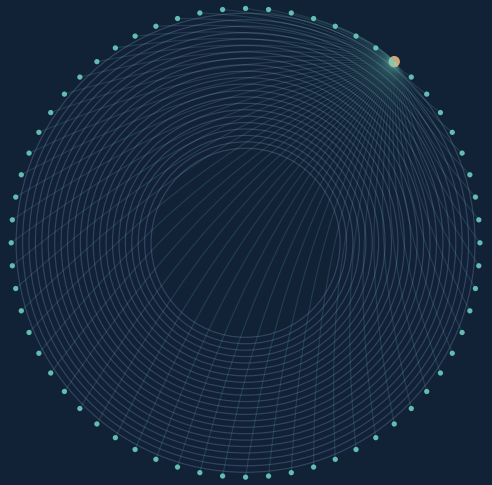
CALCOLO QUANTISTICO

Protocolli quantistici

BB84 e criticità della QKD
Codifica superdensa
Correzione degli errori



Stati, circuiti e comunicazioni protette

Indice

BB84 permette di costruire una chiave condivisa. La codifica superdensa usa una coppia entangled per trasmettere due bit. La correzione degli errori protegge le ampiezze di un qubit logico. Ogni sezione sviluppa il problema, le operazioni e un esempio di calcolo.

Parte	Argomento	Slide
Strumenti	Stati, porte e basi di misura	3–9
01	BB84: costruire una chiave condivisa	10–28
02	QKD: requisiti e criticità di impiego	29–45
03	Codifica superdensa ed entropia	46–56
04	Correzione degli errori quantistici	57–98
Conclusione	Sintesi e riferimenti	99–100

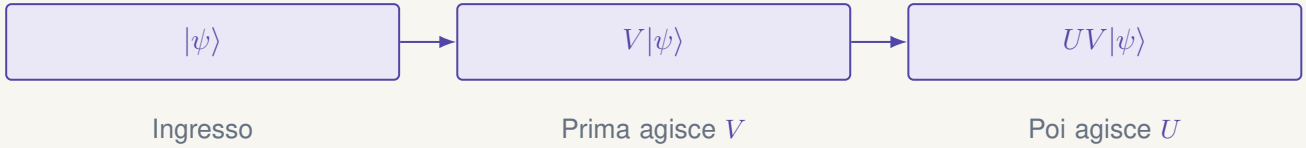
Richiami Prerequisiti: vettori e matrici, prodotto scalare e probabilità elementari. Le definizioni vengono introdotte nell'ordine di lettura delle slide.

Stati, registri e ordine delle operazioni

Un **registro** è un insieme di qubit. Il suo stato si scrive nell'ordine $|x_{n-1}\cdots x_0\rangle$: il qubit 0 è quello più a destra. La scrittura $|x\rangle|y\rangle$ abbrevia il prodotto tensoriale $|x\rangle \otimes |y\rangle$, cioè lo stato congiunto dei due sistemi.

Gli indici sulle porte indicano i qubit coinvolti: C_{ij} è una CNOT con controllo i e bersaglio j. Nel prodotto $UV|\psi\rangle$ agisce prima V e poi U; nel circuito le stesse porte si incontrano da sinistra verso destra.

Circuito: $|\psi\rangle \longrightarrow V \longrightarrow U$



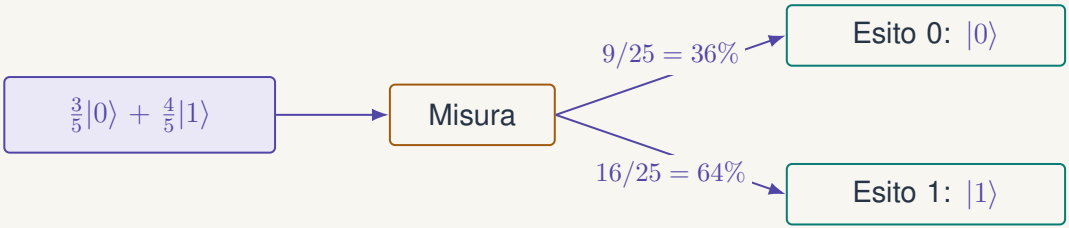
Richiami $|\psi\rangle$ è un vettore di stato; $\langle\phi|\psi\rangle$ è un prodotto scalare; I è l'identità e $\oplus$ è la somma modulo 2.

