5 CRITTOGRAFIA QUANTISTICA

1 — CRITTOGRAFIA CLASSICA

Uno degli algoritmi quantistici più importanti è quello di Shor [**Shor1999**] per la fattorizzazione di numeri interi. La sua importanza sta nel fatto che è un algoritmo quantistico che ha uno *speed-up* esponenziale rispetto agli algoritmi classici e risolve un problema di enorme importanza per la crittografia.

Il protocollo maggiormente usato per lo scambio di informazioni sicure è l'RSA (dalle iniziali degli scopritori Rivest-Shamir-Adleman). Questo si basa sul fatto che dato un numero intero (grande) prodotto di due numeri interi e primi, i.e., $m = p \cdot q$ con p e q primi, sia computazionalmente difficile trovare la sua fattorizzazione, ovvero p e q. L'algoritmo di Shor ha mostrato che un eventuale computer quantistico potrebbe fattorizzare m in tempi esponenzialmente brevi rispetto ai computer attuali. Questo significa che le chiavi crittografiche basate sulla RSA che oggi si pensano sicure per svariati anni (si pensi alle carte di credito che sono cambiate ogni tre anni) potrebbero essere decrittate in settimane o mesi rendendole inservibili [1]. Tuttavia, se da una parte la meccanica quantistica potrebbe rendere insicuri gli schemi crittografici odierni come l'RSA, dall'altra apre le porte a nuovi protocolli crittografici che sono sicuri perchè sfruttano le leggi di base della fisica quantistica.

Il protocolli crittografici quantistici sono a chiave privata (*private key cryptography*); ovvero, Alice e Bob devono avere una chiave criptografica comune e sicura. Uno dei codici a chiave privata più semplici è il *Vernam cipher* (figura 18). Alice e Bob condividono una chiave privata (*encryption key*). Alice la usa per criptare il messaggio originale (*encrypted message*) e spedirlo a Bob attraverso un canale pubblico. Bob usando la stessa chiave può decriptare il messaggio di Alice. In questo caso, se il messaggio viene intercettato da Eve, questa non riuscirà a decifrare il messaggio. Infatti, visto che la chiave criptografica è ignota (e quindi per Eve è random), l'unico approccio è cercare di trovarla mediante forza bruta; quindi, per chiavi criptografiche sufficientemente complesse, con tempi lunghi e grande potenza di calcolo.

La crittografia a chiave privata ha però degli enormi difetti pratici. Se si usa la stessa chiave per criptare un numero elevato di messaggi, Eve può accumulare abbastanza informazione e riuscire a scoprirla. Quindi le chiavi private vanno cambiate periodicamente ma anche questo comporta delle complicazioni. Infatti, la stessa chiave, ad esempio mandata tramite un canale di comunicazione, può essere intercettata e rubata. Queste motivazioni e difficoltà hanno favorito negli anni intorno al 1970, lo sviluppo della crittografia a chiave pubblica.

1 É per questo che settori che maneggiano dati sensibili come i militari o le banche si sono interessati da subito nell'informazione quantistica.

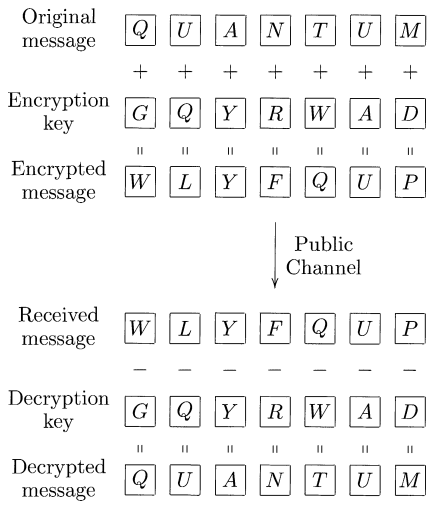

Figure 18: Il *Vernam cipher*: un esempio di crittografia a chiave privata. Immagine presa da [**nielsen-chuang_book**].

La crittografia quantistica segue uno schema a chiave privata e, in particolare, si focalizza sullo scambio delle chiavi private (si parla infatti di *Quantum Key Distribution* o QKD). Come nel caso classico, lo scambio della chiave avviene attraverso un canale pubblico (quindi insicuro e intercettatile). La differenza che, per le leggi fisiche che governano la meccanica quantistica, è possibile stabile con estrema precisione se il messaggio è stato intercettato.

