Alma Mater Studiorum · Università di Bologna

scuola di scienze

Corso di Laurea in Matematica

CRITTOGRAFIA QUANTISTICA: IL PROTOCOLLO BB84

Tesi di Laurea in
Crittografia

Relatore:
Prof.
DAVIDE ALIFFI

Correlatrice:
Prof.ssa
ELISA ERCOLESSI

Presentata da:
LORENZA PRENCIPE

Anno Accademico 2018/2019

Alla mia famiglia

Indice

Introduzione

Il termine crittologia deriva dal greco *kryptòs* (nascosto) e *logos* (discorso), ovvero discorso nascosto: è una disciplina composta da crittografia e crittoanalisi, che si occupano rispettivamente dei metodi per criptare i messaggi e di quelli per svelarne il significato senza avere accesso alla chiavi per decifrarli. Questi due aspetti sono in lotta da quando esiste il bisogno di comunicare messaggi segreti a pochi destinatari autorizzati, rendendo necessaria la ricerca di metodi sempre più sicuri per poter comunicare.
Finora in *crittografia classica* l'unico cifrario perfettamente sicuro è quello di Vernam, che prevede che la chiave sia usa e getta (per questo motivo è chiamato One Time Pad, letteralmente "taccuino monouso"), che sia lunga quanto il messaggio e che gli utenti comunichino attraverso un canale sicuro.
Oggi lo sviluppo della *crittografia quantistica* sembra mettere fine a questa lotta, almeno dal punto di vista concettuale, rendendo possibile la cifratura dei messaggi in modo tale che nessun crittoanalista possa decodificarli. Il principio alla base è quello di indeterminazione di Heisenberg, che sostiene l'impossibilità di ottenere simultaneamente e con precisione assoluta, alcune particolari coppie di caratteristiche di un oggetto quantistico. Questo principio permette la realizzazione di un cifrario del tipo One Time Pad, ma senza il problema dello scambio delle chiavi su un canale sicuro. Utilizzando una chiave quantistica, si evita l'intercettazione della stessa senza che le parti in gioco se ne accorgano, perché in tal caso ne verrebbero modificate le caratteristiche introducendo degli errori casuali e rilevabili in modo certo.
Il primo protocollo quantistico, realizzato nel 1984 da Bennet e Brassard, risolve l'aspetto teorico della creazione di una chiave attraverso l'utilizzo dei fotoni con una determinata polarizzazione, ovvero la direzione dell'oscillazione durante la propagazione. L'obiettivo di questa tesi è analizzare gli aspetti teorici del protocollo BB84, l'implementazione e la sicurezza rispetto a un semplice attacco.

Capitolo 1

Introduzione alla Meccanica Quantistica

1.1 Spazi Vettoriali Lineari

Notazione 1.1.1. Sia $\mathscr{H}$ uno spazio vettoriale complesso finito dimensionale. Secondo la *Notazione di Dirac*, indichiamo i vettori di $\mathscr{H}$ con il simbolo $|\alpha\rangle$ e li chiamiamo **ket**.

Definizione 1.1.1. Diciamo che $\mathscr{H}$ è uno **spazio di Hilbert** se esiste un'applicazione

$$\langle \ | \ \rangle : \mathscr{H} \times \mathscr{H} \to \mathbb{C},$$

chiamata **prodotto scalare**, tale che:

- $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$, $\forall\ |\alpha\rangle, |\beta\rangle \in \mathscr{H}$
  dove $\forall c = a + ib$ $(a, b \in \mathbb{R})$ numero complesso, $c^* = a - ib$ è il suo complesso coniugato;
- $\langle\alpha|c\beta + d\gamma\rangle = c\langle\alpha|\beta\rangle + d\langle\alpha|\gamma\rangle$, $\forall\ |\alpha\rangle, |\beta\rangle, |\gamma\rangle \in \mathscr{H}$ e $\forall\ c, d \in \mathbb{C}$;
- $\langle\alpha|\alpha\rangle \geq 0,\ \forall\ |\alpha\rangle \in \mathscr{H}$ e $\langle\alpha|\alpha\rangle = 0$ se e solo se $|\alpha\rangle = 0$

dove $\langle\alpha|$ è il **vettore duale** (anche chiamato **bra**) del vettore $|\alpha\rangle$; il vettore duale $\langle\alpha|$ è un operatore lineare da $\mathscr{H}$ a $\mathbb{C}$, definito da $\langle\alpha|(|\beta\rangle) = \langle\alpha|\beta\rangle$, per ogni $|\beta\rangle \in \mathscr{H}$.

Esempio 1.1.1. Possiamo definire il prodotto scalare tra due vettori $|\alpha\rangle = (\alpha_1, \ldots, \alpha_n)$ e $|\beta\rangle = (\beta_1, \ldots, \beta_n)$ in $\mathbb{C}^n$ come segue

$$\langle\alpha|\beta\rangle = \sum_{i=1}^{n} {\alpha_i}^* \beta_i$$

In seguito considereremo sempre $\mathscr{H}$ come uno spazio di Hilbert finito dimensionale.

Definizione 1.1.2. La **norma** di un vettore $|\alpha\rangle$ è definita come

$$\| \, |\alpha\rangle \, \| = \sqrt{\langle\alpha|\alpha\rangle}.$$

Esempio 1.1.2. Utilizzando il prodotto scalare in $\mathbb{C}^n$, la norma di un vettore $|\alpha\rangle = (\alpha_1, \ldots, \alpha_\mathrm{n})$ è data da

$$\| \, |\alpha\rangle \, \| = \sqrt{\sum_{i=1}^{n} |\alpha_\mathrm{i}|^2}.$$

Definizione 1.1.3. Due vettori non nulli $|\alpha\rangle$ e $|\beta\rangle$ si dicono **ortogonali** se il loro prodotto scalare è zero:

$$\langle\alpha|\beta\rangle = 0.$$

Un insieme di vettori $|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_\mathrm{n}\rangle$ si dice **ortonormale** se

$$\langle\alpha_\mathrm{i}|\alpha_\mathrm{j}\rangle = \delta_\mathrm{ij}, (i, j = 1, \ldots, n),$$

dove δ_ij è il simbolo di Kronecker, definito come $\delta_\mathrm{ij} = 1$ per i=j e $\delta_\mathrm{ij} = 0$ per i$\neq$j.

Definizione 1.1.4. Dati $|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_\mathrm{n}\rangle \in \mathscr{H}$ si dice che essi sono **linearmente indipendenti** se la relazione

$$c_1|\alpha_1\rangle + c_2|\alpha_2\rangle + \ldots + c_\mathrm{n}|\alpha_\mathrm{n}\rangle = 0$$

con $c_1, c_2 \ldots, c_\mathrm{n}$ numeri complessi, è verificata se e solo se $c_1 = c_2 = \ldots = c_\mathrm{n} = 0$

Definizione 1.1.5. La **dimensione** di uno spazio $\mathscr{H}$ è data dal massimo numero di vettori linearmente indipendenti.

Definizione 1.1.6. Un insieme di vettori $|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_\mathrm{n}\rangle$ linearmente indipendenti nello spazio $\mathscr{H}$ di dimensione n si dice **base**.
Ogni vettore $|\alpha\rangle$ si può esprimere come combinazione lineare di vettori della base $\{|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_\mathrm{n}\rangle\}$,

$$|\alpha\rangle = \sum_{i=1}^{n} a_\mathrm{i}|\alpha_\mathrm{i}\rangle.$$

dove gli $a_\mathrm{i} \in \mathbb{C}$ sono detti **componenti**.

