, and Michael Shub, "A Simple Unpredictable Pseudo-Random Number Generator", SIAM Journal on Computing, volume 15, pagg. 364–383, maggio 1986

[DLQA04] Fu-Guo Deng, Gui Lu Long – Quantum privacy amplification for quantum secure direct communication, Agosto 2004

[FGPA06] E. Filoramo, A. Giovannini, C. Pasquero – Alla scoperta della crittografia quantistica – Bollati-Boringhieri, 2006.

[FSSQ08-1] F. Scarongella – Simulazione di un protocollo di crittografia quantistica – Lo stato dell'arte, p.64, Università degli studi di Milano, 2008

[GCGU03] G. C. Ghirardi – Un'occhiata alle carte di Dio – il Saggiatore, La crittografia quantistica, p. 264-280, 2003

[GRTR02] N. Gisin, G.Ribordy, W. Tittel, H. Zbinden – Reviews of modern physics, Vol. 74, p. 145, Gennaio 2002

[HBPF04] H.B. Pasquinucci – A first Glimpse at Quantum Cryptography – Physics Principles and The BB84 protocol – Aprile 2004, v 0.5

[HBPQ04] H. B. Pasquinucci – Quantum Cryptography, pro & cons – What is Quantum Cryptography, Marzo 2004, v 0.4

[HBPQ04-1] H. B. Pasquinucci – Quantum Cryptography, pro & cons – QKD vs. Public/Private Key Protocols, Marzo 2004, v 0.4

[HBPQ06] H. B. Pasquinucci – Quantum Cryptography on the market today – UCCI.IT, Settembre 2006

[RASE07] Romain Alleaume, et al. – SECOQC White Paper on Quantum Key Distribution and Cryptography (2007)

[RIF X1] – A. Biryukov, D. Khovratovich – Related – Key Cryptanalysis of the Full AES-192 and AES-256 – (https://cryptolux.org/mediawiki/uploads/1/1a/Aes-192-256.pdf)

[SSCD01] S. Singh – Codici & Segreti – The Code Book, Introduzione, Aprile 2001

[TTBP09] T. Tarolla – Bug about PRNG – Università degli studi di Milano, Penetration Testing, Maggio 2009

[WDFK88] W. Diffie – The first ten years of public-key cryptography – Proceedings of the IEEE, Maggio 1988

[WSCR06] W. Stallings – Crittografia e sicurezza delle reti – Contenuti generali, Capitolo 0, 2006

[WSCR06-1] W. Stallings – Crittografia e sicurezza delle reti – Lo standard AES, p.137, 2006