II — CRITTOGRAFIA QUANTISTICA

La crittografia quantistica è il settore dell'informazione quantistica più sviluppato e più vicino alla produzione di massa. Al momento di scrivere, i settori della sicurezza militare e il settore bancario stanno pensando di implementare protocolli di crittografia quantistica per rendere (più) sicuri gli scambi di informazioni interni. Progetti più avveniristici prevedono la costruzioni di reti per lo scambi di dati crittografici nazionali, transnazionali e addirittura con satelliti orbitanti intorno alla terra.

La ragione per questo veloce sviluppo è legata alla semplicità dei protocolli e al numero limitato di operazioni che sono necessarie per implementarli. Per un protocollo crittografico è necessario solo riuscire a inizializzare i qubit e fare delle misure in basi diverse. Non servono quindi porte logiche che permettono di costruire un'arbitraria sovrapposizione di stati logici o operazioni complesse.

Questa è una semplificazione enorme e soprattutto permette di implementare i protocolli crittografici in sistemi ottici che usano la polarizzazione dei fotoni per codificare l'informazione quantistica. I fotoni hanno la proprietà di essere stabili

e robusti rispetto a perturbazioni esterne (ambientali), facili da manipolare e da trasmettere anche su lunghe distanze (ad esempio, attraverso una fibra ottica).

Il primo protocollo per la crittografia quantistica fu proposto da Charles Bennett and Gilles Brassard nel 1984 ed è chiamato comunemente protocollo BB84 (dalle iniziali degli autori e dall'anno di pubblicazione) [**bb84**]. É il più semplice dei protocolli ma ha in se tutte le caratteristiche e le idea essenziali tanto che gli altri si possono considerare delle ottimizzazioni del BB84.

5.2.1 Protocollo BB84: idee di base

Il protocollo BB84 è un protocollo sicuro per la distribuzione di chiavi crittografiche. L'idea è che Alice e Bob possano scambiarsi una chiave crittografica sicura con cui criptare il messaggio che si vogliono scambiare. La meccanica quantistica ha due proprietà fondamentali che permettono la sua implementazione: Un eventuale *hacker* (che chiameremo Eve)

1. non può copiare un generico qubit contenente l'informazione a causa del teorema *no-cloning* in sec. (4.2.1).

2. una misura del qubit lo perturba a causa del collasso della funzione d'onda sec:measurement.

A livello classico, se Eve si inserisse nel canale di comunicazione fra Alice e Bob, potrebbe copiare l'informazione mandata da Alice e rispedire tutto a Bob che non potrebbe accorgersi della copia. Oppure potrebbe fare una misura diretta sui bit trasmessi senza che Bob si accorga di niente. Queste due procedure sono impossibili se l'informazione è trasmessa tramite qubit invece che con bit classici.

L'implementazione del protocollo per lo scambio di una chiave crittografia sicura è complicato dal fatto che si devono stabilire con criteri quantitativi se c'è stato l'intervento di Eve o no.

L'idea alla base del protocollo BB84 è che dato uno stato quantistico esiste una base in cui l'output della misura è certo e non probabilistico 3.3. Ad esempio, se il sistema si trova nello stato $|0\rangle$ una misura nella base canonica darà il valore 1 con probabilità 1. Al contrario, se il sistema si trova nello stato $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ una misura darà il valore 1 con probabilità $1/2$ e il valore -1 con probabilità $1/2$. Però , se il sistema è nello stesso stato $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ ma misuriamo nella base $\{|+\rangle, |-\rangle\}$ (si veda sec. 3.3) otterremo il valore 1 con probabilità 1. Quindi, l'output della misura è certo o meno a seconda dello stato e della base in cui si fa la misura [2].

Dobbiamo aggiungere un'ulteriore precisazione l'informazione logica "astratta" è costituita da due bit 0 e 1. Questa però può essere fisicamente codificata in diversi stati. Ad esempio, in un sistema classico potremmo stabilire che lo stato logico 1 corrisponde al passaggio di corrente in un filo e lo 0 all'assenza di corrente. La stessa informazione potrebbe essere codificata in termini di voltaggio.

2 Nel linguaggio della Fisica si dice che viene misurato l'operatore di Pauli Z o σ_z nel primo caso, X o σ_x nel secondo. Il risultato della misura è certo se lo stato è un autostato dell'operatore da misurare ed è invece probabilistico se è sovrapposizione di autostati dell'operatore da misurare.