Uno stato e le probabilità di misura

Lo stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ determina le probabilità di una misura nella base computazionale. Le ampiezze complesse α e β soddisfano $|\alpha|^2 + |\beta|^2 = 1$, così che i due esiti esauriscano tutte le possibilità:

$$P(0) = |\alpha|^2, \qquad P(1) = |\beta|^2.$$

Per $\alpha = 3/5$ e $\beta = 4/5$, le probabilità sono $9/25$ e $16/25$. Letto l'esito, lo stato del qubit diventa rispettivamente $|0\rangle$ oppure $|1\rangle$.



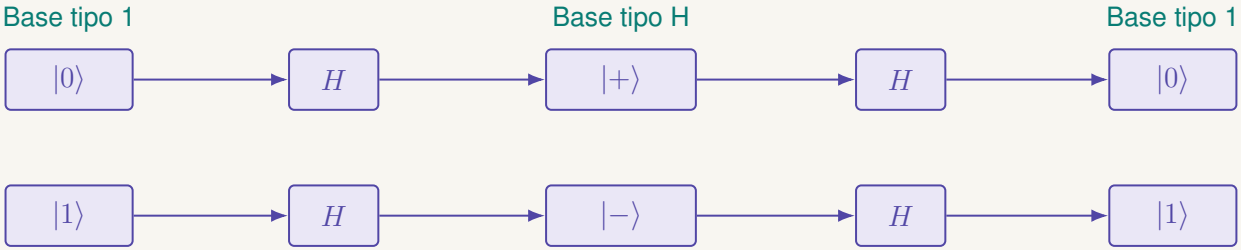
Richiami La regola di Born associa a ogni esito il modulo quadro della sua ampiezza.

Le due basi usate da BB84

Una base di misura è un insieme di stati ortogonali associati agli esiti distinguibili. Per un qubit contiene due stati. BB84 usa due basi: la prima contiene $|0\rangle$ e $|1\rangle$; la seconda si ottiene applicando Hadamard ai due stati:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Indichiamo queste basi con 1 e H. Una misura nella base H si realizza applicando Hadamard prima della misura ordinaria: $H|+\rangle = |0\rangle$ e $H|-\rangle = |1\rangle$.



Richiami La base 1 è $\{|0\rangle, |1\rangle\}$; la base H è $\{|+\rangle, |-\rangle\}$. In entrambi i casi i due stati sono ortogonali.

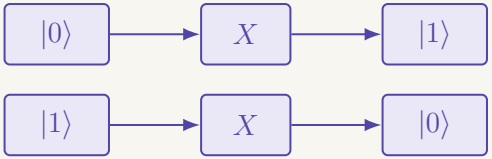
Scambi di bit e cambi di fase

Una variazione dello stato può riguardare i valori della base oppure la fase relativa delle componenti. La porta X scambia le due ampiezze; la porta Z cambia il segno della componente su $|1\rangle$:

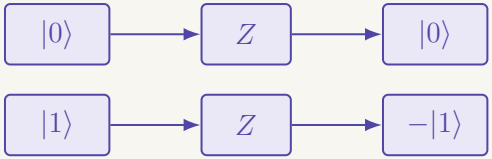
$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle, \qquad Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle.$$

Il cambio di base collega i due effetti: $HXH = Z$ e $HZH = X$. Le stesse operazioni serviranno sia a codificare messaggi sia a descrivere errori.

