Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

IL PROTOCOLLO "BB84" PER LA DISTRIBUZIONE QUANTISTICA DELLE CHIAVI

Tesi di Laurea in Crittografia

Relatore:
Chiar.mo Prof.
DAVIDE ALIFFI

Presentata da:
VERONICA MALIZIA

Correlatore:
Chiar.mo Prof.
STEFANO MANCINI

I Sessione
Anno Accademico 2015/2016

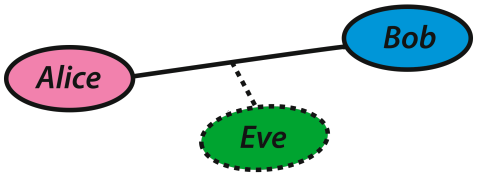
Al mio nonno matematico.

Indice

Introduzione

Il termine "crittografia" deriva dal greco ‘‘kryptó-s’’ che significa "nascosto" e ‘‘graphìa’’ che significa "scrittura"; con crittografia si intende un insieme di metodi, tecniche e algoritmi che consentono di trasformare un messaggio in modo da renderlo intellegibile solamente agli utenti legittimi, che condividono certe informazioni segrete riguardo al metodo tramite cui si è cifrato il messaggio. Ipotizziamo che due persone vogliano scambiarsi a distanza delle informazioni che devono restare riservate: chiamiamo Alice (il mittente) e Bob (il destinatario), gli utenti legittimi; Eve l'utente illegittimo o eavesdropper.

Se il canale di trasmissione non è sicuro (Eve) può cercare di intercettare il messaggio e decifrarlo (attacchi passivi) o, addirittura, di introdurre suoi messaggi nel canale e impersonare l'utente (attacchi attivi).



La maggior parte dei meccanismi crittografici comportano l'uso di chiavi, ovvero di stringhe di simboli (numeri) che servono per cifrare/decifrare il messaggio, note solo agli utenti legittimi. Storicamente, quando la crittografia si è tramutata da arte a scienza, ossia ha iniziato ad affrontare i problemi ad essa connessi in maniera analitica, con l'uso della matematica; è stato proposto un cifrario poi dimostratosi assolutamente sicuro, ma da esso originava il problema della distribuzione delle chiavi!
Infatti, tutte le tecniche risulteranno inefficienti se il metodo di distribuzione della chiave è un meccanismo debole.

Il primo capitolo prevede dunque un breve excursus sui più importanti cifrari della crittografia classica, focalizzando l'attenzione sul cifrario di Vernam del 1917, altrimenti noto come One Time Pad (OTP). La dimostrazione della sua sicurezza matematica, e dunque della sua inviolabilità definisce i punti del problema della distribuzione delle chiavi:

- necessità di una chiave lunga quanto tutto il messaggio ed utilizzata una sola volta;
- i simboli della chiave devono essere random;
- necessità di un canale sicuro per lo scambio della chiave tra Alice e Bob.

È come se Alice e Bob debbano condividere un segreto prima di scambiarsi un segreto!

Tale problema è stato affrontato nel corso del tempo nei modi più disparati (e disperati), andando dalle idee e dalle procedure ancora piuttosto semplici e acerbe della Crittografia Classica alle nuove prospettive offerte dalla Crittografia a Chiave Pubblica (si accennerà alla crittografia a chiave pubblica per mezzo del protocollo di Diffie ed Hellman), fino ad arrivare alla rivoluzione apportata nei recenti anni '80 dalla Crittografia Quantistica. Più propriamente nota con il nome di *Quantum Key Distribution (QKD)*, si tratta di un algoritmo basato sulle leggi della *Meccanica Quantistica* che risolve brillantemente il problema della distribuzione della chiave: permette di generare e scambiare chiavi segrete in modo assolutamente sicuro, dunque chiaramente preferibile a qualsivoglia sistema crittografico classico.

Il fine di questa tesi sarà quello di arrivare a formulare il problema della distribuzione delle chiavi e discutere la soluzione offerta dalla crittografia quantistica.

Il secondo capitolo della tesi fornisce dunque gli strumenti necessari per poter parlare di Meccanica Quantistica. Verranno enunciati i postulati che regolano i sistemi fisici quantistici, ai quali sono associati degli spazi di Hilbert $\mathcal{H}$ (che qui considereremo di dimensione finita); inoltre dei richiami di algebra lineare ci saranno utili per poter lavorare con operatori lineari su $\mathcal{H}$ e *prodotti tensoriali*. Protagonista del capitolo sarà il *Quantum Bit* (o brevemente *qubit*), ossia lo spazio su cui è definito il più semplice sistema quantistico; si tratta dello spazio di Hilbert $\mathbb{C}^2$ e costituisce la versione quantistica del bit classico.

Una volta in possesso dei fondamenti della teoria quantistica, nel terzo capitolo vedremo come quest'ultima ha permesso lo sviluppo della *Quantum Key Distribution (QKD)*, che sta attirando molta attenzione come potenziale meccanismo candidato a sostituire i metodi computazionali di distribuzione delle chiavi. Questo perché la QKD permette a due utenti legittimi di generare una chiave segreta, la cui sicurezza è garantita dalle leggi della fisica quantistica.
Presenteremo quindi il primo protocollo di distribuzione quantistica delle

chiavi introdotto da Bennet e Brassard - referenza [6, pag. 175-179] - nel 1984 (da cui il nome **BB84**), a partire da una bizzarra idea precedente di Wiesner circa banconote quantistiche non falsificabili. Esso risulterà essere il cuore di questa tesi. Analizzeremo la sua sicurezza rispetto ad un semplice attacco, sfruttando i teoremi di non-clonazione e di non-ortogonalità degli stati, enunciati e dimostrati nel capitolo 2. Infine dimostreremo, seppur in modo non rigoroso, la sicurezza incondizionata del BB84 usando dei teoremi di cui non riportiamo la dimostrazione.

Fino ad oggi, diversi protocolli di distribuzione quantistica delle chiavi sono stati sviluppati e alcuni di essi permettono di gestire la trasmissione delle chiavi attraverso decine di chilometri sia in fibra, sia nello spazio libero. Così, le reti LAN, presentano un grande interesse per l'uso della QKD, a causa delle aree di coperture limitate di queste ultime.

Capitolo 1

La distribuzione delle chiavi

In questo Capitolo iniziale introdurremo il concetto di *crittosistema*, che è alla base di tutti i protocolli crittografici (cifrari), e ne formalizzaremo la sicurezza facendo un breve excursus storico attraverso i cifrari più importanti. Focalizzeremo quindi l'attenzione sul problema della distribuzione delle chiavi nell'ambito della crittografia classica, poiché è proprio questo problema che è stato risolto con successo dalla crittografia quantistica di cui ci occuperemo nei Capitoli successivi.

1.1 Crittosistemi

Definiamo in dettaglio un crittosistema e il suo funzionamento:

Definizione 1. Un crittosistema è costituito dai seguenti elementi:

1. alfabeto $\mathcal{A}$
2. spazio dei messaggi $\mathcal{M}$ su $\mathcal{A}$ (e.g. $\mathcal{A}^n$)
3. spazio dei testi cifrati $\mathcal{C}$ su $\mathcal{A}$
4. spazio delle chiavi $\mathcal{K} \subset \mathbb{N}$
5. funzione di cifratura $E_k : \mathcal{A}^n \to \mathcal{A}^n$ con $k \in \mathcal{K}$
6. funzione di de-cifratura $D_{k'} : \mathcal{A}^n \to \mathcal{A}^n$ $(D_{k'} \equiv E_k^{-1})$ con $k' \in \mathcal{K}$

Se $k = k'$ il crittosistema si dice **simmetrico**; se $k \neq k'$ il crittosistema è **asimmetrico**.

Un semplice esempio è il cifrario di Cesare (II sec. d.C.):

- $\mathcal{A} = \{0, 1, \ldots, 25\}$
- $\mathcal{M} = \mathcal{A}$

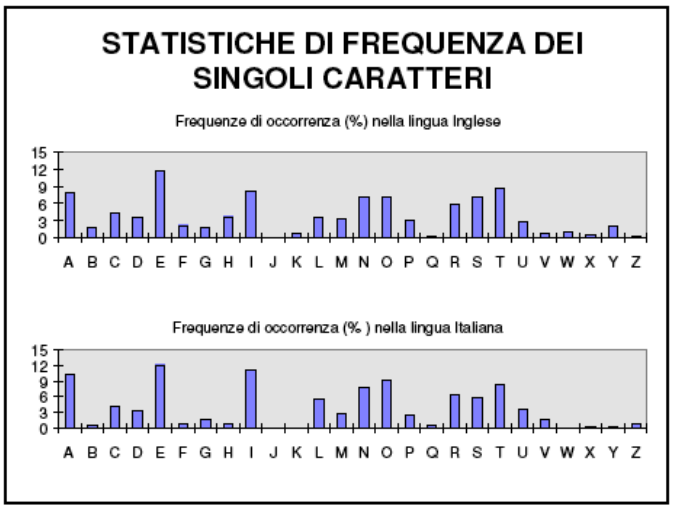


Figura 1.1: Statistiche di frequenza dei singoli caratteri nella lingua inglese ed in quella italiana.

- $\mathcal{C} = \mathcal{A}$
- $\mathcal{K} = \{1, \ldots, 25\}$
- $E_k : \mathcal{A} \to \mathcal{A}$ tale che $E_k(m) = m + k \ (mod\ 26) = c$
- $D_k : \mathcal{A} \to \mathcal{A}$ tale che $D_k(c) = c - k \ (mod\ 26) = m$

con $m, c \in \mathcal{A}$ rispettivamente testo in chiaro e messaggio cifrato e $k \in \mathcal{K}$ chiave di cifratura. Questo è un classico esempio di **cifrario monoalfabetico**. Lo spazio delle chiavi è molto limitato e un crittosistema simile può essere facilmente violato.

Si sono poi evoluti crittosistemi più sicuri, che lavorano non solo con permutazioni cicliche delle lettere dell'alfabeto, ma con ogni permutazione possibile; ad esempio:

- $\mathcal{K} = S_{26} = \{\sigma_1, \ldots, \sigma_t\}$, con $t = |\mathcal{A}|!$
- $E_k : \mathcal{A} \to \mathcal{A}$ tale che $E_k(m) = \sigma_k(m) = c$

dove σ_k è un permutazione su $\mathcal{A}$ dipendente da k ed ancora $m, c \in \mathcal{A}$.

Tuttavia, questo cifrario è facilmente violabile con un'indagine statistica sulle frequenze. Infatti in qualsiasi linguaggio, ogni lettera ha una sua frequenza caratteristica.

Osservando la figura 1.1 possiamo ad esempio supporre che in seguito ad un'analisi statistica, una lettera con frequenza alta provenga da una E,

sia per l'alfabeto inglese che per quello italiano, al contrario la lettera con frequenza più bassa provenga da una J nel caso della lingua inglese, e così via ...
Permutare un alfabeto significa dunque permutare l'istogramma delle frequenze dei singoli caratteri.

Si è cercato di ovviare a questo problema con il passaggio a **cifrari polialfabetici**, che utilizzano permutazioni su blocchi di testo di determinata lunghezza, piuttosto che su singole lettere:

- $\mathcal{K} = \{1, \ldots, (|\mathcal{A}|^b)! - 1\}$
- $E_k : \mathcal{A}^b \to \mathcal{A}^b$ tale che

$$E_k(m) = \sigma_k(m) = \sigma_{k_1}(m_1)\sigma_{k_2}(m_2)\ldots\sigma_{k_b}(m_b)$$
$$m \in \mathcal{A}^b, m_i \in \mathcal{A},\ k_i \in \{0, 1, \ldots, |\mathcal{A}|!\}$$

Esempio 1.