Definizione 1.1.7. Un **operatore** è un'applicazione che manda ogni vettore $|\alpha\rangle \in \mathscr{H}$ in un altro vettore $|\beta\rangle \in \mathscr{H}$:

$$|\beta\rangle = A|\alpha\rangle.$$

L'operatore A è detto **lineare** se per ogni coppia di vettori $|\alpha\rangle$ e $|\beta\rangle$ e per ogni coppia di numeri complessi a e b, si ha:

$$A(a|\alpha\rangle + b|\beta\rangle) = aA|\alpha\rangle + bA|\beta\rangle.$$

Due operatori A e B si dicono **uguali** (e scriviamo $A = B$) se per ogni vettore $|\alpha\rangle \in \mathscr{H}$,

$$A|\alpha\rangle = B|\alpha\rangle$$

La **somma** $C = A + B$ di due operatori lineari A e B è lineare ed è definita come segue:

$$C|\alpha\rangle = (A + B)|\alpha\rangle = A|\alpha\rangle + B|\alpha\rangle.$$

Definiamo il **prodotto** $D = AB$ di due operatori in questo modo:

$$D|\alpha\rangle = AB|\alpha\rangle = A(B|\alpha\rangle).$$

Inoltre se $AB = BA$ si dice che gli operatori **commutano**.

Osservazione 1.1.1. È possibile descrivere un operatore lineare attraverso una rappresentazione matriciale: data una base ortonormale $\{|\gamma_1\rangle, \ldots, |\gamma_n\rangle\}$, siano

$$|\alpha\rangle = \sum_i a_i|\gamma_i\rangle,$$

$$|\beta\rangle = \sum_i b_i|\gamma_i\rangle.$$

Allora

$$b_i = \langle\gamma_i|\beta\rangle = \langle\gamma_i|A\alpha\rangle = \sum_j \langle\gamma_i|A\gamma_j\rangle a_j \equiv \sum_j A_{ij}a_j, (i = 1, 2, \ldots, n),$$

dove abbiamo definito

$$A_{ij} = \langle\gamma_i|A\gamma_j\rangle.$$

Quindi il sistema di equazioni b_i si scrive come: $\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} A_{11} & \ldots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \ldots & A_{nn} \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$.

Notazione 1.1.2. Indicheremo anche con $\langle\gamma_i|A|\gamma_j\rangle \equiv \langle\gamma_i|A\gamma_j\rangle$

Definizione 1.1.8. Dato un operatore lineare A si chiama **autovettore** un vettore non nullo $|\alpha\rangle$ tale che $A|\alpha\rangle = a|\alpha\rangle$, dove $a \in \mathbb{C}$ è chiamato **autovalore**.
Lo spazio generato dagli autovettori relativi all'autovalore a è detto **autospazio** associato ad a.

Definizione 1.1.9. Le **matrici di Pauli** σ_{x}, σ_{y} e σ_{z} sono definite come segue:

$$\sigma_{\mathrm{x}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \sigma_{\mathrm{y}} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_{\mathrm{z}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Osservazione 1.1.2. Le matrici di Pauli soddisfano le seguenti proprietà:

- ${\sigma_{\mathrm{x}}}^2 = {\sigma_{\mathrm{y}}}^2 = {\sigma_{\mathrm{z}}}^2 = I$, dove I è la matrice identità

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- $\sigma_{\mathrm{x}}\sigma_{\mathrm{y}} = i\sigma_{\mathrm{z}}$, $\sigma_{\mathrm{y}}\sigma_{\mathrm{z}} = i\sigma_{\mathrm{x}}$, $\sigma_{\mathrm{z}}\sigma_{\mathrm{x}} = i\sigma_{\mathrm{y}}$

Definizione 1.1.10. Un'importante classe di operatori è data dai **proiettori**. Se $|\alpha\rangle \in \mathscr{H}$ è un vettore unitario, il proiettore unidimensionale P_α è definito, per ogni vettore $|\gamma\rangle \in \mathscr{H}$, come segue:

$$|\beta\rangle = P_\alpha|\gamma\rangle = |\alpha\rangle\langle\alpha|\gamma\rangle = \langle\alpha|\gamma\rangle|\alpha\rangle.$$

Osservazione 1.1.3. Questo operatore è chiamato proiettore poichè proietta un generico vettore $|\gamma\rangle$ lungo la direzione $|\alpha\rangle$. In particolare, $P_\alpha|\alpha\rangle = |\alpha\rangle$ e $P_\alpha|\gamma\rangle = 0$ per ogni $|\gamma\rangle$ ortogonale a $|\alpha\rangle$. Un proiettore soddisfa la seguente proprietà:

$${P_\alpha}^2 = P_\alpha.$$

Definizione 1.1.11. Un operatore è detto **diagonalizzabile** se ha una rappresentazione diagonale.

Definizione 1.1.12. Per ogni operatore lineare A su uno spazio di Hilbert $\mathscr{H}$, è possibile definire un operatore lineare $A^\dagger$ su $\mathscr{H}$, chiamato **aggiunto** o **Hermitiano coniugato** di A, tale che per tutti i vettori $|\alpha\rangle, |\beta\rangle \in \mathscr{H}$,

$$\langle\alpha|A\beta\rangle = \langle A^\dagger\alpha|\beta\rangle.$$

Un caso particolare è quello in cui A è un operatore **Hermitiano** o **autoaggiunto**, ovvero in cui A è uguale al suo aggiunto:

$$A^\dagger = A$$

.

Definizione 1.1.13. Consideriamo un operatore lineare A. Se esiste un operatore B tale che

$$AB = BA = I,$$

chiamiamo B **inverso** di A e scriviamo $B = A^{-1}$.

Definizione 1.1.14. Un operatore U è detto **unitario** se

$$UU^\dagger = U^\dagger U = I.$$

Osservazione 1.1.4. Da questa definizione, abbiamo che l'aggiunto di un operatore unitario coincide con il suo inverso,

$$U^\dagger = U^{-1},$$

e che $U^\dagger$ è unitario.

Osservazione 1.1.5. Le matrici di Pauli $\sigma_{\mathrm{x}}, \sigma_{\mathrm{y}}, \sigma_{\mathrm{z}}$, sono sia Hermitiane che unitarie.

Definizione 1.1.15. Un operatore **normale** è definito dalla condizione

$$AA^\dagger = A^\dagger A.$$

Teorema 1.1.1. (Teorema di decomposizione spettrale):
Un operatore è diagonalizzabile, con una base ortonormale di autovettori, se e solo se è normale.

Teorema 1.1.2. (Teorema di diagonalizzazione simultanea):
Due operatori normali A e B commutano se e solo se esiste una base ortonormale rispetto alla quale A e B sono diagonali.

Definizione 1.1.16. Siano $\mathscr{H}_1$ e $\mathscr{H}_2$ due spazi di Hilbert di dimensione rispettivamente m e n. Diciamo che lo spazio di Hilbert $\mathscr{H}$ è il **prodotto tensoriale** di $\mathscr{H}_1$ e $\mathscr{H}_2$ e scriviamo $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$, se è uno spazio vettoriale dotato dell'applicazione bilineare $\otimes : \mathscr{H}_1 \times \mathscr{H}_2 \to \mathscr{H}$ e generato dai vettori $|\alpha\rangle \otimes |\beta\rangle$ con $|\alpha\rangle \in \mathscr{H}_1$ e $|\beta\rangle \in \mathscr{H}_2$.