In meccanica quantistica abbiamo un elemento in più perchè nello stesso sistema fisico possiamo scegliere diverse basi in cui codificare l'informazione e fare la misura. Ad esempio, potremmo stabilire che il bit logico 0 è codificato da uno stato con polarizzazione (sez. 3.1.2) verso l'alto $|0\rangle = |\uparrow\rangle$. Ma potremmo anche decidere di usare la polarizzazione a 45° per cui dire che $|0\rangle = |\nearrow\rangle$. Questi due stati non sono ortogonali quindi ricadiamo nella distinzione discussa sopra.

Per il protocollo BB84 possiamo identificare due basi indicate con B_1 e B_2: **Base** $B_1 : \{|0\rangle, |1\rangle\}$ e **Base** $B_2 : \{|0_+\rangle, |1_+\rangle\}$. La relazione fra le due basi è

$$\begin{aligned} |0\rangle &= \frac{|+\rangle + |-\rangle}{\sqrt{2}} = \frac{|0_+\rangle + |1_+\rangle}{\sqrt{2}} \\ |1\rangle &= \frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{|0_+\rangle - |1_+\rangle}{\sqrt{2}} \end{aligned} \tag{5.2.1}$$

e

$$\begin{aligned} |0_+\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \\ |1_+\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle\,. \end{aligned} \tag{5.2.2}$$

Con questa notazione vogliamo evidenziare che l'informazione logica 0 può essere codificata in due stati fisici $|0\rangle$ e $|0_+\rangle$. A questo scopo, abbiamo usato una notazione leggermente diversa. Gli stati che nel capitolo 3 erano denotati con $|+\rangle$ e $|-\rangle$ ora sono, rispettivamente, $|0_+\rangle$ e $|1_+\rangle$. Da relazioni di sopra vediamo che se misuriamo nella base B_1 gli stati $|0\rangle$ e $|1\rangle$ otterremo il corrispondente autovalore con probabilità 1; se invece gli stessi stati vengono misurati nella base B_2 l'output sarà l'autovalore associato a $|+\rangle$ il 50% di volte e l'autovalore associato a $|-\rangle$ il rimanente 50%. In maniera analoga, nella base B_2 gli stati $|0_+\rangle = |+\rangle$ e $|1_+\rangle = |-\rangle$ otterremo il corrispondente autovalore con probabilità 1; mentre una misura nella base canonica B_1 darà l'autovalore associato con probabilità del 50%.

Protocollo BB84: implementazione

Punto 1
Fissato a n il numero di qubit da usare nel protocollo, Alice estrae due sequenze di n numeri casuali di 0 e 1. La prima sequenza n rappresenta una stringa logica associata al messaggio mentre la seconda rappresenta la base in cui codificare il messaggio. Ad esempio, potremmo decidere di usare la base B_1 ogni qualvolta nella seconda stringa compare lo 0 e la base B_2 quando compare 1. Quindi l'unione delle due stringhe ci dice bit-per-bit l'informazione che dobbiamo codificare e la base in cui dobbiamo codificarla. Un esempio è mostrato in tabella 5. Seguendo questo schema, Alice prepara una serie di qubit e li manda a Bob.

stringa logica A	0	1	1	0	1	1	1	0
stringa base A	0	0	1	0	0	0	1	0
qubit A	$\|0\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|0\rangle$

Table 5: Codifica dei qubit da parte di Alice

stringa logica A	0	①	①	0	①	1	1	⓪
stringa base A	0	$\boxed{0}$	$\boxed{1}$	0	$\boxed{0}$	0	1	$\boxed{0}$
qubit A	$\|0\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|0\rangle$
stringa base B	1	$\boxed{0}$	$\boxed{1}$	1	$\boxed{0}$	1	0	$\boxed{0}$
misura B	0^*	①	①	1^*	①	0^*	1^*	⓪

Table 6: Misura dei qubit da parte di Bob. I casi in cui la base di misura di Alice e Bob coincide sono segnalati con □. Questi portano ad un output della misura certo e in cui il valore trovato da Bob coincide con quello codificato da Alice (segnalati con ◯).

Punto 2
Bob riceve i qubit da Alice ed estrae n numeri random. Questi determinano la base in cui Bob fa la misura dei qubit. Ad esempio, se il primo numero random estratto è 1, Bob misura nella base B_2. Bob non sa la sequenza di basi che Alice ha usato per la codifica, quindi la sua stringa e le successive misure saranno scorrelate e coincideranno solo statisticamente con quelle di Alice. Rimane però vero che se quando i bit nella stringa delle basi di Alice e Bob coincidono, la misura di Bob darà un risultato con probabilità 1. Se invece non coincidono ogni out-put avrà probabilità 1/2.