Testo in chiaro: $ARRIVANOIRINFORZI$
Chiave: $VERMEVERMEVERMEVE$
Testo cifrato: $VVIUZVRFUVDRWAVUM$

Definiamo innanzitutto una corrispondenza tra le lettere dell'alfabeto ed i numeri naturali, tale che $A = 0, B = 1, C = 2, \ldots$. Osserviamo poi che è stato diviso il testo in blocchi di lunghezza $b = 5$ pari alla lunghezza della chiave "VERME". Notiamo che le due R di ARRIVANO vengono cifrate la prima con una V e la seconda con una I, a differenza dei cifrari monoalfabetici che si rivelano deboli anche per questo motivo.
Ma le due A vengono invece cifrate con la stessa lettera, la V. Il motivo è evidente: le due A si trovano a cinque caratteri di distanza l'una dall'altra e cinque è proprio la lunghezza della chiave "verme"! Di fatto il codice si riduce qui a cinque codici di Cesare intercalati.

Ma anche questo crittosistema è violabile, proprio per via di questa debolezza! Ad esempio con il metodo Kasiski:
l'attacco si basa sul fatto che si trovano spesso sequenze identiche di caratteri a una certa distanza l'una dell'altra; questo può avvenire per il motivo esposto sopra. Si costruiscono dunque b messaggi prendendo una lettera ogni b dal messaggio originale ognuno dei quali è codificato con una singola permutazione σ_{k_i}. Se allora si individuano tutte le sequenze ripetute (e in un testo lungo o in più testi se ne troveranno molte) è pressoché certo che il massimo comun divisore tra le distanze tra sequenze identiche è la lunghezza

della chiave, o tutt'al più un suo multiplo.
Una volta nota la lunghezza n della chiave, sappiamo che la prima lettera di ogni blocco è cifrata con la stessa permutazione e così via, su ognuno dei b messaggi si applica l'indagine statistica.

Si intuisce che per aumentare la sicurezza si avrebbe bisogno di chiavi abbastanza lunghe da ostacolare l'analisi delle frequenze e che siano combinazioni casuali di lettere. Tuttavia la nozione di sicurezza va definita matematicamente.

1.2 Sicurezza di un crittosistema

Per formalizzare il concetto di sicurezza (inviolabilità) di un crittosistema abbiamo bisogno di elementari nozioni di teoria dell'informazione (faremo qui riferimento ai testi [1], [2], [3]).

Iniziamo ricordando che data una *variabile aleatoria* X definita su un alfabeto $\mathcal{X}$[1], con funzione di probabilità $p(x) = Pr\{X = x\}$, con $x \in \mathcal{X}$, il concetto di *informazione* è legato all'*incertezza* associata al valore assunto da X e può essere quantificato tramite l'entropia di Shannon.

Definizione 2. L'entropia (di Shannon) di una variabile aleatoria X, che assume valori $x \in \mathcal{X}$, con funzione di probabilità $p(x)$ è

$$H(X) := -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x) = \sum_{x\in\mathcal{X}} p(x)(\log_2 \frac{1}{p(x)}).$$

Possiamo anche esprimere l'entropia di Shannon come $H(\vec{p})$, dove $\vec{p} = (p(0), \ldots, p(n-1))$ è il vettore associato delle probabilità. L'entropia così definita ha le seguenti proprietà:

1. $0 \leq H(X) \leq 1$
2. $H(X)$ dipende dalle probabilità $(p(0), \ldots, p(n-1))$, dove $p(i) = Pr\{X = i\}$;
3. $H(X)$ è una funzione continua;
4. Se X ha n valori equiprobabili con $p = \frac{1}{n} \implies H(X) = \log_2 n$, **VALORE MASSIMO DI ENTROPIA**;
5. Concavità dell'entropia di Shannon:

$$H(\lambda p_X + (1-\lambda)p'_X) \geq \lambda H(p_X) + (1-\lambda)H(p'_X),\ \lambda \in [0,1].$$

[1] In questo elaborato si considereranno esclusivamente alfabeti discreti di cardinalità finita.

Entropia congiunta Consideriamo due variabili aleatorie X, Y, definite sugli alfabeti $\mathcal{X}, \mathcal{Y}$ con probabilità congiunta

$$p(x, y) = Pr\{X = x, Y = y\}$$

e le relative probabilità condizionate

$$p(x|y) = Pr\{X = x|Y = y\},$$

$$p(y|x) = Pr\{Y = y|X = x\},$$

sono vere le seguenti relazioni (*regole di Bayes*)

$$p(x, y) = p(x|y)p(y) \tag{1.1}$$

$$p(y, x) = p(y|x)p(x), \tag{1.2}$$

dove

$$p(x) = \sum_{y \in \mathcal{Y}} p(x, y),$$

$$p(y) = \sum_{x \in \mathcal{X}} p(x, y),$$

sono le cosiddette distribuzioni di probabilità *marginali*.
Le due variabili aleatorie X,Y si dicono **statisticamente indipendenti** se $p(x, y) = p(x)p(y)$, altrimenti sono correlate.

Definizione 3. Date due variabili aleatorie X, Y, definite sugli alfabeti $\mathcal{X}, \mathcal{Y}$ con probabilità congiunta $p(x, y)$, la loro entropia congiunta è

$$H(X, Y) := -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 p(x, y).$$

Vale la seguente proprietà (*subadditività*):

$$H(X, Y) \leq H(X) + H(Y),$$

con l'uguaglianza se e solo se le variabili sono indipendenti.

Entropia condizionata

Definizione 4. Date due variabili aleatorie X, Y, definite sugli alfabeti $\mathcal{X}, \mathcal{Y}$ con probabilità congiunta $p(x, y)$ e probabilità condizionata $p(x|y)$, l'entropia condizionata di Y rispetto a X è

$$H(Y|X) := \sum_{x \in \mathcal{X}} p(x) H(Y|X = x),$$

dove $H(Y|X = x) = -\sum_{y \in \mathcal{Y}} p(y|x) \log_2 p(y|x)$ è l'entropia di Shannon di Y per un certo valore fissato x di X.

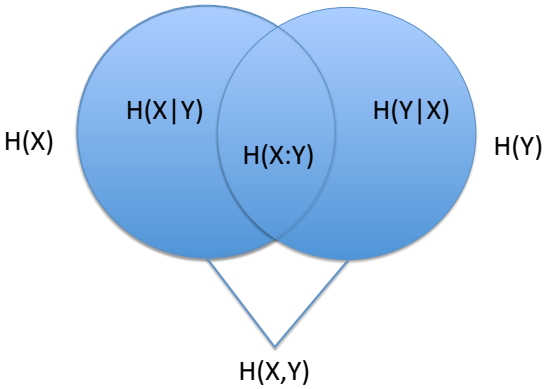


Figura 1.2: Diagramma di Venn indicante le varie entropie per due variabili aleatorie X ed Y.

Analogamente possiamo definire $H(X|Y)$.
L'entropia condizionata $H(Y|X)$ quantifica l'incertezza residua sulla variabile Y, conoscendo il valore x di X.

È facile constatare dalle definizioni che

$$H(X,Y) = H(Y|X) + H(X) \quad \text{e} \quad H(X,Y) = H(X|Y) + H(Y)$$

Risulta inoltre essere

$$H(Y|X) \leq H(Y),$$

con l'uguaglianza se e solo se le variabili sono indipendenti.

Sussiste poi la seguente proprietà: *regola della catena*

$$H(X,Y,Z) = H(X) + H(Y|X) + H(Z|X,Y)$$

Essa segue da

$$\begin{aligned} H(X,Y,Z) &= H(X,Y,Z) \\ &= H(X,Y,Z) + H(X) - H(X) + H(X,Y) - H(X,Y) \\ &= H(X) + H(Y|X) + H(Z|X,Y). \end{aligned}$$

Le relazioni di inclusione tra le varie entropie sono riassunte nella Fig.1.2.
Possiamo ora definire la *sicurezza perfetta* di un crittosistema.

Definizione 5. Un crittosistema ha *sicurezza perfetta* se $H(m|c) = H(m)$ (o $Pr(m|c) = Pr(m)$), con m e c valori delle variabili aleatorie M e C definite rispettivamente su $\mathcal{M}$ e $\mathcal{C}$.

In altre parole nessun vantaggio circa m può derivare ad Eve dalla conoscenza di c. In pratica questo significa anche che le variabili M e C devono essere indipendenti, infatti usando al regola di Bayes (1.1) si ha

$$Pr(m, c) = Pr(m|c)Pr(c) = Pr(m)Pr(c).$$

Da ciò consegue anche che per ogni c il valore $Pr(c = E_k(m)) \equiv Pr(c|m)$ è costante sugli m.

Teorema 1.1. *Se un cifrario ha sicurezza perfetta, allora* $|K| \geq |\mathcal{M}|$.

Dimostrazione. Sia m un messaggio e c la sua versione cifrata rispetto ad una qualche chiave k. Dunque $Pr(c = E_k(m)) > 0$. Se il crittosistema ammette più messaggi che chiavi possiamo trovare m' tale che $m' \neq D_k(c)$ per ogni $k \in \mathcal{K}$ e quindi $Pr(c = E_k(m')) = 0$. Ma questo contraddice l'ipotesi di perfezione perchè si ottiene $Pr(c = E_k(m)) \neq Pr(c = E_k(m'))$, i.e. la probabilità di ottenere c non è costante sui messaggi. Segue che ci devono essere almeno tante chiavi quanti messaggi. □

Teorema 1.2 (Teorema di Shannon)**.** *Un cifrario ha sicurezza perfetta se e solo se ogni chiave è utilizzata con probabilità uniforme* $\frac{1}{|\mathcal{K}|}$ *e per ogni* $x \in \mathcal{M}$ *e* $y \in \mathcal{C}$*, esiste un unica chiave* k *tale che* $E_k(x) = y$.

1.3 Cifrario di Vernam

Il cifrario di Vernam è un cifrario simmetrico a blocchi proposto da Gilbert S. Vernam nel 1917. Vediamone nel dettaglio il funzionamento:

Si definiscono:

- un alfabeto $\mathcal{A}$, ad esempio $\mathcal{A} = \{0, 1\} \cong \mathbb{Z}_2$;
- n: lunghezza del blocco;
- $\mathcal{M} = \mathcal{A}^n$, insieme dei testi in chiaro;
- $\mathcal{C} = \mathcal{A}^n$, insieme dei testi cifrati;
- $\mathcal{K} = \mathcal{A}^n$, spazio delle chiavi.

$\forall k \in \mathcal{K}$ la funzione di cifratura è:

$$E_k : \mathcal{A}^n \to \mathcal{A}^n \quad \text{tale che} \quad E_k(m) = c = m + k \ (mod\ 2)$$

segue la funzione di decifrazione:

$$D_k : \mathcal{A}^n \to \mathcal{A}^n \quad \text{tale che} \quad D_k(c) = m = c - k \ (mod\ 2)$$

La condizione importante è che la chiave $k \in \mathcal{A}^n$ viene scelta in maniera random, è lunga quanto tutto il testo e viene utilizzata una sola volta (da cui anche il nome **OTP**, **O**ne **T**ime **P**ad). Queste caratteristiche rendono il cifrario di Vernam **un sistema inviolabile**.