Notazione 1.1.3. Spesso useremo più brevemente $|\alpha\rangle|\beta\rangle$, $|\alpha\rangle, |\beta\rangle$ o $|\alpha\beta\rangle$ al posto di $|\alpha\rangle \otimes |\beta\rangle$.

Osservazione 1.1.6. La dimensione dello spazio di Hilbert $\mathscr{H}$ è data dal prodotto mn delle dimensioni di $\mathscr{H}_1$ e $\mathscr{H}_2$. Infatti se $|i\rangle$ e $|j\rangle$ sono basi ortonormali di $\mathscr{H}_1$ e $\mathscr{H}_2$, allora $|i\rangle \otimes |j\rangle$ è una base ortonormale per $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$

Definizione 1.1.17. Se A e B sono due operatori lineari che agiscono rispettivamente su $\mathscr{H}_1$ e $\mathscr{H}_2$, l'azione di $A \otimes B$ su un generico vettore

$$|\psi\rangle = \sum_{ij} c_{ij} |i\rangle \otimes |j\rangle$$

appartenente a $\mathscr{H}$, con $c_{ij} = \langle ij|\psi\rangle$, è definita da

$$(A \otimes B)(\sum_{ij} c_{ij} |i\rangle \otimes |j\rangle) = \sum_{ij} c_{ij} A|i\rangle \otimes B|j\rangle.$$

Osservazione 1.1.7. La rappresentazione matriciale dell'operatore $A \otimes B$ nella base $|K\rangle \equiv |ij\rangle$ è data da

$$A \otimes B = \begin{bmatrix} A_{11}B & \dots & A_{1m}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \dots & A_{mm}B \end{bmatrix},$$

dove i termini di $A \otimes B$ sono i singoli termini di A moltiplicati per B, quindi sottomatrici di dimensione $n \times n$, con A e B rappresentazioni matriciali dei rispettivi operatori (A e B sono matrici rispettivamente $m \times m$ e $n \times n$).

1.2 I Postulati della Meccanica Quantistica

Postulato 1. Lo stato di un sistema fisico S è descritto da un vettore unitario $|\psi\rangle$, chiamato **vettore di stato** o **funzione d'onda**, appartenente allo spazio di Hilbert $\mathscr{H}_S$ associato al sistema.
L'evoluzione temporale di un vettore di stato $|\psi\rangle$ è data dall'equazione di Schrödinger

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle,$$

dove H è un operatore autoaggiunto chiamato Hamiltoniano e $\hbar \equiv h/2\pi$, con h costante di Planck, il cui valore è determinato sperimentalmente ($h \approx 6.626 \times 10^{-34}$ Joule sec).

Definizione 1.2.1. L'**operatore di evoluzione temporale** U è definito da

$$|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle$$

Osservazione 1.2.1. È importante osservare che l'equazione di Schrödinger è un'equazione differenziale lineare di primo ordine rispetto al tempo. Quindi, dato uno stato iniziale $|\psi(t_0)\rangle$, lo stato $|\psi(t)\rangle$ è univocamente determinato dalla soluzione di questa equazione.
Poichè l'equazione di Schrödinger è lineare, segue il **principio di sovrapposizione**: se $|\psi_1(t)\rangle$ e $|\psi_2(t)\rangle$ sono soluzioni dell'equazione di Schrödinger, allora è soluzione anche la sovrapposizione $|\psi(t)\rangle = \alpha|\psi_1(t)\rangle + \beta|\psi_2(t)\rangle$, dove α e β sono numeri complessi.
Se l'Hamiltoniano H è indipendente dal tempo, la soluzione dell'equazione di Schrödinger può essere scritta come

$$|\psi(t)\rangle = exp\left[-\frac{i}{\hbar}H(t-t_0)\right]|\psi(t_0)\rangle,$$

e quindi

$$U(t, t_0) = exp\left[-\frac{i}{\hbar}H(t-t_0)\right],$$

dove l'esponenziale dell'operatore $-\frac{i}{\hbar}H(t-t_0)$ è definita come segue:

$$exp\left[-\frac{i}{\hbar}H(t-t_0)\right] \equiv \sum_{i=0}^{\infty}\frac{1}{n!}\left[-\frac{i}{\hbar}(t-t_0)\right]^n H^n.$$

Partendo da questa equazione si ricava che l'operatore di evoluzione temporale U è unitario.

Postulato 2. Associamo ad ogni osservabile A un operatore autoaggiunto A sullo spazio di Hilbert $\mathscr{H}_{\mathrm{S}}$. L'unico risultato possibile della misurazione di tale osservabile A è uno degli autovalori di A. Se scriviamo l'equazione dell'autovalore per l'operatore A,

$$A|i\rangle = a_{\mathrm{i}}|i\rangle,$$

dove $|i\rangle$ è una base ortonormale di autovettori dell'operatore A, e espandiamo il vettore di stato $|\psi(t)\rangle$ attraverso questa base:

$$|\psi(t)\rangle = \sum_i c_{\mathrm{i}}(t)|i\rangle,$$

allora la probabilità di misurare un'osservabile A al tempo t con risultato a_{i} è data da

$$p_{\mathrm{i}}(t) = p(a = a_{\mathrm{i}}|t) = |\langle i|\psi(t)\rangle|^2 = |c_{\mathrm{i}}(t)|^2.$$

I coefficienti c_{i} prendono il nome di **ampiezze di probabilità**.

Osservazione 1.2.2. È importante sottolineare che le osservabili sono l'analogo quantistico delle variabili dinamiche in meccanica classica, come la posizione, il momento lineare e angolare e così via. Come in meccanica classica, le altre caratteristiche di un sistema come massa o carica elettrica, non sono nella categoria di osservabili, ma rientrano come parametri nell'Hamiltoniano del sistema.

Osservazione 1.2.3. La ragione per cui associamo operatori autoaggiunti a osservabili fisiche risiede nel seguente motivo: gli autovalori di un operatore autoaggiunto sono reali e i suoi autovettori formano una base ortonormale per lo spazio di Hilbert $\mathscr{H}_S$ associato al sistema. Poichè $|\psi(t)\rangle$ ha norma unitaria, abbiamo

$$\sum_i p_{\mathrm{i}}(t) = \sum_i |c_{\mathrm{i}}(t)|^2 = 1,$$

e quindi le probabilità sono normalizzate, ovvero la probabilità totale di ottenere un risultato dalla misurazione dell'osservabile A è uguale a 1. È esattamente il motivo per cui il Postulato 1 richiede che $|\psi(t)\rangle$ abbia norma unitaria.

Osservazione 1.2.4. Nel caso particolare in cui il vettore di stato $|\psi(t_0)\rangle$ a un certo istante t_0 coincide con l'autovettore dell'operatore A con autovalore a_{i},

$$|\psi(t_0)\rangle = |i\rangle,$$

la misurazione dell'osservabile A al tempo t_0 da come risultato a_{i} con probabilità unitaria. Per questo motivo gli autovettori dell'operatore A sono anche chiamati **autostati** di A.

Osservazione 1.2.5. Siano $|\psi_1\rangle$ e $|\psi_2\rangle$ due autovettori dell'operatore A distinti e normalizzati, con autovalori rispettivi a_1 e a_2.
Per il principio di sovrapposizione, lo stato

$$|\psi\rangle = \lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle,$$

con λ_1 e λ_2 numeri complessi tali che $|\lambda_1|^2 + |\lambda_1|^2 = 1$, è ancora uno stato del sistema. Quindi, se un sistema è descritto dal vettore di stato $|\psi\rangle$ e misuriamo un'osservabile A, otteniamo come risultato a_1 con probabilità $|\lambda_1|^2$ e a_2 con probabilità $|\lambda_2|^2$.