Inversione di bit



Cambio di fase



$$H \longrightarrow Z \longrightarrow H \quad = \quad X$$

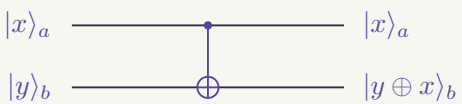
Richiami Una fase relativa distingue, per esempio, $|+\rangle$ da $|-\rangle$: dopo Hadamard si leggono rispettivamente 0 e 1.

La CNOT e le correlazioni fra due qubit

Sui vettori della base computazionale, la CNOT mantiene il valore del controllo e somma quel valore al bersaglio modulo 2. Se il controllo è 0 il bersaglio rimane uguale; se è 1 il bersaglio viene invertito.

$$C_{ab}|x\rangle_a|y\rangle_b = |x\rangle_a|y \oplus x\rangle_b.$$

Per una sovrapposizione si applica la regola a ciascun termine e si mantengono le sue ampiezze. La CNOT può così correlare i due qubit. Due CNOT consecutive sugli stessi fili si annullano, perché $(y \oplus x) \oplus x = y$.



Ingresso	Uscita
00	00
01	01
10	11
11	10

Il punto pieno indica il controllo; il cerchio con il segno più indica il bersaglio.

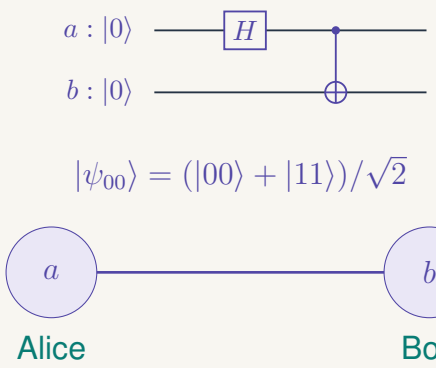
Richiami C_{ab} ha controllo sul filo a e bersaglio sul filo b; $C_{ab}^2 = I$.

Preparare una coppia di Bell

Per ottenere una coppia entangled partiamo da $|00\rangle$. Hadamard crea sul primo qubit due componenti con la stessa ampiezza. La CNOT inverte poi il secondo qubit soltanto nella componente in cui il primo vale 1:

$$|00\rangle \xrightarrow{H_a} \frac{|00\rangle + |10\rangle}{\sqrt{2}} \xrightarrow{C_{ab}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\psi_{00}\rangle.$$

Una misura di entrambi i qubit nella base computazionale restituisce 00 oppure 11, ciascuno con probabilità $1/2$. Il risultato locale è casuale, mentre i due risultati sono sempre uguali.



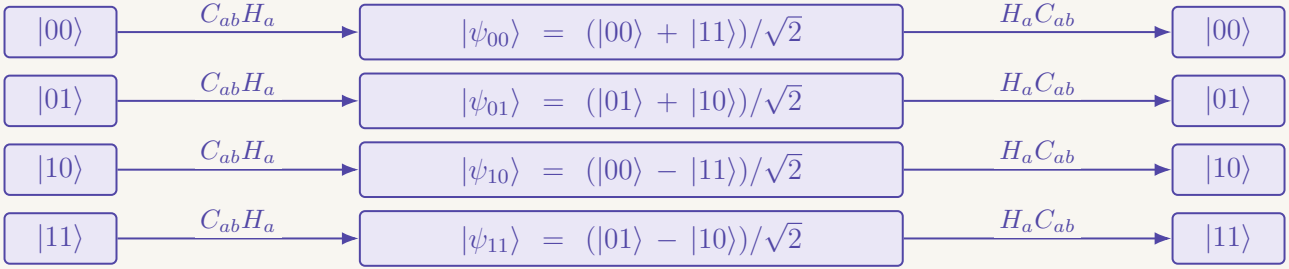
La coppia si prepara applicando prima Hadamard e poi CNOT.