Teorema 1.3 (Shannon, 1949)**.** *OTP ha sicurezza perfetta.*

Dimostrazione. $\mathcal{A} = \{0,1\}$, n: lunghezza del blocco, $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$
$\forall k \in \mathcal{K}$ si ha $Pr(k) = \frac{1}{2^n}$ e

$\forall c \in \mathcal{C}$ si ha $Pr(c) = \frac{1}{2^n}$.

Allora $H(k) = H(c) = \log_2 2^n = n$.

Osserviamo ora che $H(m,k,c) = H(m,k)$ e $H(m,k,c) = H(m,c)$, poichè fissato il testo in chiaro l'incertezza sul testo cifrato è uguale a quella sulle chiavi, i.e. $H(c) = H(k)$ e utilizziamo le relazioni

$$\begin{cases} H(m,k) = H(m) + H(k) & (m \text{ e } k \text{ sono indipendenti}); \\ H(m,c) = H(m|c) + H(c) \end{cases}$$

Uguagliando otteniamo $H(m|c) = H(m)$. □

Ricapitolando allora le caratteristiche del cifrario di Vernam:

- la chiave deve essere lunga quanto il messaggio ed utilizzata una sola volta
- la chiave deve essere random
- la chiave deve essere prima condivisa tra Alice e Bob

Tuttavia, pur trattandosi di un sistema perfettamente sicuro, le proprietà sopra elencate rappresentano degli inconvenienti che rendono il cifrario di Vernam praticamente inutilizzabile; si avrebbe infatti bisogno di chiavi troppo grandi e di un canale sicuro per lo scambio di esse tra Alice e Bob.

1.4 La crittografia a chiave pubblica

Una possibile soluzione al problema della distribuzione delle chiavi è data dalla crittografia a chiave pubblica.
Per semplicitÃ qui ci limiteremo a discutere solo il protocollo che è stato

storicamente il primo a chiave pubblica, tuttavia ne esistono poi molti altri. In "New Directions in Cryptography", 1976, W. Diffie e M. Hellman introducono l'idea di crittografia (asimmetrica) a chiave pubblica: la funzione cifrante deve essere nota a tutti, essa però è difficile da invertire, ossia è difficile decifrare senza la conoscenza di una chiave privata.
Il protocollo prevede che se Alice e Bob vogliono condividere una chiave k, allora:

1. Alice e Bob si accordano su un primo N (grande) e su un generatore g di $\mathbb{Z}_N^*$;
2. N e g vengono resi pubblici;
3. Alice sceglie un intero random $x \in \{1, \ldots, N-2\}$ e invia a Bob $u = g^x \ (mod\ N)$;
4. Bob sceglie un intero random $y \in \{1, \ldots, N-2\}$ e invia ad Alice $v = g^y \ (mod\ N)$;
5. Alice calcola $v^x \ (mod\ N) = g^{yx} \ (mod\ N)$;
6. Bob calcola $u^y \ (mod\ N) = g^{xy} \ (mod\ N)$.

Adesso Alice e Bob possegono la stessa chiave $k = g^{xy}$ e possono comunicare con essa su un cifrario simmetrico.
Eve, per conoscere k, dovrebbe calcolare $x = \log_g u \ (mod\ N)$ oppure $y = \log_g v \ (mod\ N)$. La sicurezza di questo protocollo risiede proprio nella **difficoltà computazionale** del calcolo del *logaritmo discreto*: i passi necessari per il calcolo del logaritmo cresce in modo non polinomiale rispetto alla lunghezza dell'input ($\log_N$).

1.4.1 Complessità computazionale

Diciamo che un algoritmo è *efficiente* se termina in un numero di passi polinomiale rispetto alla lunghezza dell'input, mentre consideriamo *inefficienti* quegli algoritmi con complessità computazionale maggiore, ad esempio quelli che necessitano di un numero di operazioni esponenziale rispetto alla lunghezza dell'input. Questa definizione è dovuta a EDMONDS-COOK-KARP.

Definizione 6. Un algoritmo $\mathfrak{A}$ si dice **polinomiale** se esiste un polinomio $poly(n)$ tale che $\forall x \in \{0,1\}^*$, $\mathfrak{A}(x)$ termina in un numero di passi minore o uguale a $poly(l)$, dove l indica la lunghezza della stringa x.

La classe dei problemi che hanno un algoritmo di soluzione che lavora in un tempo polinomiale, viene denotata P. Si chiama invece NP la classe dei problemi che ammettono un algoritmo rapido di verifica delle soluzioni, nel senso che adesso spieghiamo.

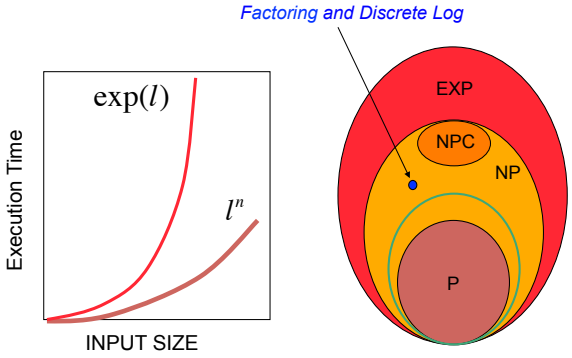


Figura 1.3: Relazione tra la lunghezza dell'input e il tempo di esecuzione di un algortimo (sinistra). Relazione tra le principali classi di complessità computazionale (destra).

Ammettiamo per semplicità che il nostro problema preveda una risposta del tipo *sì* o *no*. Allora diciamo che il problema sta in NP esattamente quando, per ogni input w, esso ha risposta *sì* se e solo se si può trovare una qualche testimonianza y che sa confermarlo in tempi rapidi ed è breve da scriversi. Il confronto tra le due classi P e NP è dunque, una comparazione tra i tempi di dimostrazione e di verifica della soluzione dei problemi matematici o riconducibili a modelli matematici. Chiaramente

$$P \subseteq NP$$

perché ogni algoritmo (rapido) di soluzione costituisce implicitamente anche una verifica.

In conclusione, come si vede in Fig. 1.3, non sono noti algoritmi efficienti per il calcolo dei logaritmi discreti. Essi fanno parte della classe di problemi NP. Esistono algoritmi sofisticati, generalmente ispirati da simili algoritmi per la fattorizzazione degli interi, ma nessuno ha tempo di esecuzione polinomiale.

Un cifrario deve essere praticamente, se non matematicamente, indecifrabile.

Questo è il primo dei sei principi enunciati da Kerckhoffs nel suo celebre articolo del 1883 *La cryptographie militaire*. Esso riassume molto bene il

concetto di **sicurezza computazionale**: non è necessario che uno schema sia perfettamente sicuro, ma è sufficiente che non venga violato in un tempo ragionevole e con una ragionevole probabilità di successo.
Abbiamo quindi due sostanziali differenze rispetto alla nozione di sicurezza perfetta:

1. La sicurezza viene preservata solamente contro avversari efficienti, che agiscono in un tempo polinomiale;

2. Gli avversari possono potenzialmente avere successo, ma con una bassissima probabilità.

Capitolo 2

Cenni di meccanica quantistica

Questo capitolo si occuperà di fornire le nozioni base della meccanica quantistica.
Essa è la teoria fisica più completa che si ha a disposizione al momento. Si fonda su alcuni postulati che descrivono il comportamento dei sistemi fisici. Le conseguenze di questi postulati sono spesso controintuitive.

2.1 I postulati della meccanica quantistica

Prima di formulare i Postulati, introduciamo la notazione di Dirac [Dirac, 1958]. Considereremo solo spazi di Hilbert di dimensione finita $\mathcal{H} \simeq \mathbb{C}^n$.
Indichiamo i vettori colonna con $|\psi\rangle$ (*Ket*) mentre con $\langle\psi|$ (*Bra*) si intende il rispettivo trasposto coniugato.
Per esempio, la base ortonormale $\{|e_1\rangle, |e_2\rangle\}$ può essere espressa come $\{(1,0)^T, (0,1)^T\}$ e una qualsiasi combinazione lineare di $|e_1\rangle$ e $|e_2\rangle$, $a|e_1\rangle + b|e_2\rangle$, può essere scritta $(a,b)^T$. La scelta dell'ordine dei vettori della base è arbitraria.

Dati due vettori $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, il loro prodotto scalare è indicato con $\langle\phi|\psi\rangle$; se i vettori hanno norma unitaria vale che $\langle\psi|\psi\rangle = 1$.
Per esempio, dati i vettori della base canonica ortonormale di $\mathcal{H}^{\in}$, $\{|0\rangle, |1\rangle\}$, si ha $\langle 0|0\rangle = 1$ e, poiché sono anche ortogonali tra loro $\langle 0|1\rangle = 0$.

Introduciamo gli operatori lineari su $\mathcal{H}$.

Definizione 7. Un operatore lineare A è una trasformazione $A : \mathcal{H} \longrightarrow \mathcal{H}$[1], tale che

$$A(a|\psi_1\rangle + b|\psi_2\rangle) = aA|\psi_1\rangle + bA|\psi_2\rangle,$$

per ogni $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ e per ogni $a, b \in \mathbb{C}$.

[1] Qui consideriamo semplicemente operatori tra spazi identici. Tutte le nozioni possono essere facilmente estese ad operatori tra spazi differenti.

Dati due vettori $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, la notazione $|\phi\rangle\langle\psi|$ rappresenta invece il prodotto esterno di $|\phi\rangle$ e $\langle\psi|$, che risulta un operatore lineare. Infatti

$$(|\phi\rangle\langle\psi|)|v\rangle = (\langle\psi \,|\, v\rangle)|\phi\rangle = |\phi\rangle\langle\psi \,|\, v\rangle .$$

Per esempio, $|0\rangle\langle 1|$ è la trasformazione che manda $|1\rangle$ in $|0\rangle$ e $|0\rangle$ in $(0,0)^T$:

$$|0\rangle\langle 1|\,|1\rangle = |0\rangle\langle 1 \,|\, 1\rangle = |0\rangle$$
$$|0\rangle\langle 1|\,|0\rangle = |0\rangle\langle 1 \,|\, 0\rangle = 0\,|0\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Equivalentemente, $|0\rangle\langle 1|$ può essere scritto in forma matriciale dove $|0\rangle = (1,0)^T$, $\langle 0| = (1,0)$, $|1\rangle = (0,1)^T$, $\langle 1| = (0,1)$. Allora

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0,1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

È sempre possibile specificare le trasformazioni sugli stati in termini di ciò che accade sui vettori della base.
Generalizzando, sia $\{|e_i\rangle\}_{i=1}^n$ una base ortonormale di $\mathcal{H}$, quindi dato $|\psi\rangle \in \mathcal{H}$, possiamo scrivere $|\psi\rangle = \sum_i \psi_i |e_i\rangle$ con $\psi_i = \langle e_i \,|\, \psi\rangle \in \mathbb{C}$, allora si ha

$$\left(\sum_{i=1}^n |e_i\rangle\langle e_i|\right)|\psi\rangle = \sum_{i=1}^n \psi_i |e_i\rangle , \qquad \forall\, |\psi\rangle \in \mathcal{H}$$

che implica la seguente relazione

$$\sum_{i=1}^n |e_i\rangle\langle e_i| = I.$$

Come conseguenza, dato $A : \mathcal{H} \longrightarrow \mathcal{H}$ lineare, si ha

$$A = \sum_{i=1}^n |e_i\rangle\langle e_i| \, A \sum_{j=1}^n |e_j\rangle\langle e_j|$$
$$= \sum_{i,j=1}^n \langle e_i \,|\, A \,|\, e_j\rangle \, |e_i\rangle\langle e_j|$$

con $A_{ij} := \langle e_i \,|\, A \,|\, e_j\rangle$ coefficienti della matrice $n \times n$ associata ad A rispetto alla base canonica $\{|e_i\rangle\}_{i=1}^n$.
Il **proiettore** sul sottospazio $\mathcal{K} \subset \mathcal{H}$ generato da $\{|e_i\rangle\}_{i=1}^k$, $k < n$, è dato da

$$P_{\mathcal{K}} = \sum_{i=1}^k |e_i\rangle\langle e_i| \tag{2.1}$$

e soddisfa $P_{\mathcal{K}}^2 = P_{\mathcal{K}}$.