Ora discutiamo l'effetto delle misurazioni sullo stato del sistema. Assumiamo che la misurazione di un'osservabile A dia come risultato a_{n}, con a_{n} autovalore non degenere. Se la misurazione non distrugge il sistema e viene effettuata immediatamente una nuova misurazione dell'osservabile A, otteniamo di nuovo a_{n} come risultato con probabità unitaria. Questo risultato sperimentale si spiega assumendo che la funzione d'onda del sistema, che nell'istante precedente della prima misurazione era nello stato $|\psi\rangle$, immediatamente dopo la misurazione collassi nell'autostato $|n\rangle$ di A associato all'autovalore a_{n}. Nel caso in cui l'autovalore sia degenere, possiamo espandere lo stato $|\psi\rangle$ prima della misurazione come segue:

$$|\psi\rangle = \sum_{n} \sum_{s=1}^{g_{\mathrm{n}}} c_{\mathrm{n_s}} |n_{\mathrm{s}}\rangle,$$

con

$$c_{\mathrm{n_s}} = \langle n_{\mathrm{s}} | \psi \rangle,$$

e dove g_{n} misura l'ordine di degenerazione dell'autovalore a_{n}, ovvero la dimensione del sottospazio generato dagli autovettori $|n_{\mathrm{s}}\rangle$ di A relativi allo stesso autovalore a_{n}. Dopo una misurazione con risultato a_{n}, lo stato del sistema appartiene a questo sottospazio ed è dato da

$$\frac{1}{\sqrt{\sum_{s=1}^{g_{\mathrm{n}}} |c_{\mathrm{n_s}}|^2}} \sum_{s=1}^{g_{\mathrm{n}}} c_{\mathrm{n_s}} |n_{\mathrm{s}}\rangle.$$

Questo stato è la proiezione di $|\psi\rangle$ sul sottospazio relativo a a_{n}.

Postulato 3. Se un sistema è descritto dal vettore d'onda $|\psi\rangle$ e misuriamo un'osservabile A ottenendo come risultato a_{n}, allora immediatamente dopo la misurazione, lo stato del sistema è dato da

$$\frac{P_{\mathrm{n}} |\psi\rangle}{\sqrt{\langle \psi | P_{\mathrm{n}} | \psi \rangle}},$$

dove P_{n} è la proiezione sul sottospazio relativo ad a_{n}.

Osservazione 1.2.6. Nel caso in cui l'autovalore a_{n} sia degenere, il proiettore P_{n} soddisfa

$$P_{\mathrm{n}} = \sum_{s=1}^{g_{\mathrm{n}}} |n_{\mathrm{s}}\rangle \langle n_{\mathrm{s}}|.$$

Osservazione 1.2.7. Poichè gli autovettori di A costituiscono una base ortonormale per lo spazio di Hilbert $\mathscr{H}_{\mathrm{S}}$ associato al sistema, si verifica che i P_{n} soddisfano la relazione di completezza,

$$\sum_{n} P_{\mathrm{n}} = I,$$

e la condizione di ortogonalità

$$P_{\mathrm{n}} P_{\mathrm{m}} = \delta_{\mathrm{mn}} P_{\mathrm{m}}$$

Osservazione 1.2.8. Nel caso in cui l'autovalore a_n non sia degenere, $g_\mathrm{n} = 1$, la funzione d'onda del sistema dopo la misurazione collassa nello stato

$$\frac{1}{|c_\mathrm{n}|} c_\mathrm{n} |n\rangle,$$

e quindi nell'autostato $|n\rangle$ corrispondente.

Definizione 1.2.2. Il **valore medio** dell'osservabile A è dato da

$$\langle A \rangle = \sum_n a_\mathrm{n} p_\mathrm{n}$$

Osservazione 1.2.9. Osserviamo che la probabilità di ottenere un risultato a_n nel caso in cui questo degeneri è data da

$$p_\mathrm{n} = \langle \psi | P_\mathrm{n} | \psi \rangle,$$

quindi

$$\langle A \rangle = \sum_n a_\mathrm{n} \langle \psi | P_\mathrm{n} | \psi \rangle = \langle \psi | \left(\sum_n a_\mathrm{n} P_\mathrm{n} \right) | \psi \rangle = \langle \psi | A | \psi \rangle,$$

dove abbiamo usato la decomposizione spettrale $A = \sum_n a_\mathrm{n} P_\mathrm{n}$.

Definizione 1.2.3. La **deviazione standard** ΔA è associata all'osservabile A è data da

$$\Delta A = \sqrt{\langle (A - \langle A \rangle)^2 \rangle} = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}.$$

Partendo dall'analisi di alcuni esperimenti ideali, Heisenberg mostrò che non è possibile assegnare ad una particella posizione e velocità in modo simultaneo e determinato. Se aumentiamo la precisione nella nostra misurazione della velocità della particella, aumentiamo l'incertezza sulla posizione e viceversa. Questa limitazione intrinseca è espressa dalle relazioni di indeterminazione di posizione e momento di Heisenberg:

$$\Delta x \Delta p_\mathrm{x} \geq \tfrac{\hbar}{2}, \qquad \Delta y \Delta p_\mathrm{y} \geq \tfrac{\hbar}{2}, \qquad \Delta z \Delta p_\mathrm{z} \geq \tfrac{\hbar}{2}$$

dove Δx, Δy, Δz e Δp_x, Δp_y, Δp_z sono le indeterminazioni della posizione e del momento della particella. In seguito diamo la formulazione matematica precisa del principio di indeterminazione di Heisenberg, sviluppata da Jordan.

Il principio di indeterminazione di Heisenberg: Siano A e B operatori Hermitiani associati alle osservabili e $|\psi\rangle$ uno stato quantico. Allora vale la seguente disuguaglianza:

$$\Delta A \Delta B \geq \frac{|\langle \psi | [A, B] | \psi \rangle|}{2}$$

Il principio di Heisenberg afferma che, date due osservabili A e B che non commutano, c'è un limite intrinseco sull'accuratezza delle misurazioni simultanee di A e B: la misurazione di una, disturba necessariamente l'altra. Se misuriamo A con un'accuratezza ΔA, allora B viene disturbato di ΔB e $\Delta A \Delta B$ soddisfa la disuguaglianza di Heisenberg.

Capitolo 2

Computazione e Informazione Quantistica

2.1 Il Quantum Bit

Un bit classico è un sistema che può esistere in due stati differenti, solitamente rappresentati con 0 e 1, che sono singole cifre binarie. Le uniche operazioni possibili in questo sistema sono l'identità ($0 \to 0, 1 \to 1$) e la negazione NOT ($0 \to 1, 1 \to 0$).
La versione quantistica del bit classico è il quantum bit (qubit), un sistema quantistico a due livelli descritto da uno spazio di Hilbert complesso bidimensionale. Su questo spazio definiamo la base canonica, costituita dai due stati quantistici

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

che rappresentano i valori 0 e 1 di un bit classico.
Quindi per il principio di sovrapposizione, lo stato generico di un qubit è descritto da

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

dove le ampiezze α e β sono numeri complessi tali che $|\alpha|^2 + |\beta|^2 = 1$.
Un sistema quantistico a due livelli può essere utilizzato come qubit se è possibile manipolarlo come segue:

- può essere preparato in uno stato definito, per esempio lo stato $|0\rangle$;
- ogni stato del qubit può essere trasformato in un altro stato;
- lo stato del qubit può essere misurato nella base canonica $\{|0\rangle, |1\rangle\}$.