Richiami Uno stato puro è entangled quando non si può scrivere come prodotto degli stati dei singoli qubit.

Quattro stati di Bell, quattro esiti

Applicando il circuito $C_{ab}H_a$ ai quattro stati $|xy\rangle$ si ottengono quattro stati di Bell. Poiché il circuito è unitario, conserva l'ortogonalità: le quattro uscite costituiscono una nuova base dello spazio di due qubit.

Per distinguerle, applichiamo il circuito inverso H_aC_{ab}. Ogni stato di Bell torna nel corrispondente $|xy\rangle$ e due misure ordinarie ne leggono le etichette. Questa procedura realizza una misura nella base di Bell.



Richiami Una trasformazione unitaria conserva ortogonalità e normalizzazione.

CAPITOLO 01

BB84 e distribuzione delle chiavi

Preparazione, misura e confronto delle basi
Il controllo del disturbo sul canale

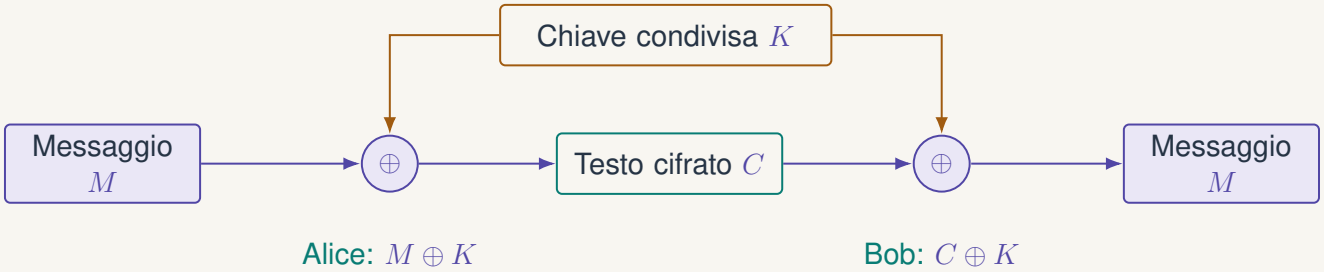
Mermin, §6.2, pp. 137–143

Una chiave casuale condivisa

Alice vuole inviare un messaggio M a Bob. Se condividono una stringa segreta K, scelta uniformemente, indipendente da M, lunga quanto il messaggio e usata una sola volta, possono usarla per un one-time pad. Alice trasmette $C = M \oplus K$ e Bob recupera il messaggio con la stessa operazione:

$$C \oplus K = M \oplus K \oplus K = M.$$

La disponibilità di nuove chiavi condivise diventa quindi una risorsa essenziale. BB84 affronta la loro distribuzione attraverso la preparazione e la misura di qubit.



Richiami Lo XOR è applicato posizione per posizione: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$.

Un esempio di one-time pad

Lo XOR agisce su ciascuna posizione in modo indipendente: un bit 0 della chiave lascia invariato il bit del messaggio, mentre un bit 1 lo inverte. Consideriamo due stringhe di otto bit:

$$\begin{aligned} M &= 10110010 \\ K &= 01101001 \\ \hline C = M \oplus K &= 11011011 \\ C \oplus K &= 10110010 \end{aligned}$$

Bob ripete le stesse inversioni. Le posizioni modificate da Alice vengono invertite una seconda volta, e il messaggio torna alla forma iniziale. A chi conosce soltanto C, ogni messaggio possibile corrisponde a una diversa chiave K. Con una chiave uniforme e indipendente, il testo cifrato lascia inalterate le probabilità dei possibili messaggi.

Richiami Una chiave uniforme di otto bit ammette 2^8 valori equiprobabili.