Postulato 2.1. *Ad un sistema fisico isolato è associato uno spazio degli stati che è rappresentato da uno spazio di Hilbert $\mathcal{H}$. Gli stati del sistema sono esattamente i vettori $|\psi\rangle$ di tale spazio (normalizzati ad 1).*

Postulato 2.2. *Lo spazio degli stati di un sistema fisico composito è il prodotto tensoriale $\otimes$ degli spazi degli stati dei suoi sottosistemi.*

Postulato 2.3. *I cambiamenti di stato di un sistema fisico isolato con uno spazio di Hilbert $\mathcal{H}$ associato, sono descritti da trasformazioni unitarie*

$$\begin{aligned} U :&\mathcal{H} \longrightarrow \mathcal{H} \\ &|\psi\rangle \mapsto \left|\psi'\right\rangle = U\,|\psi\rangle \end{aligned}$$

con $UU^\dagger = U^\dagger U = I$, dato $U^\dagger$ l'operatore aggiunto di U e I l'operatore identità su $\mathcal{H}$

Postulato 2.4. *Gli osservabili sono operatori autoaggiunti sullo spazio degli stati $\mathcal{H}$, i.e. $A : \mathcal{H} \longrightarrow \mathcal{H}$, tale che $A = A^\dagger$.*
La misura di un osservabile ha come possibili risultati i suoi autovalori $\{a_j\}_j (a_j \in \mathbb{R})$.
La probabilità di ottenere come risultato uno specifico autovalore a_j, sapendo che il sistema era nello stato $|\psi\rangle$, è

$$Pr(a_j) = \langle\psi \,|\, P_j \,|\, \psi\rangle\,,$$

con $P_j = |a_j\rangle\langle a_j|$ il proiettore (2.1) *sul sottospazio dell'autovettore $|a_j\rangle$ di A, corrispondente all'autovalore a_j.*
L'effetto della misura è una proiezione

$$|\psi\rangle \to \left|\psi'\right\rangle = \frac{P_j\,|\psi\rangle}{\langle\psi \,|\, P_j \,|\, \psi\rangle^{\frac{1}{2}}}.$$

Osserviamo che il valore atteso della misura di A quando il sistema si trova nello stato $|\psi\rangle$ è

$$\mathbb{E}(A) \equiv \langle A\rangle = \sum_j Pr(a_j) a_j = \langle\psi \,|\, A\psi\rangle\,.$$

2.2 Il Quantum Bit

Il più semplice sistema quantistico è quello definito sullo spazio di Hilbert $\mathbb{C}^2$. Ad esso è stato dato il nome di *quantum bit* (S. Wisner 1969-1983, B. Schumacher 1995).[2] Il *quantum bit* (o brevemente *qubit*) è lo spazio degli

[2] Contrariamente a quanto si possa pensare esso non deriva dal considerare la versione quantistica del bit, ma da *cubito*, con l'intenzione di considerarlo come un'unità di misura di informazione quantistica.

stati $\mathbb{C}^2$ e costituisce la versione quantistica del bit classico, spazio degli stati $\mathbb{F}_2$.
Su questo spazio definiamo la base canonica

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.2}$$

Dunque, un generico stato è descritto dal vettore

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.3}$$

con α e $\beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$.

Una visualizzazione utile di un qubit si può ottenere mediante un'interpretazione geometrica che associa gli stati di un qubit ai punti sulla superficie di una sfera di raggio unitario. Il polo sud della sfera corrisponde a $|1\rangle$ e il polo nord a $|0\rangle$. Le altre locazioni sono le sovrapposizioni quantistiche di 0 e 1. Questa sfera è nota come **la sfera di Bloch** ed è rappresentata in Figura 2.1.

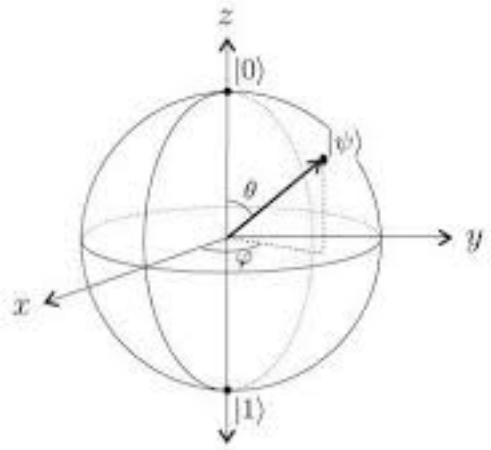


Figura 2.1: La sfera di Bloch.

Esiste una corrispondenza biunivoca tra un generico stato di un qubit

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

e un punto sulla sfera unitaria in $\mathbb{R}^3$ rappresentato come

$$\cos\Big(\frac{\theta}{2}\Big)\,|0\rangle + e^{i\varphi}\sin\Big(\frac{\theta}{2}\Big)\,|1\rangle\,,$$

dove $\theta \in [0, \pi]$ e $\varphi \in [0, 2\pi]$.
Per vedere questa corrispondenza ricordiamo che in un qubit $|\psi\rangle = \alpha\,|0\rangle +$

$\beta\,|1\rangle$, i valori α e β sono numeri complessi tali che $|\alpha|^2 + |\beta|^2 = 1$. Usando la descrizione di α e β in coordinate polari possiamo scrivere $|\psi\rangle$ come

$$|\psi\rangle = r_0 e^{i\phi_0}\,|0\rangle + r_1 e^{i\phi_1}\,|1\rangle\,,$$

con $r_0^2 + r_1^2 = 1$, equazione che descrive i punti della circonferenza unitaria in $\mathbb{R}^2$.
Possiamo quindi rappresentare i moduli di α e β mediante l'angolo ρ, ponendo

$$r_0 = \cos(\rho) \quad \text{e} \quad r_1 = \sin(\rho).$$

Ponendo $\rho = \frac{\theta}{2}$, otteniamo l'espressione

$$|\psi\rangle = \cos\Big(\frac{\theta}{2}\Big)e^{i\phi_0}\,|0\rangle + \sin\Big(\frac{\theta}{2}\Big)e^{i\phi_1}\,|1\rangle$$

con $0 \le \theta \le \pi$, o equivalentemente

$$|\psi\rangle = e^{i\gamma}\Big(\cos\Big(\frac{\theta}{2}\Big)\,|0\rangle + e^{i\varphi}\sin\Big(\frac{\theta}{2}\Big)\,|1\rangle\Big)$$

con $\varphi = \phi_1 - \phi_0$ e $\gamma = \phi_0$, $0 \le \varphi \le 2\pi$.

Da un punto di vista fisico il fattore $e^{i\gamma}$ (detto fase globale), si può ignorare in quanto non ha effetti osservabili, cioè dal punto di vista osservazionale i due stati $e^{i\gamma}\,|\psi\rangle$ e $|\psi\rangle$ sono identici (dal principio di misurazione quantistica). Notiamo infine che l'angolo sferico θ che un punto sulla sfera unitaria in $\mathbb{R}^3$ forma con l'asse z, soddisfa esattamente la stessa condizione $0 \le \theta \le \pi$ dell'angolo θ nella rappresentazione del qubit $\cos\big(\frac{\theta}{2}\big)\,|0\rangle + e^{i\varphi}\sin\big(\frac{\theta}{2}\big)\,|1\rangle$. Anche l'angolo φ in questa rappresentazione varia nello stesso intervallo $0 \le \varphi \le 2\pi$ dell'angolo che la proiezione di un vettore unitario nella sfera di Bloch sul piano (x, y) forma con l'asse x.

Quindi esiste effettivamente una corrispondenza biunivoca tra i qubit rappresentati come $\cos\Big(\frac{\theta}{2}\Big)\,|0\rangle + e^{i\varphi}\sin\Big(\frac{\theta}{2}\Big)\,|1\rangle$ e i punti sulla sfera di Bloch.

2.2.1 Osservabili rilevanti per un qubit

Nello spazio $\mathbb{C}^2$ introduciamo gli *operatori di Pauli* definiti come

$$X := |0\rangle\langle 1| + |1\rangle\langle 0|\,, \quad Y := -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|\,, \quad Z := |0\rangle\langle 0| - |1\rangle\langle 1|\,.$$

X, Y, Z insieme all'operatore identità I, costituiscono una base per lo spazio $\mathcal{L}(\mathbb{C}^2)$ delle applicazioni lineari su $\mathbb{C}^2$. Segue la rapprentazione in forma matriciale degli operatori di Pauli rispetto alla base canonica (2.2) :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Osserviamo dunque che

- Z è tale che $Z|0\rangle = |0\rangle$ e $Z|1\rangle = -|1\rangle$, quindi $\{|0\rangle, |1\rangle\}$ è detta base Z con rispettivi autovalori $\{+1, -1\}$;
- X è tale che $X|+\rangle = |+\rangle$ e $X|-\rangle = -|-\rangle$, quindi $\{|+\rangle, |-\rangle\}$ è detta base X con rispettivi autovalori $\{+1, -1\}$, dove

$$\Big\{|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big\};$$

- Y, tale che $Y = iXZ$.

Si ha che misurare un osservabile, considerando il sistema in un generico stato (2.3), significa dunque trasformare tale stato, in maniera probabilistica, in uno degli autostati dell'osservabile. La trasformazione non è unitaria, ma è il risultato di un proiettore (2.1).

Partendo da un generico stato $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$,
sia $Z := |0\rangle\langle 0| - |1\rangle\langle 1|$; calcoliamo la misura di Z su $|0\rangle$ e $|1\rangle$ come accennato sopra:

$$\begin{aligned} Z\,|0\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\,|0\rangle \\ &= |0\rangle\langle 0\,|\,0\rangle - |1\rangle\langle 1\,|\,0\rangle \\ &= |0\rangle \end{aligned} \qquad \begin{aligned} Z\,|1\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\,|1\rangle \\ &= |0\rangle\langle 0\,|\,1\rangle - |1\rangle\langle 1\,|\,1\rangle \\ &= -\,|1\rangle \end{aligned}$$

Allora Z proietta su $|0\rangle$ con probabilità $Pr = |\alpha|^2$ e su $|1\rangle$ con probabilità $Pr = |\beta|^2$.
Analogamente sia $X := |0\rangle\langle 1| + |1\rangle\langle 0|$, possiamo anche scriverlo come $X := |+\rangle\langle +| - |-\rangle\langle -|$; calcoliamo la misura di X sulla rispettiva base $\{|+\rangle, |-\rangle\}$:

$$\begin{aligned} X\,|+\rangle &= (\,|+\rangle\langle +| - |-\rangle\langle -|\,)\,|+\rangle \\ &= (\,|+\rangle\langle +\,|\,+\rangle\,) - (\,|-\rangle\langle -\,|\,+\rangle\,) \\ &= |+\rangle \end{aligned} \qquad \begin{aligned} X\,|-\rangle &= (\,|+\rangle\langle +| - |-\rangle\langle -|\,)\,|-\rangle \\ &= (\,|+\rangle\langle +\,|\,-\rangle\,) - (\,|-\rangle\langle -\,|\,-\rangle\,) \\ &= -\,|-\rangle \end{aligned}$$

La misura di X proietta con probabilità $Pr = \frac{|\alpha+\beta|^2}{2}$ su $|+\rangle$ e con probabilità $Pr = \frac{|\alpha-\beta|^2}{2}$ su $|-\rangle$.