2.1.1 Polarizzazione

Uno degli approcci più comuni per realizzare concretamente un qubit è quello di considerare i due diversi stati di polarizzazione di un fotone, $|0\rangle$ quando è polarizzato lungo l'asse x e $|1\rangle$ quando è polarizzato lungo l'asse y. Inoltre un fotone può essere polarizzato lungo una direzione che forma un angolo β con l'asse x. In questo caso è descritto dalla funzione d'onda

$$|\psi\rangle = cos\beta|0\rangle + sin\beta|1\rangle$$

Assumiamo che il fotone sia mandato verso un analizzatore di polarizzazione (un cristallo birifrangente come la calcite), allora fuoriesce dall'analizzatore polarizzato lungo l'asse x (se passa attraverso il cristallo) o lungo l'asse y (se viene deflesso). Questi due possibili risultati che chiamiamo 0 e 1, si verificano con probabilità rispettive

$$p_0 = |\langle 0|\psi\rangle|^2 = cos^2\beta \qquad \text{e} \qquad p_1 = |\langle 1|\psi\rangle|^2 = sin^2\beta$$

calcolate usando il Postulato 2 della meccanica quantistica.

2.1.2 Sfera di Bloch

È possibile rappresentare gli stati come punti sulla superficie di una sfera di raggio unitario, chiamata **sfera di Bloch**. Quindi, lo stato generico di un qubit può essere scritto come

$$|\psi\rangle = cos\tfrac{\theta}{2}|0\rangle + e^{i\phi}sin\tfrac{\theta}{2}|1\rangle = \begin{bmatrix} cos\frac{\theta}{2} \\ e^{i\phi}sin\frac{\theta}{2} \end{bmatrix} \qquad (0 \leq \theta \leq \pi, 0 \leq \phi < 2\pi).$$

Questa sfera può essere vista come uno spazio tridimensionale di coordinate Cartesiane $(x = cos\phi sin\theta, y = sin\phi sin\theta, z = cos\theta)$, quindi lo stato può essere riscritto come

$$|\psi\rangle = \begin{bmatrix} \sqrt{\frac{1+z}{2}} \\ \frac{x+iy}{\sqrt{2(1+z)}} \end{bmatrix}.$$

2.2 Misurare lo Stato di un Qubit

Lo stato di un qubit può essere misurato nella base canonica $\{|0\rangle, |1\rangle\}$, quindi si può misurare la polarizzazione di un qubit lungo l'asse z. L'operatore Hermitiano associato a questa misurazione è l'operatore di Pauli σ_z, che ha autostati $\{|0\rangle, |1\rangle\}$ e rispettivi autovalori $\{+1, -1\}$ con probabilità

$$p_0 = |\langle 0|\psi\rangle|^2 = cos^2\tfrac{\theta}{2}, \qquad p_1 = |\langle 1|\psi\rangle|^2 = sin^2\tfrac{\theta}{2},$$

calcolate usando il Postulato 2 della meccanica quantistica.
Mostreremo in questa sezione che è possibile misurare le coordinate x, y, z di un qubit sulla sfera di Bloch.
Usando le matrici di Pauli

$$\sigma_x|\psi\rangle = e^{i\phi}sin\tfrac{\theta}{2}|0\rangle + cos\tfrac{\theta}{2}|1\rangle,$$

$$\sigma_y|\psi\rangle = -ie^{i\phi}sin\tfrac{\theta}{2}|0\rangle + icos\tfrac{\theta}{2}|1\rangle,$$

$$\sigma_z|\psi\rangle = cos\tfrac{\theta}{2}|0\rangle - e^{i\phi}sin\tfrac{\theta}{2}|1\rangle.$$

Quindi

$$\langle\psi|\sigma_x|\psi\rangle = \langle\psi| \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |\psi\rangle = sin\theta cos\phi = x$$

$$\langle\psi|\sigma_y|\psi\rangle = \langle\psi| \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} |\psi\rangle = sin\theta sin\phi = y$$

$$\langle\psi|\sigma_z|\psi\rangle = \langle\psi| \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} |\psi\rangle = cos\theta = z.$$

Le coordinate (x, y, z) possono essere ottenute con precisione arbitraria misurando σ_z. Infatti:

$$p_0 - p_1 = cos^2\frac{\theta}{2} - sin^2\frac{\theta}{2} = cos\theta = z.$$

Quindi, la coordinata z è data dalla differenza delle probabilità di ottenere risultati 0 o 1 da una misurazione di σ_z. Se abbiamo a disposizione un grande numero N di sistemi preparati in modo autentico, possiamo stimare z come $N_0/N - N_1/N$, dove N_0 e N_1 sono rispettivamente il numero di risultati 0 e 1. Pertanto z può essere misurato con qualsiasi grado di precisione richiesto, a condizione di misurare un numero sufficientemente grande di stati.
Le coordinate x e y possono essere ottenute usando una trasformazione unitaria sul qubit. Se applichiamo la trasformazione unitaria descritta dalla matrice

$$U_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

allo stato $|\psi\rangle$, otteniamo lo stato $|\psi^{(1)}\rangle = U_1|\psi\rangle$.
Una misurazione proiettiva sulle basi canoniche dà quindi come risultato 0 o 1 con probabilità rispettivamente ${p_0}^{(1)} = |\langle 0|\psi^{(1)}\rangle|^2$ e ${p_1}^{(1)} = |\langle 1|\psi^{(1)}\rangle|^2$. Perciò otteniamo

$$ {p_0}^{(1)} - {p_1}^{(1)} = cos\phi sin\theta = x. $$

Allo stesso modo, se trasformiamo lo stato $|\psi\rangle$ attraverso la matrice

$$ U_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}, $$

otteniamo lo stato $|\psi^{(2)}\rangle = U_2|\psi\rangle$. Perciò

$$ {p_0}^{(2)} - {p_1}^{(2)} = sin\phi sin\theta = y, $$

dove ${p_0}^{(2)} = |\langle 0|\psi^{(2)}\rangle|^2$ e ${p_1}^{(2)} = |\langle 1|\psi^{(2)}\rangle|^2$ sono le probabilità di ottenere come risultato 0 o 1 dalla misurazione della polarizzazione del qubit lungo l'asse z.