Una chiave nuova per ogni messaggio

Il riuso di una chiave crea una relazione visibile fra i messaggi. Se Eve, l'avversaria che ascolta il canale, intercetta due testi cifrati con la stessa stringa K, può calcolarne lo XOR; i due contributi della chiave si cancellano:

$$C_1 = M_1 \oplus K, \quad C_2 = M_2 \oplus K, \quad C_1 \oplus C_2 = M_1 \oplus M_2.$$

Rimane così un vincolo fra i testi originali. Le loro regolarità possono aiutare a ricostruirli. Ogni messaggio cifrato con un one-time pad richiede perciò una chiave nuova, uniforme e segreta: Alice e Bob devono rifornire continuamente la loro riserva comune.

Richiami La cancellazione della chiave deriva dall'identità $K \oplus K = 0$.

Le quattro preparazioni di Alice

Alice compie due scelte casuali per ogni trasmissione: un bit x e una base. Le scelte sono indipendenti ed equiprobabili. La base stabilisce quale coppia di stati usare; il bit individua uno dei due stati della coppia.

Si ottengono così le quattro preparazioni $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, ciascuna con probabilità $1/4$. Alice conserva un registro della base e del bit: in seguito renderà pubblica la base, lasciando riservata la scelta del bit.

	Bit 0	**Bit 1**
Base 1	$\|0\rangle \quad P = 1/4$	$\|1\rangle \quad P = 1/4$
Base H	$\|+\rangle \quad P = 1/4$	$\|-\rangle \quad P = 1/4$

Richiami BB84 prende il nome da Bennett e Brassard e dall'anno 1984.

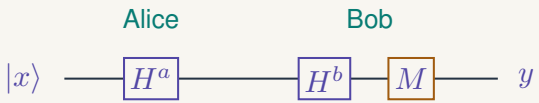
La scelta di misura di Bob

Bob riceve il qubit prima di conoscere la base scelta da Alice. Decide quindi casualmente come misurarlo. Nella base 1 effettua la misura ordinaria; nella base H la precede con Hadamard.

Chiamiamo y l'esito della misura di Bob e indichiamo le scelte delle basi con $a, b \in \{0, 1\}$, dove 0 significa base 1 e 1 significa base H. Lo stato immediatamente prima della misura è

$$H^b H^a |x\rangle = H^{a \oplus b} |x\rangle.$$

Se $a = b$, le trasformazioni restituiscono $|x\rangle$. Se $a \neq b$, rimane una Hadamard e i due esiti sono equiprobabili. Dalla coincidenza delle basi dipende dunque la possibilità di recuperare il bit.



M indica la misura nella base computazionale. I bit a e b sono scelte classiche.

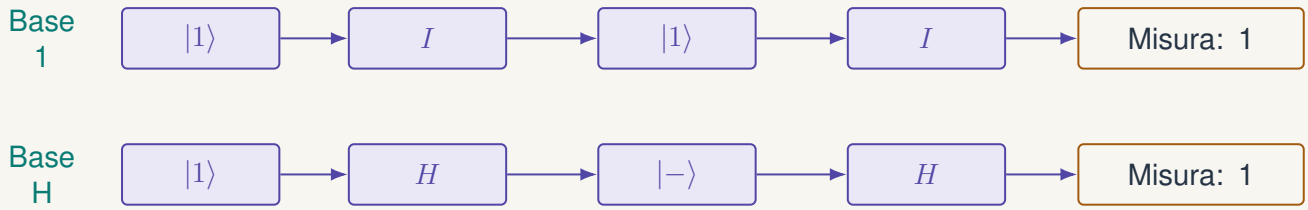
Richiami $H^0 = I$, $H^1 = H$ e $H^2 = I$.

Basi uguali: il bit viene recuperato

Quando Alice e Bob scelgono la stessa base, la preparazione e il cambio di base alla ricezione si compensano. Nel caso della base H questa proprietà segue da $H^2 = I$:

$$H(H|0\rangle) = |0\rangle, \qquad H(H|1\rangle) = |1\rangle.$$

Nella base H, per rappresentare il bit 1 Alice prepara $|-\rangle$. Bob lo trasforma in $|1\rangle$ e legge 1 con certezza. Perciò, nel collegamento ideale, $P(y = x \mid a = b) = 1$.