2.3 Entanglement

In accordo con il Postulato 2.2 lo spazio degli stati per due qubits sarà $\mathbb{C}^2 \otimes \mathbb{C}^2$. Considerando la base canonica $\{|0\rangle, |1\rangle\}$ di ciascun qubit, il suddetto spazio avrà come base $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$, che può essere scritta in modo più compatto come $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Pertanto in $\mathbb{C}^2 \otimes \mathbb{C}^2$ possiamo avere ad esempio lo stato $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. La peculiarità di tale stato è che non si può assegnare ad ognuno dei sottosistemi

(ognuno dei due qubit) un preciso stato, come per esempio accade nel caso $|00\rangle$ (dove il primo qubit è nello stato $|0\rangle$ ed il secondo analogamente è nello stato $|0\rangle$).

In altre parole non riusciamo a trovare a_1, a_2, b_1, b_2 tali che

$$(a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) = |00\rangle + |11\rangle ,$$

poiché

$$(a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

e $a_1 b_2 = 0$ implica che anche $a_1 a_2 = 0$ oppure $b_1 b_2 = 0$. Gli stati di un sistema complesso che non riusciamo a scrivere come prodotto tensoriale di stati delle singole componenti, sono chiamati ***entangled***.

Definizione 8. Dato un sistema bipartito AB con associato spazio degli stati $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, gli stati $|\Psi_{AB}\rangle \in \mathcal{H}_{AB}$ che possono essere scritti come $|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$ con $|\Psi_A\rangle \in \mathcal{H}_A$ e $|\Psi_B\rangle \in \mathcal{H}_B$ sono definiti **fattorizzabili**.
Gli stati $|\Psi_{AB}\rangle \in \mathcal{H}_{\mathcal{AB}}$ che invece **non** sono fattorizzabili, i.e. $\mathcal{H}_{\mathcal{AB}} \neq \mathcal{H}_A \otimes \mathcal{H}_B$ e $|\Psi_{AB}\rangle \neq |\Psi_A\rangle \otimes |\Psi_B\rangle$ per qualsiasi $|\Psi_A\rangle \in \mathcal{H}_A$ e $|\Psi_B\rangle \in \mathcal{H}_B$, sono definiti **entangled**.

In pratica se un sistema bipartito è in uno stato entangled non si può assegnare uno stato ben preciso ad ognuno dei sottosistemi (come accade invece nel caso di stato fattorizzabile). Gli stati entangled comportano delle forti correlazioni tra i sottosistemi. Ciò può essere visto con un semplice esempio. Supponiamo di avere due qubit nello stato

$$|\Psi_A\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle |0_A\rangle + |1_A\rangle |1_A\rangle) .$$

La misura dell'osservabile Z_A darà come risultato l'autovalore $+1$ (rispettivamente -1) con $Pr = 1/2$ (rispettivamente $Pr = 1/2$). In tal caso si può arguire che la ipotetica misura di Z_B darebbe con certezza risultato $+1$ (rispettivamente -1).

I membri di una collezione entangled non hanno un proprio stato individuale, solo l'intera collezione possiede uno stato ben definito. Gli stati entangled si comportano come se fossero strettamente connessi l'uno all'altro indipendentemente dalla distanza che li separa.

2.4 No cloning

Nella fisica classica, è sempre possibile costruire una *copia* dello stato di un sistema fisico. A tal fine, consideriamo la permutazione $\pi : \mathbb{F}_d \times \mathbb{F}_d \to \mathbb{F}_d \times \mathbb{F}_d$ tale che

$$(x, y) \to \pi(x, y) = \big(x, (x \oplus y)\big); \qquad (x, y) \in \mathbb{F}_d \times \mathbb{F}_d.$$

Semplicemente scegliendo $y = 0$, la mappa precedente restituisce una copia di x qualsiasi sia il suo valore. Dal punto di vista quantistico invece, non è possibile elaborare una trasformazione di copiatura che valga in modo *universale* per qualunque stato in input.

Definizione 9. Dato uno spazio di Hilbert $\mathcal{H}$, un *operatore di copiatura universale* è una trasformazione unitaria $U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ tale che, fissato un $|\alpha\rangle \in \mathcal{H}$,

$$U |\psi\rangle |\alpha\rangle = |\psi\rangle |\psi\rangle , \qquad \forall |\psi\rangle \in \mathcal{H}.$$

In generale, l'impossibilità di copiare uno spazio degli stati è una proprietà dei sistemi quantistici nota come teorema del *no cloning*:

Teorema 2.5. *Per i sistemi quantistici non esiste un operatore di copiatura universale.*

Dimostrazione. Supponiamo che una tale trasformazione U esista. Allora consideriamo $|\psi_1\rangle , |\psi_2\rangle \in \mathcal{H}$ e abbiamo

$$\begin{aligned} U |\psi_1\rangle |\alpha\rangle &= |\psi_1\rangle |\psi_1\rangle , \\ U |\psi_2\rangle |\alpha\rangle &= |\psi_2\rangle |\psi_2\rangle . \end{aligned}$$

Calcoliamo il prodotto scalare dei membri a sinistra e lo eguagliamo al prodotto scalare dei membri a destra:

$$\langle\alpha| \langle\psi_1| U^\dagger U |\psi_2\rangle |\alpha\rangle = \langle\psi_1| \langle\psi_1 | \psi_2\rangle |\psi_2\rangle ,$$

Per definizione di operatore unitario di U, si ha $U^\dagger U = I$, otteniamo

$$\begin{aligned} \langle\alpha | \alpha\rangle \langle\psi_1 | \psi_2\rangle &= | \langle\psi_1 | \psi_2\rangle |^2, \\ \langle\psi_1 | \psi_2\rangle &= | \langle\psi_1 | \psi_2\rangle |^2. \end{aligned}$$

L'ultima equazione si verifica solo quando $\langle\psi_1 | \psi_2\rangle = 1$, i.e. i due vettori coincidono, oppure quando $\langle\psi_1 | \psi_2\rangle = 0$, ossia i due vettori sono ortogonali. □

2.5 Guadagno di informazione implica Disturbo

Nella fisica classica è sempre possibile misurare un sistema fisico (dunque ottenere informazioni su esso), senza disturbarlo. Conseguenza di ciò, sarà sempre possibile distinguere perfettamente tra due stati. Nella meccanica quantistica le cose sono differenti.

Teorema 2.6. *Dati due stati* $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ *tali che* $\langle\psi_1 \,|\, \psi_2\rangle \neq 0, 1$*, non è possibile distinguere perfettamente (i.e. con zero errori) tra essi attraverso il procedimento di misura.*

Dimostrazione. Essendo $|\psi_1\rangle, |\psi_2\rangle$ due stati **non ortogonali**, essi non possono essere autovettori di uno stesso osservabile (operatore autoaggiunto) corrispondenti ad autovalori differenti. Dunque non possono essere distinti con perfezione. □

Corollario 2.7. *Qualsiasi tentativo di distinguere tra* $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$*, tali che* $\langle\psi_1 \,|\, \psi_2\rangle \neq 0, 1$*, implica un disturbo.*

Dimostrazione. Supponiamo di aggiungere un secondo sistema quantistico e applicare una trasformazione unitaria globale sui due sistemi. Questo secondo sistema gioca il ruolo di strumento di misura.
Consideriamo il suo spazio di Hilbert $\mathcal{H}_\mathcal{M}$ e prendiamo uno stato $|u\rangle \in \mathcal{H}_\mathcal{M}$. Allora, sia $U : \mathcal{H} \otimes \mathcal{H}_\mathcal{M} \to \mathcal{H} \otimes \mathcal{H}_\mathcal{M}$, si ha:

$$|\psi_1\rangle |u\rangle \to U |\psi_1\rangle |u\rangle = |\psi_1\rangle |v_1\rangle ,$$
$$|\psi_2\rangle |u\rangle \to U |\psi_2\rangle |u\rangle = |\psi_2\rangle |v_2\rangle ,$$

con $|v_1\rangle \neq |v_2\rangle$. In questo modo, per ottenere le etichette 1 o 2, possiamo allora eseguire una misura sul sistema $\mathcal{H}_\mathcal{M}$ senza perturbare il sistema originario ($|\psi 1\rangle |v_1\rangle$ sono stati fattorizzabili). Tuttavia, procedendo come nella dimostrazione del Teorema 2.5 arriviamo a

$$\langle\psi_1 \,|\, \psi_2\rangle = \langle\psi_1 \,|\, \psi_2\rangle \langle v_1 \,|\, v_2\rangle .$$

L'ultima equazione implica che o $|\psi_1\rangle$ e $|\psi_2\rangle$ sono ortogonali, oppure $\langle v_1 \,|\, v_2\rangle = 1$, il che significa $|v_1\rangle = |v_2\rangle$. □

Attualmente, l'unico caso in cui è possibile distinguere perfettamente tra due stati senza perturbarli è quello di due stati ortogonali.

2.6 Interpretazione fisica

La descrizione astratta di un qubit come un vettore in uno spazio bi- dimensionale complesso ha un corrispondente nel mondo reale. In particolare, un

qualsiasi sistema fisico con almeno due livelli di energia discreti e sufficientemente separati è un candidato appropriato per rappresentare un qubit. Per realizzare fisicamente un qubit i tre approcci più comuni sono quelli basati su:

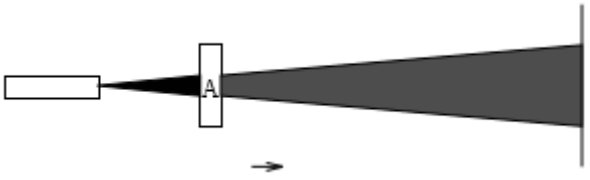
- le due diverse polarizzazione di un fotone;
- l'allineamento di uno spin nucleare in un campo magnetico uniforme;
- due livelli di energia[3] di un elettrone che orbita in un singolo atomo.

2.6.1 Polarizzazione di un fotone

I fotoni sono le uniche particelle che possiamo osservare direttamente. Lo "stato di polarizzazione" è una proprietà che la luce presenta sia nella sua rappresentazione elettromagnetica (ad onde) che nella sua rappresentazione ad intensità (numero di fotoni): è quindi un dato caratteristico fondamentale della luce e dei suoi costituenti fondamentali: i fotoni.
In generale i fotoni si propagano con un comportamento isotropo, cioè in tutte le direzioni, questo moto è coerente con un moto elicoidale. Invece se studiamo un raggio polarizzato, le sue onde di propagazione sono orientate su un piano, quindi se parliamo di polarizzazione di un fotone, vuol dire che il suo moto è disposto su un piano.
Il seguente semplice esperimento dimostra alcuni dei postulati della meccanica quantistica attraverso i fotoni e la loro polarizzazione.