Capitolo 3

Crittografia Classica

3.1 Sistemi Crittografici e Sicurezza Perfetta

Definizione 3.1.1. Uno **schema di cifratura a chiave privata** è un sistema che prevede gli insiemi $\mathscr{M}$ di messaggi in chiaro e $\mathscr{K}$ di chiavi ed è composto da:

- Gen: un algoritmo randomizzato che restituisce $k \in \mathscr{K}$, prendendo in input un parametro di sicurezza (come la lunghezza della chiave);
- Enc: algoritmo deterministico di cifratura "encryption" che produce il messaggio cifrato c, prendendo in input $m \in \mathscr{M}$ e $k \in \mathscr{K}$, formalmente $Enc_k(m) = c$;
- Dec: algoritmo inverso di decifratura $Dec_k(c) = m$ con $k \in \mathscr{K}$ e la seguente condizione di sicurezza $Pr[Dec_k(Enc_k(m)) = m] = 1$

Notazione 3.1.1. Denotiamo con:

- $\mathscr{C}$ l'insieme di tutti i testi cifrati possibili, output di $Enc_k(m)$, per ogni scelta possibile di $k \in \mathscr{K}$ e $m \in \mathscr{M}$;
- K una variabile casuale che indica il valore della chiave output di Gen, quindi per ogni $k \in \mathscr{K}$ scriviamo $Pr[K = k]$ per indicare la probabilità che l'output di Gen sia esattamente k;
- M una variabile casuale che rappresenta il messaggio in chiaro, quindi con $Pr[M = m]$ la probabilità che il messaggio in chiaro assuma il valore $m \in \mathscr{M}$;
- C una variabile casuale del testo cifrato, quindi per $c \in \mathscr{C}$ scriviamo $Pr[C = c]$ intendendo la probabilità che il testo cifrato sia esattamente uguale al valore c fissato.

Definizione 3.1.2. Un sistema di crittografia a chiave privata $(\mathscr{M}, \mathscr{K}, Gen, Enc, Dec)$ è detto **perfettamente sicuro** se per ogni distribuzione di probabilità su $\mathscr{M}$, per ogni messaggio in chiaro $m \in \mathscr{M}$ e per ogni messaggio cifrato $c \in \mathscr{C}$ tale che $Pr[C = c] > 0$:

$$Pr[M = m|C = c] = Pr[M = m]$$

3.2 Il Cifrario di Vernam

Nel 1917 Vernam brevettò un sistema crittografico perfettamente sicuro chiamato *One-Time Pad* (OTP). Quando Vernam propose lo schema, non vi era dimostrazione che fosse perfettamente sicuro, perché la sicurezza perfetta non era ancora stata definita. Circa 25 anni dopo, Shannon introdusse questa definizione e dimostrò che OTP soddisfa tale livello di sicurezza.

Costruzione:
Sia $n > 0$. Lo spazio $\mathscr{M}$ dei messaggi in chiaro, lo spazio $\mathscr{K}$ delle chiavi e lo spazio $\mathscr{C}$ dei messaggi cifrati sono tutti uguali a $\{0,1\}^n$ (l'insieme di tutte le stringhe binarie di lunghezza n).

- Gen: l'algoritmo estrae casualmente una chiave da $\mathscr{K} = \{0,1\}^n$ (ognuna delle 2^n stringhe è scelta come chiave con probabilità 2^{-n}).
- Enc: data una chiave $k \in \{0,1\}^n$ e un messaggio in chiaro $m \in \{0,1\}^n$, l'algoritmo di cifratura restituisce un messaggio in chiave $c := k \oplus m$.
- Dec: data una chiave $k \in \{0,1\}^n$ e un messaggio cifrato $c \in \{0,1\}^n$, l'algoritmo di decifratura restituisce un messaggio in chiaro $m := k \oplus c$.

Nella descrizione dello schema di cifratura OTP denotiamo con $a \oplus b$ la **disgiunzione esclusiva** (XOR) di due stringhe binarie (se $a = a_1 \cdots a_\mathrm{n}$ e $b = b_1 \cdots b_\mathrm{n}$ sono stringhe di n bit, allora $a \oplus b$ è la stringa di n bit data da $a_1 \oplus b_1 \cdots a_\mathrm{n} \oplus b_\mathrm{n}$). Prima di discuterne la sicurezza, verifichiamo la correttezza: per ogni chiave k e per ogni messaggio in chiaro m abbiamo che $Dec_\mathrm{k}(Enc_\mathrm{k}(m)) = k \oplus k \oplus m = m$, quindi OTP risulta uno schema di cifratura valido.

Teorema 3.2.1. Il sistema di crittografia one-time pad è perfettamente sicuro.

Dimostrazione. Innanzitutto calcoliamo $Pr[C = c|M = m']$ per $c \in \mathscr{C}$ arbitrario e $m' \in \mathscr{M}$. Per l'OTP,

$$Pr[C = c|M = m'] = Pr[Enc_K(m') = c] = Pr[m' \oplus K = c] = Pr[K = m' \oplus c] = 2^{-n},$$

dove l'ultima uguaglianza segue dal fatto che la chiave K è una stringa di n bit casuale. Fissata una qualsiasi distribuzione su $\mathscr{M}$, per ogni $c \in \mathscr{C}$ abbiamo

$$Pr[C = c] = \sum_{m' \in \mathscr{M}} Pr[C = c | M = m'] \cdot Pr[M = m'] = 2^{-n} \cdot \sum_{m' \in \mathscr{M}} Pr[M = m'] = 2^{-n},$$

con $Pr[M = m'] \neq 0$. Per il Teorema di Bayes:

$$Pr[M = m | C = c] = \frac{Pr[C = c | M = m] \cdot Pr[M = m]}{Pr[C = c]} = \frac{2^{-n} \cdot Pr[M = m]}{2^{-n}} = Pr[M = m].$$

L'OTP possiede numerosi inconvenienti, il più importante è che la chiave deve essere lunga quanto il messaggio. Questo limita l'utilità dello schema per l'invio di messaggi molto lunghi, visto che può essere difficile condividere e memorizzare in modo sicuro una chiave molto lunga, ed è problematico quando le parti non possono prevedere in anticipo un limite superiore per la lunghezza del messaggio.

Inoltre l'one-time pad, come indica il nome, è sicuro solo se usato una volta con la stessa chiave, perché cifrare più messaggi con la stessa chiave genererebbe la perdita di molte informazioni.
In particolare, siano m, m' due messaggi in chiaro cifrati con la stessa chiave k. Un avversario che ottiene $c = m \oplus k$ e $c' = m' \oplus k$ può calcolare

$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'$$

e quindi apprendere la disgiunzione esclusiva dei due messaggi, ovvero di quanto differiscono esattamente gli stessi. Sebbene possa non sembrare molto significativo, è sufficiente ad escludere qualsiasi pretesa di sicurezza perfetta: dato che messaggi cifrati sufficientemente lunghi possiedono delle ridondanze, attraverso l'analisi delle frequenze si potrebbe risalire a quelli in chiaro. Pertanto, il problema principale della crittografia non è la trasmissione del messaggio cifrato, ma la distribuzione della chiave segreta, che richiede una sorta di "corriere di fiducia". Un intercettatore Eve potrebbe trovare un modo per leggere la chiave senza lasciare traccia, quindi la comunicazione tra due personaggi, Alice e Bob non sarà mai assolutamente sicura riguardo la segretezza della chiave. Nel capitolo successivo mostreremo che la meccanica quantistica risolve questo problema, offrendo un'unica strada per la *distribuzione* e l'*archiviazione* della chiave.

3.3 Limiti della Sicurezza Perfetta

Nella sezione precedente abbiamo notato alcuni inconvenienti dello schema di cifratura OTP, in questa mostreremo che non sono peculiari di questo schema, ma riguardano più in generale la sicurezza perfetta. In particolare, dimostreremo che ogni schema di cifratura perfettamente sicuro deve avere uno spazio delle chiavi più grande dello spazio dei messaggi. Se tutte le chiavi sono della stessa lunghezza , allora lo spazio delle chiavi è formato da tutte le stringhe di lunghezza fissata e la chiave deve essere lunga almeno quanto il messaggio. In particolare la lunghezza della chiave OTP è ottimale.