Un esempio è mostrato in Tabella 6. La riga più interessante è l'ultima (misura di B). Qui con l'asterisco sono segnati i risultati della misura che sono probabilistici (escono con il 50% di probabilità) perchè le stringhe della basi di Alice e Bob non coincidono. Invece sono cerchiati i risultati della misura di Bob per cui l'output è certo dato che le stringhe della basi di Alice e Bob coincidono (segnalati con un quadrato). Il punto fondamentale è che in questo caso il valore misurato da Bob è lo stesso di quello codificato inizialmente da Alice (come evidenziato nell'ultima riga in Tabella 6).

Punto 3
Alice e Bob pubblicano apertamente la stringhe di bit con cui hanno scelto, rispettivamente, la base di codifica e misura. A questo punto, sanno i bit logici associati saranno gli stessi per entrambi e quindi condividono una chiave segreta (perchè solo loro conoscono il valore effettivo dei bit che non è stato pubblicato).

Nell'esempio in tabella 6, Alice e Bob sanno che i bit $2, 3, 5$ e 7 sono associati alla stessa base e come si deduce dalla tabella la stringa associata *a questi sarà* 1110 e potrà essere usata per criptare un messaggio.

Fino a questo punto abbiamo esaminato, come Alice e Bob possono scambiarsi una chiave pubblica usando qubit. La vera forza della QKD sta nel fatto che, a differenza di quella classica, può essere resa sicura rispetto agli attacchi di Eve.

Intervento di Eve
Visto che Eve non può copiare i qubit per il teorema *no-cloning*, l'unica cosa che può fare è inserirsi nella comunicazione fra Alice e Bob e sostituirsi a Bob nella misura per poi mandare a Bob dei qubit. Eve può estrarre una sua stringa di numeri random, in base a questa scegliere la base in cui misurare e mandare un informazione a Bob. Come nel caso di Bob, i risultati della misura di Eve saranno gli stessi del bit logico codificato da Alice solo nel caso in cui le stringhe della basi di Alice e Eve coincidono. Per minimizzare la perturbazione dell'informazione (e quindi non essere scoperta) Eve manderà a Bob il risultato della della sua misura. Ad esempio, se misura un qubit nella base B_2 e il risultato è 0, manderà a Bob lo stato $|0_+\rangle$. Se per tale qubit la base di Eve coincide con quella di Alice, la misura non perturberà lo stato e Bob riceverà esattamente lo stesso qubit mandato da Alice. Eve è riuscita nell'intento di rubare l'informazione senza essere osservata.

Allo stesso tempo, nei casi in cui la la base di Eve e Alice non coincidono, Eve misurerà , distruggerà lo stato originale e mandrà a Bob un qubit logico che è quello originale solo il 50% delle volte. Facciamo un esempio, supponiamo che Eve misuri il qubit 2 nella base B_2 (Alice aveva usato la base B_1) e che il sistema collassi nello stato $|0_+\rangle$. Eve manderà a Bob lo stesso stato e Bob che, secondo la tabella 6 sceglie la base la stessa base di Alice B_1, non misurerà con certezza lo stato 1 ma solo con probabilità 1/2.

Da questa analisi arriviamo alla conclusione che, statisticamente, Eve perturba la metà dei qubit in cui Alice e Bob dovrebbero avere uguali. Quindi la presenza di Eve può essere svelata con il seguente

Punto 4
Fra i qubit che sono stati misurati nella stessa base, Alice e Bob selezionano la prima metà e svelano pubblicamente i risultati delle misure. In assenza di Eve la correlazione fra i risultati dovrebbe essere completa. La presenza di Eve si rivela quando le misure fra questi qubit danno risultati diversi. Una volta che Alice e Bob stabiliscono che il minimo di correlazione per la sicurezza è , ad esempio, del 90%, decidono che la comunicazione è stata "disturbata" ogni volta che le correlazione scende sotto tale soglia. Se è così , il protocollo viene annullato e viene riattivato usando altri canali non intercettabili.

Quanti qubit sono necessari per scambiare una chiave crittografia di m bit? Se si parte da n qubit iniziali, solo nella metà dei casi Alice e Bob sceglieranno la stessa base di misura; quindi, i qubit correlati sono solo $n/2$. Per stabilire o escludere la presenza di Eve, vegono pubblicati la metà di questi. Quindi se il controllo della sicurezza va a buon fine, solo $n/4$ sono correlati e non pubblicati e possono essere usati come chiave criptografica. Quindi per avere una chiave crittografia sicura di m bit, è necessario usare in partenza $n = 4m$ qubit.

III — PROTOCOLLO EPR CON STATI ENTANGLED.