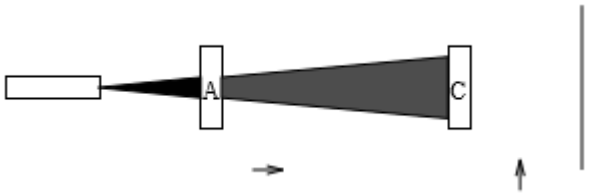
Un fascio di luce viene proiettato su uno schermo. I filtri A, B, C sono polarizzati rispettivamente, orizzontalmente, a 45° e verticalmente; vengono posizionati in modo da intersecare il fascio di luce.

Senza alcun filtro l'intensità del fascio proiettato è del 100%. Posizioniamo in primis, il filtro A. Assumendo che la luce proveniente dalla sorgente sia polarizzata in modo random, ossia che ogni singolo fotone abbia polarizzazione uniformemente casuale, il numero di fotoni che raggiunge il rivelatore è dimezzato: il filtro assorbe il 50% dei fotoni. I fotoni uscenti saranno polarizzati orizzontalmente.

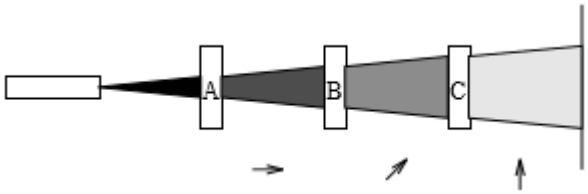


[3]In un atomo i livelli di energia dei vari elettroni sono discreti. Due di essi possono essere selezionati per rappresentare i valori logici 0 e 1. Questi livelli corrispondono a specifici stati di eccitazione degli elettroni nell'atomo.

Inseriamo ora il filtro C ed osserviamo che l'intensità della luce in output scende a zero. Nessuno dei fotoni polarizzato orizzontalmente riesce ad attraversare il filtro verticale.



Infine, dopo aver inserito il filtro B tra il filtro A e il filtro C, osserviamo che una piccola quantità di luce sarà visibile sullo schermo, esattamente un ottavo della sorgente iniziale.



Questo effetto si discosta dall'esperienza classica, secondo cui l'aggiunta di un filtro può solo far diminuire il numero di fotoni che raggiungono lo schermo. Come spiegare invece questa crescita?

Una polarizzazione arbitraria può essere espressa come una combinazione lineare $a\,|0\rangle + b\,|1\rangle$ dei vettori della base $|0\rangle$ (con cui indichiamo una polarizzazione verticale) e $|1\rangle$ (polarizzazione orizzontale); dove a e b sono numeri complessi tali che $|a|^2 + |b|^2 = 1$. Osserviamo che la scelta della base per questa rappresentazione è del tutto arbitraria.
Scriviamo un generico stato $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. In accordo con il postulato 2.4 sulla misura, scelto per esempio l'osservabile Z come strumento di misurazione, lo stato viene proiettato su $|0\rangle$ con probabilità $|a|^2$ e su $|1\rangle$ con probabilità $|b|^2$. Dunque nel primo caso lo stato $|\psi\rangle$ viene cambiato in $|0\rangle$ e la seconda misurazione rispetto alla stessa base restituirà $|0\rangle$ con probabilità 1. La misura cambia lo stato e non è possibile determinare quale fosse lo stato di partenza.
Focalizzandoci in particolare sull'esperimento, l'azione del filtro A può essere descritta come la misura di Z tale per cui se si ottiene il risultato $+1$ il fotone viene respinto, mentre se si ottiene il risultato -1 viene lasciato passare. Il viceversa corrisponde al filtro C. Se guardiamo all'azione dei filtri solo su ciò che passa, questo può essere descritto mediante i proiettori $|1\rangle\langle 1|$ e $|0\rangle\langle 0|$.
Segue che, i fotoni che dopo essere stati misurati dal filtro, combaciano con

la polarizzazione di esso, riescono ad attraversarlo. Gli altri vengono riflessi ed assumono una polarizzazione perpendicolare a quella del filtro.

Assumendo che i fotoni provenienti dalla sorgente abbiano polarizzazione random, il filtro A misurerà il 50% di essi come orizzontalmente polarizzati. Questi fotoni attraverseranno il filtro e saranno tutti nello stato $|1\rangle$. In seguito, il filtro C misurerà tali fotoni facendo emergere solo quelli che hanno componente lungo $|0\rangle$; ma lo stato $|1\rangle = 0\,|0\rangle + 1\,|1\rangle$ verrà proiettato su $|0\rangle$ con probabilità 0, dunque nessun fotone passerà attraverso C.

Infine, il filtro B misura lo stato dei fotoni rispetto alla base

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\},$$

che che abbiamo denotato con $\{|+\rangle, |-\rangle\}$ (con tali vettori indichiamo la polarizzazione a $\pm 45°$).
Osserviamo che $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$ e $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$. Per costruzione di B, passano attraverso il filtro quei fotoni che hanno componente non nulla lungo $|+\rangle$. Dunque, i fotoni che passano attraverso A, quindi polarizzati orizzontalmente, saranno proiettati da B su $|+\rangle$ con probabilità $\frac{1}{2}$, perciò il 50% dei fotoni che hanno attraversato A, passeranno per il filtro B e saranno nello stato $|+\rangle$. Come prima, questi fotoni saranno proiettati dal filtro C su $|0\rangle$ con probabilità $\frac{1}{2}$. In seguito a questo procedimento, otteniamo che solo un ottavo dei fotoni di partenza riescono a passare attraverso la sequenza di filtri A, B e C.

2.7 Bits vs Qubits

In conclusione riassumiamo e compariamo in questa sezione le proprietà dei bits e dei qubits.

- Lo spazio degli stati per un bit è $\mathbb{F}_2$.
  Lo spazio degli stati per un qubit è $\mathbb{C}^2$, con gli stati della base canonica $\{|z\rangle\}_{z\in\mathbb{F}_2}$ corrispondenti agli stati del bit.

- Lo spazio degli stati per n bits è $\mathbb{F}_2^n$.
  Lo spazio degli stati per n qubits è $\mathbb{C}^{2\otimes n} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^n}_{nvolte}$, con gli stati della base canonica $\{|z\rangle\}_{z\in\mathbb{F}_2^n}$ corrispondenti agli stati degli n bits. In caso di stati entangled non possiamo assegnare un preciso stato ad ogni qubit.

- Le operazioni su un bit sono descritti dalle permutazioni $\pi : \mathbb{F}_2 \to \mathbb{F}_2$.
  Le operazioni su un qubit sono descritte da operatori unitari $U : \mathbb{C}^2 \to \mathbb{C}^2$.

- Dato uno stato $z \in \mathbb{F}_2$ relativo ad un bit, la misura dell'unico osservabile restituisce (con certezza) z e lascia lo stato imperturbato.
  Dato uno stato bidimensionale $\sum_{z\in\mathbb{F}_2} c_z \left|z\right\rangle$, la misura dell'osservabile Z (ci sono altri infiniti osservabili) restituisce $z \in \mathbb{F}_2$ con probabilità $Pr(z) = |c_z|^2$ e proietta lo stato su $\left|z\right\rangle$. Perciò non c'è possibiltà di ricostruire lo stato di un qubit dalla misura di un singolo osservabile.

Capitolo 3

La distribuzione quantistica delle chiavi

In questo capitolo vedremo come la teoria quantistica fornisce un'alternativa alla crittografia a chiave pubblica per risolvere il problema della distribuzione delle chiavi.
Cosa ancor più importante, tale alternativa risulterà avere una sicurezza incondizionale, a fronte della semplice sicurezza computazionale.
Ci riferiamo d'ora in avanti alla *distribuzione quantistica delle chiavi* con QKD, acronimo di *quantum key distribution.*

3.1 Il protocollo BB84

Il primo protocollo di distribuzione quantistica delle chiavi fu descritto da C. H. Bennett e G. Brassard nel 1984 e fu chiamato "protocollo BB84". Analizziamone il funzionamento.

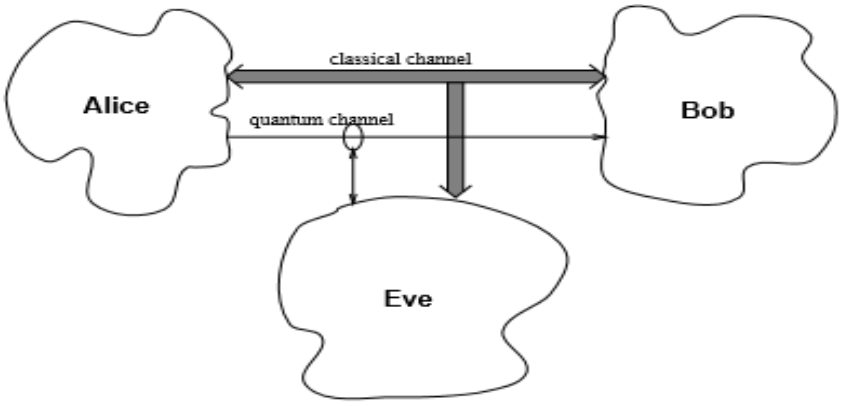


Figura 3.1: Schema del funzionamento di BB84

In primis specifichiamo che la comunicazione tra Alice e Bob avviene in questo caso, attraverso due canali: *un canale quantistico* unidirezionale, mezzo su cui viaggiano i qubits e attaccabile da Eve, e *un canale classico*, che è pubblico ma non modificabile, ovvero tutti possono ascoltare ma non modificare l'informazione ivi trasmessa. Tale situazione è illustrata nella Figura 3.1:

Per iniziare il processo, Alice darà il via ad una prima fase di **codifica**:

- Alice decide una base, ad esempio Z[1], ed associa il valore '0' (rispettivamente '1') del bit classico allo stato quantistico $|0\rangle$ (rispettivamente allo stato $|1\rangle$);
- Alice seleziona in maniera *random* tra $|0\rangle$ e $|1\rangle$ lo stato del qubit da inviare a Bob attraverso un canale quantistico, che si assume poter essere attaccabile da un avversario. Questa procedura viene ripetuta un certo numero 2ℓ di volte. Tuttavia, se Alice inviasse a Bob dei qubits in questo modo, la comunicazione non sarebbe sicura. Infatti, un potenziale avversario potrebbe misurare rispetto alla base Z il qubit che sta viaggiando, apprenderne l'informazione codificata (valore del bit) e inoltrare il qubit a Bob senza averlo alterato in alcun modo.
- Allora Alice aggiunge un espediente alla sua codifica. Lei associa l'informazione classica '0' ad uno stato scelto in modo *random* tra $|0\rangle$, autovettore di Z e $|+\rangle$, autovettore di X; analogamente associa l'informazione classica '1' ad uno stato scelto in modo *random* tra $|1\rangle$, autovettore di Z e $|-\rangle$, autovettore di X.

Segue la seconda fase di **decodifica**, eseguita da Bob:

- Bob decide, ancora una volta in modo *random*, se misurare l'osservabile Z o X, quindi se proiettare sulla base Z o X.
- Quando la scelta della base di misura di Bob coincide con quella della base di codifica di Alice (ad esempio, entrambi utilizzano Z), il valore misurato deve essere lo stesso, mentre laddove utilizzano basi differenti, non c'è correlazione tra il suo risultato e la scelta originaria di Alice; in questo caso, il valore ottenuto dovrebbe essere scartato.