Teorema 3.3.1. Se $(\mathscr{M}, \mathscr{K}, Gen, Enc, Dec)$ è uno schema di cifratura perfettamente sicuro, allora $|\mathscr{K}| \geq |\mathscr{M}|$.

Dimostrazione. Mostriamo che assumendo $|\mathscr{K}| < |\mathscr{M}|$, lo schema non può essere perfettamente sicuro. Consideriamo la distribuzione uniforme su $\mathscr{M}$ e sia $c \in \mathscr{C}$ un testo cifrato che si verifica con probabilità non nulla. Sia $\mathscr{M}(c)$ l'insieme di tutti i messaggi possibili che possono decifrare c, formalmente

$$\mathscr{M}(c) = \{m | m = Dec_k(c) \text{ per qualche } k \in \mathscr{K}\}.$$

Chiaramente $|\mathscr{M}(c)| \leq |\mathscr{K}|$. Se $|\mathscr{K}| < |\mathscr{M}|$, esiste un $m' \in \mathscr{M}$ tale che $m' \notin \mathscr{M}(c)$. Ma allora

$$Pr[M = m' | C = c] = 0 \neq Pr[M = m'],$$

quindi lo schema non è perfettamente sicuro.

Capitolo 4

Crittografia Quantistica

4.1 Il Teorema di No Cloning

Differentemente da un bit classico che può essere copiato, lo stato generico di un qubit non può essere clonato. Questo è il contenuto del teorema di no cloning di Dieks, Wootters e Zurek.

Definizione 4.1.1. Dato uno spazio di Hilbert $\mathscr{H}$, un **operatore di copiatura universale** è una trasformazione unitaria $U : \mathscr{H} \otimes \mathscr{H} \to \mathscr{H} \otimes \mathscr{H}$ tale che, fissato $|\alpha\rangle \in \mathscr{H}$,

$$U|\psi\rangle|\alpha\rangle = |\psi\rangle|\psi\rangle,$$

per ogni $|\psi\rangle \in \mathscr{H}$.

Teorema 4.1.1. Per i sistemi quantistici non esiste un operatore di copiatura universale.

Dimostrazione. Supponiamo che una tale trasformazione U esista. Siano $|\psi_1\rangle, |\psi_2\rangle \in \mathscr{H}$, allora

$$U|\psi_1\rangle|\alpha\rangle = |\psi_1\rangle|\psi_1\rangle,$$
$$U|\psi_2\rangle|\alpha\rangle = |\psi_2\rangle|\psi_2\rangle.$$

Calcoliamo il prodotto scalare dei rispettivi membri:

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

quindi, per definizione di operatore unitario

$$\langle\alpha|\alpha\rangle\langle\psi_1|\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|^2,$$

ovvero

$$\langle\psi_1|\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|^2,$$

verificata quando $\langle\psi_1|\psi_2\rangle = 1$ oppure $\langle\psi_1|\psi_2\rangle = 0$, cioè quando i due stati coincidono o sono ortogonali.

4.2 Distribuzione Quantistica di Chiavi (QKD)

In crittografia classica è impossibile sapere con certezza se un intercettatore Eve stia controllando un messaggio, perché l'informazione classica può essere copiata senza cambiare il messaggio originale. Infatti l'informazione deve essere codificata in un sistema fisico (un pezzo di carta, segnali radio, ecc.), le cui proprietà possono essere misurate *passivamente*. Invece in meccanica quantistica il processo di misurazione disturba il sistema per il principio d'indeterminazione di Heisenberg: se consideriamo una coppia di osservabili che non commutano, la misurazione di un'osservabile disturba (randomizza) l'altra. In questa sezione vedremo che questa proprietà consente il *rilevamento di intrusioni*: Alice e Bob possono scoprire se Eve sta intercettando la loro comunicazione. Questa possibilità può essere usata per creare una chiave privata tra le parti, che consente di comunicare segretamente attraverso il cifrario di Vernam.

4.2.1 Canale Quantistico

Il canale quantistico è composto da:

- un dispositivo ottico di emissione capace di produrre fotoni polarizzati lungo le quattro configurazioni determinate dalle direzioni che formano i rispettivi angoli con l'asse x: $0°, 45°, 90°, 145°$;
- un cavo (es. fibra ottica) su cui viaggiano i fotoni;
- un analizzatore di polarizzazione in possesso del destinatario.

4.2.2 Il Protocollo BB84

Il primo protocollo di scambio della chiave per via quantistica è il BB84, chiamato così perchè sviluppato da Bennet e Brassard nel 1984. Utilizza quattro stati e due basi binarie di trasmissione/ricezione, dette alfabeti:

- $|0\rangle$ e $|1\rangle$ (lo z-alfabeto),
- $|+\rangle \equiv |0\rangle_{\mathrm{x}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle \equiv |1\rangle_{\mathrm{x}} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (l'x-alfabeto),

associati rispettivamente con gli autostati delle matrici di Pauli σ_{z} e σ_{x}.

Algoritmo a passi:

1. Alice sceglie la chiave iniziale K, una sequenza casuale di 1 e di 0.

2. Alice codifica ogni bit in qubit scegliendo casualmente uno degli alfabeti, attraverso una moneta equa:
   $|0\rangle$ o $|+\rangle = |0\rangle_x$ se il bit corrispondente è 0,
   $|1\rangle$ o $|-\rangle = |1\rangle_x$ se il bit corrispondente è 1.

3. Alice trasmette a Bob la stringa risultante di qubit.

4. Bob riceve i qubit e decide a caso quale alfabeto usare per misurare la polarizzazione, x o z.
   Osserviamo che la metà delle volte Bob sceglie lo stesso asse di Alice quindi, assumendo che non ci siano intercettatori o disturbi, condividono lo stesso bit (riassumiamo sotto la parola disturbi: preparazione o rilevazione imperfetta dello stato, interazioni della trasmissione del qubit con l'ambiente ecc.).
   Se invece Bob sceglie un asse diverso da Alice, il bit risultante concorda con il bit inviato da Alice solo metà delle volte.

   Da ora in poi Alice e Bob scambiano solo informazioni classiche attraverso un canale di comunicazione pubblico.

5. Bob comunica ad Alice quale alfabeto ha usato per ogni decodifica di qubit, senza svelare il risultato della ricezione.

6. Alice comunica a Bob quale alfabeto ha usato per ogni codifica di qubit, senza svelare il risultato della trasmissione.

7. Alice e Bob eliminano tutti i bit corrispondenti ai casi in cui hanno utilizzato alfabeti diversi. Dopo condividono la chiave allo stato grezzo RK (acronimo di raw key).

   Per mezzo dei seguenti passaggi, Alice e Bob costruiscono la chiave segreta a partire dalla chiave RK:

8. Alice e Bob si scambiano e comparano una parte della chiave RK per stimare l'*errore percentuale* R, causato da un generico intercettatore Eve o da disturbi.
   Se la percentuale è troppo alta, Alice e Bob ricominciano il protocollo dall'inizio, altrimenti eseguono il processo di *riconciliazione dell'informazione* e *amplificazione della privacy* sui rimanenti bit della RK.