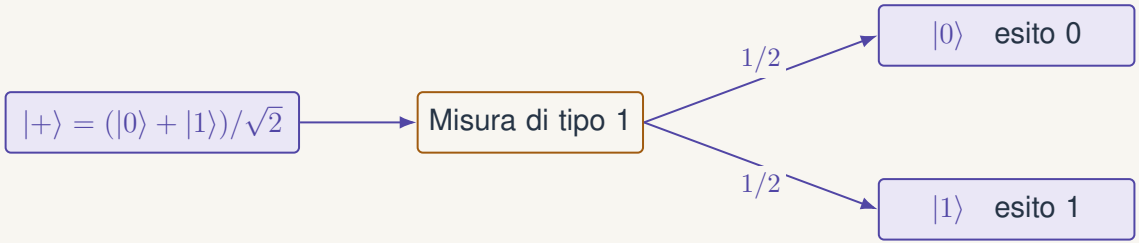
Richiami La probabilità è calcolata dopo tutte le operazioni che precedono la misura.

Basi diverse: due esiti equiprobabili

Consideriamo ora Alice che prepara $|+\rangle$ e Bob che misura nella base computazionale. Nella base scelta da Bob, lo stato ha due ampiezze di modulo $1/\sqrt{2}$; la regola di Born assegna probabilità uguali agli esiti:

$$P(y = 0 \mid a \neq b) = P(y = 1 \mid a \neq b) = \frac{1}{2}.$$

Lo stesso accade per tutte le preparazioni lette nell'altra base. Questi risultati sono indipendenti dal bit di Alice e vengono scartati nel confronto successivo.



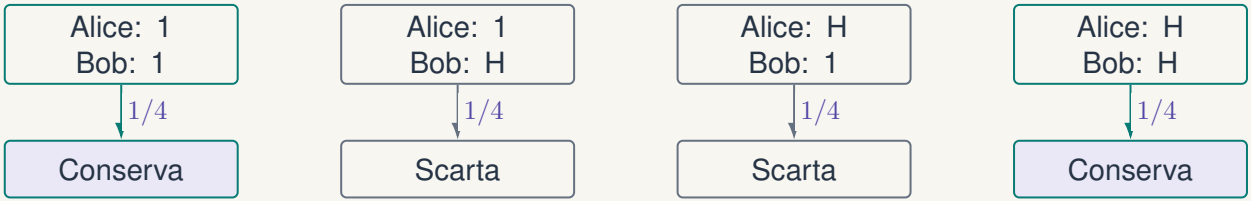
Richiami Le probabilità dipendono dai moduli quadrati: $|1/\sqrt{2}|^2 = |-1/\sqrt{2}|^2 = 1/2$.

Confrontare le basi e selezionare i dati

Terminate le misure, Alice annuncia le basi e Bob indica le posizioni in cui ha usato la stessa base. Conservando soltanto quelle posizioni, i due estraggono sequenze correlate. Questa selezione prende il nome di *sifting*.

$$P(a = b) = \frac{1}{2}, \qquad \mathbb{E}[n_{\text{sel}}] = \frac{N_{\text{ricevuti}}}{2}.$$

Il confronto rende pubbliche le basi, mentre i bit rimangono riservati. I messaggi classici devono essere autenticati, così che ciascun partecipante possa riconoscere l'interlocutore.



Due casi su quattro: $P(a = b) = 1/2$

Richiami N_{ricevuti} conta i qubit rilevati da Bob; n_{sel} conta le basi coincidenti. $E[n_{\text{sel}}]$ è la media su molte esecuzioni.