Il risultato è costituito da due stringhe di 2ℓ bits (una nelle mani di Alice ed una nelle mani di Bob) i cui valori, in assenza di eavesdropper, saranno identici nelle istanze in cui Alice e Bob hanno utilizzato la stessa base e completamente scorrelati altrove. La situazione è riassunta nella seguente Tabella: 3.1.

[1]In questo capitolo, per brevità ci riferiremo alla base Z, (rispettivamente X) come la base degli autostati di Z (rispettivamente di X).

Alice basis	Encoding	q-ch	Bob basis	Bob result	Decoding	public-ch
Z	$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	Z	$\|0\rangle$, Pr $= 1$	0	OK
			X	$\|+\rangle$, Pr $= 1/2$	0	-
			X	$\|-\rangle$, Pr $= 1/2$	1	-
Z	$1 \leftrightarrow \|1\rangle$	$\rightsquigarrow$	Z	$\|1\rangle$, Pr $= 1$	1	OK
			X	$\|+\rangle$, Pr $= 1/2$	0	-
			X	$\|-\rangle$, Pr $= 1/2$	1	-
X	$0 \leftrightarrow \|+\rangle$	$\rightsquigarrow$	Z	$\|0\rangle$, Pr $= 1/2$	0	-
			Z	$\|1\rangle$, Pr $= 1/2$	1	-
			X	$\|+\rangle$, Pr $= 1$	0	OK
X	$1 \leftrightarrow \|-\rangle$	$\rightsquigarrow$	Z	$\|0\rangle$, Pr $= 1/2$	0	-
			Z	$\|1\rangle$, Pr $= 1/2$	1	-
			X	$\|-\rangle$, Pr $= 1$	1	OK

Tabella 3.1: Tabella riassuntiva BB84

Si osserva dalla tabella, che ogniqualvolta le basi scelte da Alice e Bob coincidono, anche le stringhe di bits sono uguali, come spiegato sopra; nel caso in cui le basi utilizzate da Alice e Bob sono differenti, i risultati corrispondenti sono inutilizzabili e dovrebbero essere scartati.

Come possono gli utenti legittimi decidere quale dato mantenere e quale scartare? Dunque riuscire a sapere quando le basi di preparazione e misura coincidono?

Alice e Bob utilizzano il canale classico per eseguire la procedura di *key-sifting*, in cui entrambi comunicano la loro scelta riguardo la base (e non riguardo agli stati!) pubblicamente. Discutendo dunque sul canale classico, Alice e Bob si accordano sull'eliminare tutti quei casi in cui essi non hanno utilizzato la stessa base. Questa procedura è anche chiamata *riconciliazione delle basi*.
Se 2ℓ è molto grande è lecito attendersi che Alice e Bob dopo tale procedura condividano una chiave di ℓ bits (ad ogni istanza del protocollo BB84 le basi coincidono con $Pr = 1/2$.).

Ma in particolare, cosa si guadagna con la distribuzione quantistica delle chiavi?
Innanzitutto notiamo che gli stati utilizzati (autovettori di X e Z) sono *non ortogonali*; ciò comporta che Eve non ha possibilità di copiarli perfettamente o misurarli senza alterarli (Vedi le sottosezione "No cloning" (2.4) e "Guadagno d'informazione implica Disturbo" (2.5)).

Pertanto risulterà impossibile rubare informazione senza che gli utenti legittimi se ne accorgano.

Infatti, se Alice e Bob, una volta eseguito il key-sifting, sacrificano alcuni bit della chiave che hanno ottenuto pubblicandone i valori sul canale classico, si aspettano per essi valori perfettamente coincidenti. Vediamo cosa succede in presenza di Eve, i.e. analizziamo la sicurezza per il protocollo BB84.

3.2 Intercept resending

Il più semplice tipo di attacco è il cosiddetto *Intercept-Resend*, in cui Eve esegue una misura su ogni singolo qubit inviato da Alice e poi lo invia a Bob nello stato risultante dalla misurazione. Poiché Eve non è a conoscenza della base con cui è stato codificato il valore del bit classico da Alice, ella sceglie in maniera *random* la base su cui misurare.
Se la scelta coincide con la base di codifica, Eve riesce ad ottenere il corretto valore codificato da Alice, senza perturbare lo stato del qubit ed in seguito inviare quindi lo stato corretto a Bob. In questo caso il suo intervento risulta essere perfettamente trasparente.

D'altra parte, se Eve sceglie una base che non coincide con quella di codifica, il valore del bit che ottiene dalla misurazione è casuale e lo stato da inviare a Bob risulterà alterato rispetto a quello inviato da Alice.
Dopodiché se Bob misura la stessa base scelta da Alice, anche lui otterrà un risultato casuale (poiché Eve gli ha inviato uno stato codificato con la base opposta). Avrà quindi il 50% di possibilità di ottenere un esito erroneo (invece di ottenere il risultato corretto, come nel caso in cui non ci fosse stata la presenza dell'avversario).
La tabella 3.2 sottostante presenta un esempio di questo tipo di attacco:

Alice	q-ch	Eve	Eve result	q-ch	Bob	Bob result	Pr
$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	$Z,\ \Pr = 1/2$	$\|0\rangle,\ \Pr = 1$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1$	$1/2$
		$X,\ \Pr = 1/2$	$\|+\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1/2$	$1/8$
			$\|+\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \Pr = 1/2$	$1/8$
		$X,\ \Pr = 1/2$	$\|-\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1/2$	$1/8$
			$\|-\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \Pr = 1/2$	$1/8$

Tabella 3.2: Attacco *Intercept-Resend*

La probabilità che Eve scelga la base scorretta è del 50% (tenendo conto che Alice sceglie la base in modo random), se Bob misura la stessa base con cui Alice aveva codificato il qubit intercettato da Eve, egli ottiene un risultato casuale, i.e. un esito erroneo con la probabilità del 50%. Dunque la probabilità che un qubit intercettato, generi un errore nella stringa delle chiavi è del $50\% \times 50\% = 25\%$.
Se Alice e Bob confrontano pubblicamente n bits della chiave, la probabilità

che questi n bits della chiave passino il check su di un canale pubblico (siano dunque concordi) è pari a

$$Pr = \left(\frac{3}{4}\right)^n \overset{n\to\infty}{\longrightarrow} 0.$$

Passando al caso complementare, la probabilità che loro determinino una discordanza e quindi scoprano la presenza di Eve, è pari a

$$Pr = 1 - \left(\frac{3}{4}\right)^n \overset{n\to\infty}{\longrightarrow} 1$$

Ad esempio, per individuare un avversario con probabilità $Pr = 0.999999999$ Alice e Bob hanno bisogno di confrontare $n = 72$ bits della chiave, che è un numero relativamente esiguo.

La conclusione molto importante che si evince da questo tipo di attacco è che l'avversario può essere sempre scoperto!
Sembrerebbe però che non appena Alice e Bob riscontrino dei valori discordanti di bits debbano abortire il protocollo. Invero la discordanza dei valori di alcuni bits della chiave potrebbe anche nascere da errori casuali che intervengono nella trasmissione e non necessariamente originare dall'intervento malizioso di un avversario. È quindi di fondamentale importanza avere una soglia non nulla di errore tollerabile. Inoltre è altrettanto importante poter derivare tale soglia per il più potente attacco che Eve può realizzare. Questi due aspetti vengono affrontati nella prossima sezione.

3.3 Sicurezza Incondizionata

In questa sezione utilizzeremo alcuni **teoremi** per mostrare (seppur in maniera non rigorosa) la sicurezza incondizionata del protocollo BB84 e derivare la soglia massima di errore tollerabile nelle chiavi.

Iniziamo con il definire il rate di errore.

Definizione 10. Il rate di errore è chiamato "Quantum Bit Error Rate" (QBER) ed è definito come

$$QBER = \frac{n.\,dei\,bits\,errati\,sifted - key}{n.\,dei\,bits\,totali\,sifted - key} \tag{3.1}$$

Per stimare Q, come già detto in precedenza, Alice e Bob sacrificano alcuni bits della sifted-key e confrontano i loro valori attraverso il canale classico. Il numero di tali bits da confrontare rispetto al numero totale di bits della sifted-key può essere stimato grazie al seguente teorema.

Teorema 3.1. *Per ogni $\delta > 0$, la probabilità di ottenere meno di δn errori sul check dei bits e più di $(\delta + \epsilon)n$ errori sui rimanenti n bits non testati, è asintoticamente meno di $\exp[-O(\epsilon^2 n)]$ per n grande.*

Per stabilire una soglia per il rumore Q (3.1) al di sotto della quale, Alice e Bob possano arrivare a condividere una chiave perfettamente segreta, mentre al di sopra della quale debbano abortire il protocollo, facciamo ricorso al seguentel teorema:

Teorema 3.2 (Csiszar-Korner, 1978)**.** *Data una distribuzione di probabilità congiunta $p(A, B, E)$ per variabili random A, B, E, nelle mani di Alice, Bob e Eve rispettivamente, Alice e Bob possono distillare una chiave perfettamente segreta, se e solo se*

$$H(A:B) \geq H(A:E) \qquad \text{o} \qquad H(A:B) \geq H(B:E).$$

dove $H(\bullet:\bullet)$ rappresenta l'entropia mutua ed è tale che $H(A:B) = H(A) - H(A|B)$.

Le entropie mutue del teorema 3.2 dipendono dal tipo di attacco.
La **sicurezza incondizionata** è quella contro una tipologia di attacchi, detti *attacchi coerenti*. Il nostro obbiettivo è quello di ricavare la soglia massima di sicurezza, relativa al BB84, per gli attacchi coerenti, che le attuali conoscenze a riguardo, hanno posto a $Q_{coh} = 11\%$.
Facciamo ricorso al seguente teorema.

Teorema 3.3 (Teorema di Hall (1985))**.** *Siano E e B due osservabili in uno spazio di Hilbert N-dimensionale. Siano e, b, $|e\rangle$, $|b\rangle$ i corrispondenti autovalori ed autovettori, allora*[2]

$$H(A:B) + H(A:E) \leq 2\log_2 \left[N \max_{e,b} |\langle e|b\rangle| \right]$$

In modo più intuitivo, questo teorema afferma che se Eve fa una misura su di un sistema preparato da Alice, ottenendo informazione $H(A:E)$, allora l'informazione che otterrà Bob da una eventuale sua misura è necessariamente limitata. Esempi di E e B possono essere proprio gli operatori Z e X di Pauli.

L'attacco più distruttivo di Eve che possiamo immaginare è quello in cui supponiamo che Eve conosca in anticipo le basi utilizzate da Alice! Infatti se Eve conosce le basi, può semplicemente misurare i qubits nelle basi corrette ed ottenere tutta l'informazione generata da Alice, senza perturbare gli stati che arriveranno poi a Bob.
Assumiamo allora che le basi utilizzate da Alice e Bob (e conosciute da

[2]Per semplicità indichiamo con la stessa lettera sia l'osservabile che la variabile random ad esso corrispondente tramite il processo di misura quantistica.

Eve) in una comunicazione su BB84 di n qubits, siano date dalla seguente sequenza casuale:

$$\underbrace{XZZXZXZXXZ\ldots XZZXZ}_{n-volte}.$$

Siccome Eve conosce in anticipo le basi ciò è equivalente ad utilizzare la sequenza più semplice

$$\underbrace{XXXXXXXXXX\ldots XXXX}_{n-volte}.$$

In questo caso riusciamo a calcolare il valore $c = \max_{e,b} |\langle e|b\rangle|$ dato dal teorema di Hall 3.3.