9. La riconciliazione dell'informazione è un codice di correzione classico dell'errore: Alice e Bob dividono i rimanenti bit della RK in sottoinsiemi di lunghezza l, scelta in modo tale che sia improbabile che ci sia più di un errore per sottoinsieme ($Rl \ll 1$). Per ogni sottoinsieme, Alice e Bob fanno il controllo di parità (la parità P di una stringa binaria $\{b_1,b_2,...,b_l\}$ è definita come $P=b_1 \oplus b_2 \oplus ... \oplus b_l$), scartando ogni

volta l'ultimo bit. Se le parità di un dato sottoinsieme sono differenti tra Alice e Bob, questi individuano ed eliminano il bit errato attraverso la ricerca binaria nel modo seguente: dividono il sottoinsieme in due, cercano le parità dei nuovi blocchi $P_1 = b_1 \oplus b_2 \oplus ... \oplus b_{(l-1)/2}$ e $P_2 = b_{(l-1)/2+1} \oplus b_{(l-1)/2+2} \oplus ... \oplus b_{l-1}$), ripetono la bisezione sul blocco in cui le parità sono differenti e così via. Ogni volta Alice e Bob cancellano l'ultimo bit dei blocchi la cui parità viene annunciata pubblicamente, impedendo a Eve di ottenere informazioni dai loro controlli di parità. Alla fine, con molta probabilità, Alice e Bob hanno la stessa stringa di bit.

10. L'amplificazione della privacy riduce a valori arbitrariamente piccoli le informazioni di Eve sulla chiave finale segreta, attraverso il seguente protocollo:
sia s un parametro di sicurezza e n il numero di bit rimanenti della chiave, Alice e Bob stimano (attraverso l'errore percentuale R) il numero massimo k di bit conosciuti da Eve e scelgono a caso n - k - s sottoinsiemi della loro chiave; le parità di questi sottoinsiemi diventano la chiave finale, molto più sicura di quella precedente poiché Eve deve conoscere ogni bit di un sottoinsieme per ottenere informazioni sulla sua parità.

Osserviamo che non essendo noto alcun meccanismo per l'autenticazione, è richiesta una chiave di autenticazione su un canale sicuro classico per essere certi di non comunicare con qualcun altro.

4.2.3 Intercept and Resend

La strategia di intercettazione più semplice è l'*intercept and resend*, in cui Eve intercetta e rileva i qubit inviati da Alice soltanto la metà delle volte.
Se indovina la base di codifica, Eve riesce ad ottenere il corretto qubit senza alterarne lo stato ed in seguito lo invia a Bob, intervenendo così in modo perfettamente trasparente. Altrimenti, se Eve sceglie una base diversa, lo stato da inviare a Bob risulterà alterato rispetto a quello inviato da Alice. Inoltre la probabilità che Bob scelga la stessa base di Alice è $\frac{1}{2}$, quindi la probabilità che un qubit intercettato generi un errore nella stringa delle chiavi è di $\frac{1}{2}\frac{1}{2} = \frac{1}{4}$.
Se Alice e Bob confrontano n bit della chiave, la probabilità che questi siano concordi è pari a

$$\left(\frac{3}{4}\right)^n \xrightarrow{n\to\infty} 0,$$

quindi la probabilità che siano discordi è

$$1 - \left(\frac{3}{4}\right)^n \xrightarrow{n\to\infty} 1.$$

Ad esempio, per individuare un avversario con probabilità pari a 0.999999999, Alice e Bob hanno bisogno di confrontare $n = 72$ bits della chiave.

Indipendentemente dalla strategia di intercettazione, è possibile mostrare che la QKD è sicura, nel senso che è possibile garantire che l'informazione di Eve sulla chiave sia un numero arbitrariamente piccolo.
Sottolineiamo che la validità del protocollo BB84 è basata sul principio di indeterminazione di Heisenberg. I due alfabeti sono associati con σ_z e σ_x ed Eve non può misurare per lo stesso qubit sia la polarizzazione lungo l'asse x sia lungo z.
Sottolineiamo inoltre l'importanza del teorema di no cloning: garantisce che Eve non possa distinguere con certezza stati quantistici non ortogonali.

Conclusioni

I limiti del protocollo BB84 sono innanzitutto di tipo tecnologico, perché legati alla difficoltà di realizzare dispositivi che lavorino con singoli fotoni e con errori di trasmissione limitati. Inoltre l'architettura del sistema affida la propria sicurezza alla crittografia a chiave simmetrica e non alla crittografia quantistica, che viene utilizzata solo per l'interscambio della chiave, rappresentando un limite di tutti i sistemi QKD.
Ma negli ultimi anni sono stati effettuati molti esperimenti e contestualmente sviluppati dei sistemi che potrebbero essere la chiave di volta per rendere sicure le comunicazioni.
Il 20 dicembre 2018 è stata pubblicata una ricerca italiana sulla rivista "Quantum Science and Technology" dell'Institute of Physics inglese, frutto della collaborazione tra il gruppo di ricerca QuantumFuture del Dipartimento di Ingegneria dell'Informazione dell'Università di Padova e l'osservatorio Matera Laser Ranging Observatory (Mlro) che dimostra l'applicabilità della crittografia quantistica nella gestione dei sistemi di navigazione satellitare: realizzando lo scambio di pochi fotoni per impulso tra due satelliti diversi della costellazione Glonass e Mlro, ha esteso il risultato record delle comunicazioni quantistiche a una distanza di 20000 km.
Inoltre nello studio intitolato "All-fiber self-compensating polarization encoder for Quantum Key Distribution" e pubblicato dalla rivista ≪Optics Letters≫, il gruppo QuantumFuture ha proposto un nuovo sistema per codificare efficientemente e rapidamente i qubit nella polarizzazione dei singoli fotoni. ≪Ci si aspetta che la QKD abbia un profondo impatto sulla privacy e sulla sicurezza dei cittadini - dice Giuseppe Vallone che ha guidato questa ricerca all'interno del gruppo coordinato dal co-autore Paolo Villoresi - Il nostro schema semplifica la generazione di qubit codificati nella polarizzazione dei fotoni. La polarizzazione è in particolare la codifica più adatta alle comunicazioni quantistiche in spazio libero, come da satellite verso Terra o tra i terminali mobili, in quanto non viene perturbata durante la propagazione≫.
Lo sviluppo della QKD ha suscitato negli ultimi anni grande interesse da parte della comunità scientifica globale, ricevendo importanti finanziamenti sia dal settore privato che da quello pubblico, come dimostrato dall'avvio della Quantum Flagship, un investimento europeo da un miliardo di euro per sviluppare queste nuove tecnologie nell'arco dei prossimi dieci anni.

I sistemi di navigazione satellitare (Gnss) sono infrastrutture di importanza strategica a livello mondiale che permettono a dispositivi elettronici dotati di appositi ricevitori, di localizzarsi precisamente in un qualsiasi punto della Terra, un servizio oggi fondamentale per governi, istituzioni e cittadini. Motivo per cui i responsabili dello sviluppo di questi sistemi ne stanno considerando l'utilizzo per rendere sicure sia le comunicazioni intra-satellitari all'interno della costellazione, che quelle tra i satelliti e le stazioni a terra.

Bibliografia

[1] Giuliano Benenti, Giulio Casati, Giuliano Strini, *Principles of Quantum Computation and Information, Volume I: Basic Concepts,* World Scientific, (2004)

[2] Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography, Second Edition,* CRC Press, (2014)

[3] Raphael Pass, Abhi Shelat, *A Course in Cryptography,* Disponibile online, (2010)

[4] Charles Bennett, Gilles Brassard, *Proceedings of IEEE International Conference on Computers,* Systems and Signal Processing, New York, (1984)

[5] Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press, (2000)

[6] Preskill, *Lecture Notes for Physics: Quantum Information and Computation,* California Institute of Technology, (1998)