Nel 1991 Arthur Ekert propose un protocollo di crittografia quantistica che usa gli stati entangled. Questo protocollo è detto EPR dai nomi di Einstein-Poldosky e Rosen che discussero per la prima volta le proprietà degli stati entangled.

Il protocollo BB84 è intrinsecamente asimmetrico: Alice genera la chiave che poi, criptata, viene mandata a Bob. Inoltre all'atto della generazione della chiave c'è lo scambio di qubit (Alice manda i suoi qubit a Bob dopo averli criptati). Il protocollo EPR elimina queste due condizioni.

Supponiamo che Alice e Bob condividano n qubit entangled come

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{5.3.1}$$

Questi potrebbero essere, ad esempio, generati da Alice che poi ne manda la metà a Bob, vice versa, o addirittura potrebbe essere un operatore esterno addetto alla generazione.

Alice genera un bit random classico b e, a seconda del suo valore, misura il suo qubit nella base $B_1 = \{|0\rangle, |1\rangle\}$ o nella base $B_2 = \{|+\rangle, |-\rangle\}$. Supponiamo che il valore di questa misura sia a. Allo stesso modo, Bob genera un bit random classico b' e, a seconda del suo valore, misura nella base B_1 o B_2.

Supponiamo che il bit random di Alice sia $b = 0$ e che Alice misuri nella base B_1. Se misura 0 (cosa che capita) il 50% delle volte, il sistema collasserà nello stato $|00\rangle$. Se Bob estrae il numero $b' = 0$ e misura bella base B_1, il suo risultato sarà 0 il 100% delle volte. Allo stesso modo se Alice misura 1 il sistema collassa nello stato $|11\rangle$ e se $b' = 0$, Bob misurerà sempre 1. Ne consegue che se $b = b' = 0$ i qubit di Alice e Bob sono perfettamente correlati.

Supponiamo ora che Alice estragga il numero $b = 1$ e decida di misurare nella base B_2. Abbiamo che lo stato entangled può essere scritto come

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big[\frac{|+\rangle + |-\rangle}{\sqrt{2}} \otimes |0\rangle + \frac{|+\rangle - |-\rangle}{\sqrt{2}} \otimes |1\rangle\Big]. \tag{5.3.2}$$

Raccogliendo gli stati $|+\rangle$ e $|-\rangle$ abbiamo che

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big[|+\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} + |-\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big] = \frac{|++\rangle + |--\rangle}{\sqrt{2}}. \tag{5.3.3}$$

Seguendo il ragionamento precedente è chiaro che se Bob estrae $b' = 1$, le misure di Alice e Bob sono perfettamente correlate. Ovvvero, se il qubit di Alice collassa in $|\pm\rangle$ anche quello di Bob si troverà nello stato $|\pm\rangle$.

Concludiamo che se $b = b'$ (indipendentemente dallo specifico valore) le misure di Alice e Bob sono perfettamente correlate e quindi $a = a'$. Questi sono i bit che andranno a formare la chiave crittografica segreta.

I qubit per i quali $b \neq b'$ vengono scartati perchè statisticamente scorrelati. Infatti, supponiamo che Alice abbia $b = 0$ e $b' = 1$ e che la misura di Alice faccia collassare i qubit nello stato $|00\rangle$. Questo può essere scritto come

$$|00\rangle = |0\rangle \otimes \frac{|+\rangle + |-\rangle}{\sqrt{2}}. \tag{5.3.4}$$

É chiaro che una misura di Bob nella base B_2 darà la metà delle volte lo stato $|+\rangle$ e il risultato $a' = 0$ e la rimanente metà lo stato $|-\rangle$ e il risultato $a' = 1$. Quindi solo il la metà delle volte $a = a'$ e questi qubit non possono essere usati per costruire una chiave segreta. In maniera analoga, si può far vedere che è necessario scartare tutti i qubit per i quali $b \neq b'$.

É importante notare che il protocollo è completamente simmetrico. Non è importante ai fini del protocollo se la prima misura è fatta da Alice o Bob e, addirittura, le misure potrebbero essere simultanee.

In secondo luogo, la chiave è completamente random ed in questo caso è generata nel momento della misura. Infatti, è completamente indeterminata fino a quando Alice e Bob non misurano i qubit.

Terzo, anche questo protocollo crittografico è sicuro in presenza di Eve. Ci sono infatti tecniche che permettono di stabilire se i qubit sono statisticamente correlati o se hanno perso le correlazioni quantistiche a causa dell'intervento di Eve.