Se $A = B = E = X^{\otimes n}$, la quantità c è:

$$\begin{aligned} c &= \max_{e,b}(|\langle e|b\rangle|) \\ &= \max_{e,b}(|\langle x_1|\langle x_2|\ldots\langle x_n|x_1\rangle|x_2\rangle\ldots|x_n\rangle|) = 1 \end{aligned}$$

Allora dal teorema di Hall 3.3 si ha:

$$H(A:B) + H(A:E) \leq 2\log_2 N = 2\log_2 2^n = 2n \tag{3.2}$$

dove $N = 2^n$ è la dimensione dello spazio di Hilbert relativo agli n qubits inviati da Alice.

Facciamo ora questa considerazione: lo scenario in cui Eve conosce la sequenza di basi esatte equivale a quello in cui conosce la sequenza di basi sbagliate, quindi $A = B = X^{\otimes n}$ e $E = Z^{\otimes n}$. Infatti se Eve conosce tutte le basi sbagliate ha soltanto bisogno di scambiare ogni base X con una Z e ottenere la sequenza di basi corrette.

Dato ciò, calcoliamo di nuovo il limite c quando Eve conosce tutte le basi sbagliate. In questo caso, l'osservabile E di Eve è dato da:

$$E = \underbrace{ZZZ\ldots Z}_{n-volte};$$

mentre le variabili A e B di Alice e Bob sono come prima (Bob conosce la sequenza corretta delle basi, in seguito alla procedura di riconciliazione delle basi del BB84):

$$A = B = \underbrace{XXX\ldots X}_{n-volte}.$$

La quantità c è:

$$\begin{aligned} c &= \max_{e,b}(|\langle e|b\rangle|) \\ &= \max_{e,b}(|\langle z_1|\langle z_2|\ldots\langle z_n \,|\, x_1\rangle|x_2\rangle\ldots|x_n\rangle|) \\ &= \max_{e,b}(|\langle z_1 \,|\, x_1\rangle\langle z_2 \,|\, x_2\rangle\ldots\langle z_n \,|\, x_n\rangle|) \\ &= \Big(\frac{1}{\sqrt{2}}\Big)^n = 2^{-\frac{n}{2}} \end{aligned}$$

Dunque il teorema di Hall 3.3 diventa:

$$\begin{aligned} H(A:B) + H(A:E) \leq 2\log_2(N2^{-\frac{n}{2}}) = \\ = 2\log_2\big(2^n 2^{-\frac{n}{2}}\big) \\ = 2\log_2\big(2^{\frac{n}{2}}\big) \\ = n \end{aligned} \tag{3.3}$$

Allora abbiamo un nuovo limite sull'informazione mutua che non è insignificante: la somma dell'informazione mutua di Alice e Bob e dell'informazione di Eve riguardo la sequenza di n qubits, non può essere maggiore di n.
Questo significa che se un bit di informazione è stato catturato da Eve, allora Bob deve avere una perdita sull'informazione, pari a quel bit. Non può accadere che entrmbi Eve e Bob condividano un bit di informazione riguardo la codifica di Alice.

Banalmente quando è vero la seconda disuguaglianza (3.3) (sequenza di basi sbagliate), è vera anche $H(A:B) + H(A:E) \leq 2n$ (3.2) (sequenza di basi corrette). Questo significa che se vogliamo fornire una disuguaglianza sempre vera sull'informazione di Eve, dobbiamo utilizzare l'Eq. (3.3).

Data l'Eq. (3.3), vediamo facilmente che:

$$H(A:E) \leq n - H(A:B).$$

Inoltre, considerando che la variabile A è caratterizzata da una stringa di n valori binari indipendenti ed identicamente distribuiti con $Pr(0) = Pr(1) = 1/2$, si ha

$$H(A:B) = n[1 - H(Q)],$$

dove Q è il rate di errore (3.1)

Esse comportano

$$H(A:B) \geq H(A:E)$$

quando

$$n[1 - H(Q)] \geq n - H(A:B) = n - n + nH(Q) = nH(Q).$$

Seguono una serie di implicazioni:

$$\begin{aligned} n - nH(Q) &\geq nH(Q) \\ n[1 - 2H(Q)] &\geq 0 \\ H(Q) &\leq \frac{1}{2} \\ Q &\leq 11\% \end{aligned}$$

Questa è la soglia definitiva di sicurezza per il protocollo BB84: se il rumore sul canale è più alto dell'11%, Alice e Bob devono interrompere il protocollo, mentre se è minore di tale valore, essi possono facilmente distillare una chiave in seguito al teorema di Csiszar-Korner 3.2.

Conclusioni

In conclusione, abbiamo visto che la *crittografia quantistica* si basa su idee che hanno origine dalla *Fisica quantistica*. Il contributo di questa disciplina alla crittografia è duplice e di segno contrastante: distruttivo, in un certo senso; costruttivo in un altro.

Gli sviluppi della Fisica quantistica rendono, infatti, teoricamente possibile la creazione di un computer di tipo completamente diverso e innovativo rispetto a quelli classici, il cosiddetto *computer quantistico*. Se realizzato in pratica, sarebbe in grado di effettuare in tempo *polinomiale* calcoli svolti da un computer classico in tempo *esponenziale*. Questo renderebbe vulnerabile ogni attuale sistema crittografico, mettendo in serio pericolo sistemi di sicurezza civili, militari, bancari ecc.
D'altro canto, le stesse idee su cui poggia il concetto di computer quantistico portano a concepire e realizzare sistemi crittografici quantistici assolutamente inattaccabili, anche da un eventuale computer quantistico, con la sorprendente capacità di scoprire se eventuali malintenzionati hanno solo tentato (anche senza riuscirvi del tutto) di intromettersi abusivamente in una comunicazione riservata.

La Fisica quantistica, sviluppatasi nel secolo scorso, è la branca più recente della Fisica. Parte dall'osservazione che le leggi della Fisica classica prevalentemente deterministiche, valide per la spiegazione dei fenomeni macroscopici, non sembrano potersi applicare con successo ai fenomeni microscopici. Si è trattato, da parte dei fisici, di concepire modi completamente nuovi, talvolta apparentemente bizzarri, contrari alla naturale intuizione e spesso controversi, di guardare ai fenomeni che riguardano il microscopico. In aggiunta, per la trattazione dei fenomeni in questione, si sono costruiti dei modelli matematici assai raffinati che giocano un ruolo basilare nella crittografia quantistica.
Il futuro è ormai cominciato. La teoria, se non la pratica, dei computer quantistici è già sviluppata. Inoltre sono già disponibili, sebbene per ora solo su piccola scala, efficaci sistemi crittografici quantistici.

In questa tesi si è voluto vedere come la meccanica quantistica offra soluzioni in ambito crittografico all'annoso problema della distribuzione delle chiavi.
Si è discusso in particolare, facendo uso della teoria quantistica, il *protocollo*

BB84, cuore centrale della tesi. Si tratta del primo protocollo di distribuzione quantistica delle chiavi, descritto da Bennet e Brassard nel 1984 (dai suoi autori e dall'anno di pubblicazione prende il suo nome). Nostro obbiettivo è stato quello di dimostrare attraverso questo protocollo, come la crittografia quantistica fornisce un'alternativa alla crittografia a chiave pubblica per risolvere il problema della distribuzione delle chiavi. Tale problema era stato enunciato nel Primo Capitolo, in cui dopo un rapido excursus storico sui diversi crittosistemi, abbiamo voluto far luce sui limiti della crittografia classica che hanno dato modo di elaborare e sviluppare delle possibili alternative quantistiche.
Cosa ancor più importante è stata lo studio della *sicurezza incondizionata* del protocollo BB84, a fronte della semplice sicurezza computazionale.
La dimostrazione di sicurezza incondizionata è stata completata solo intorno al 2000 (referenza [6]).

Quella presentata in questo elaborato è una versione non rigorosa basata sui teoremi di Csiszár-Körner e di Hall (referenze [8], [9]). L'idea principale è quella di sfruttare una sorta di relazione entropica di indeterminazione.
La conclusione molto importante della distribuzione quantistica delle chiavi, in seguito allo studio della sicurezza, è che un eventuale avversario può sempre essere scoperto!

Sebbene la QKD garantisca la sicurezza incondizionata, si fanno sempre comunque delle assunzioni, e.g. Alice e Bob hanno un controllo completo dei loro dispositivi (solo il canale quantistico è attaccabile); la dimensione dello spazio di Hilbert è nota esattamente. Alla luce di ciò, sviluppi futuri riguardano quindi:

- Sicurezza indipendente dai dispositivi (idealmente la sicurezza dovrebbe essere basata solo su caratteristiche testabili, e.g. la statistica degli eventi).

- Teorie post-quantum (ovvero teorie in cui sono contemplate modifiche alla corrente versione della meccanica quantistica).

- Sicurezza non solo "asintotica" ma anche per chiavi di lunghezza finita.

La crittografia quantistica è annoverata da "Technology Review" (un magazine innovativo e digitale, che scrive sulle più importanti tecnologie ed innovazioni, già dal 1899), come una delle dieci future tecnologie che rivoluzioneranno la nostra vita.
Recenti dimostrazioni sperimentali di QKD, sono state fatte su distanze di molti Km utilizzando come quantum bit la polarizzazione dei fotoni. I dispositivi crittografici quantistici sono già una realtà commerciale.
La prima quantum cryptographic network fu presentata a Boston nel 2003, l'ultima è stata proposta dalla Toshiba nel 2013.

Figura 3.2: Toshiba Quantum Crypto System

Il prototipo elaborato dalla Toshiba (di cui in figura 3.2 si riportano alcuni elementi), basato sulla crittografia quantistica, prevede un metodo intrinsecamente sicuro per la distribuzione di chiavi segrete digitali, con costi significativi e vantaggi nella gestione delle chiavi. In particolare consente la distribuzione delle chiavi su collegamenti in fibra ottica Telecom standard, superiori a 100 km di lunghezza e rates di bit sufficienti per generare 1 Megabit al secondo di chiavi su una distanza di 50 km - sufficientemente lunga per la copertura metropolitana.
Inoltre il sistema permette distribuzione di materiale in modo continuo, anche nelle condizioni operative più difficili, senza alcun intervento da parte dell'utente. Il sistema può essere utilizzato per una vasta gamma di applicazioni crittografiche, per esempio, codifica o autenticazione di documenti sensibili, messaggi o transazioni.

Bibliografia

[1] S. Singh, *Codici e Segreti*, Rizzoli (1999).

[2] P. Ferragina, F. Luccio, *Crittografia: Principi, Algoritmi, Applicazioni*, Bollati Boringhieri (2001).

[3] C. Toffalori, F. Corradini, S. Leonesi, S. Mancini, *Teoria della Computabilità e della Complessità*, McGraw-Hill (2005).

[4] E. Rieffel, FX Palo Alto Laboratory and W. Polak , *An introduction to Quantum Computing for Non-Physicists.*

[5] Douglas R. Stinson, University of Waterloo, Ontario, Canada, *Criptography. Theory and practice. Third edition*, Chapman & Hall — CRC (2006).

[6] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York, (1984).

[7] H. K. Lo and H. F. Chau, *Science 2050*, (1999); P. W. Shor and J. Preskill, *Physical Review Letters*,(2000).

[8] I. Csiszár e J. Körner, *IEEE Transactions on Information Theory*, (1978).

[9] M. J. W. Hall, *Physical Review Letters*, (1995).

Elenco delle figure

Elenco delle tabelle