Nove trasmissioni, quattro bit condivisi

Seguiamo nove trasmissioni. Ogni colonna riporta la preparazione di Alice e la misura di Bob. Il confronto fra le due righe delle basi stabilisce quali posizioni conservare.

Posizione	1	2	3	4	5	6	7	8	9
Base di Alice	1	H	H	H	1	1	H	1	H
Bit di Alice	0	1	0	1	1	0	1	0	0
Base di Bob	H	H	H	1	1	H	1	1	1
Esito di Bob	1	1	0	0	1	1	1	0	0
Si conserva?	–	sì	sì	–	sì	–	–	sì	–

Le basi coincidono nelle posizioni 2, 3, 5 e 8: entrambe le sequenze selezionate sono 1010. Una coincidenza casuale dei bit nelle altre colonne viene comunque scartata. La selezione dipende dalla base, che garantisce la correlazione nel modello ideale.

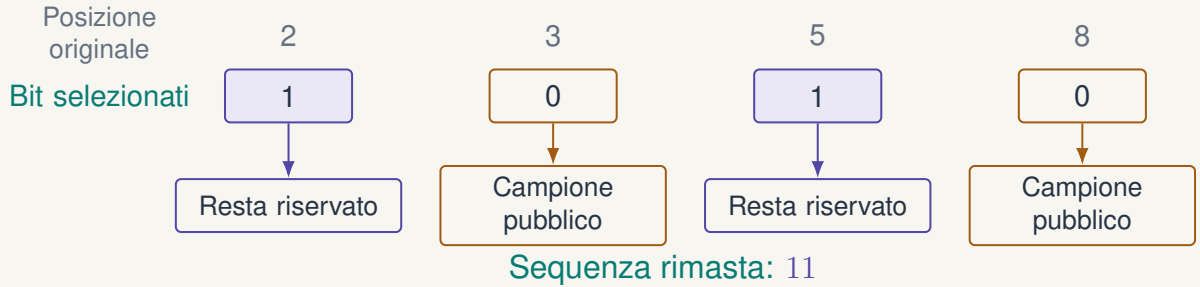
Richiami Una media probabilistica descrive molte esecuzioni; il numero effettivo varia da una sequenza all'altra.

Il campione di controllo

La coincidenza delle basi indica quali bit dovrebbero essere uguali. Per controllare il collegamento, Alice e Bob estraggono casualmente un campione delle posizioni conservate, pubblicano i valori e contano i disaccordi:

$$q_{\text{oss}} = \frac{\text{disaccordi nel campione}}{\text{bit confrontati}}.$$

Nell'esempio precedente confrontiamo le posizioni 3 e 8, entrambe uguali a 0. Restano i bit delle posizioni 2 e 5, cioè 11. I bit rivelati nel controllo vengono eliminati dalla sequenza riservata.



Richiami Nell'esempio $q_{\text{oss}} = 0/2 = 0$. Due confronti illustrano la procedura; la valutazione statistica dipende dalla dimensione del campione.

Intercettare, misurare e reinviare

Eve intercetta il qubit mentre viaggia verso Bob. Sceglie con uguale probabilità una delle due basi, misura e invia un nuovo qubit nello stato corrispondente al risultato. Questo attacco è chiamato intercetta–misura–reinvia.

Quando la base scelta da Eve coincide con quella di Alice, la misura conserva lo stato trasmesso. Con l'altra base, Eve ottiene uno dei due risultati casuali e reinvia uno stato diverso dalla preparazione originaria.

Il disturbo si manifesta anche nelle posizioni in cui Alice e Bob hanno usato basi uguali. Sono proprio queste le posizioni che entreranno nel campione di controllo e potranno rivelare l'intercettazione.

Alice
Prepara $H^a|x\rangle$.

↓

Eve
Misura nella base scelta e reinvia.

↓

Bob
Misura; Alice e Bob selezionano $a = b$.

L'intervento di Eve è collocato sul canale quantistico.

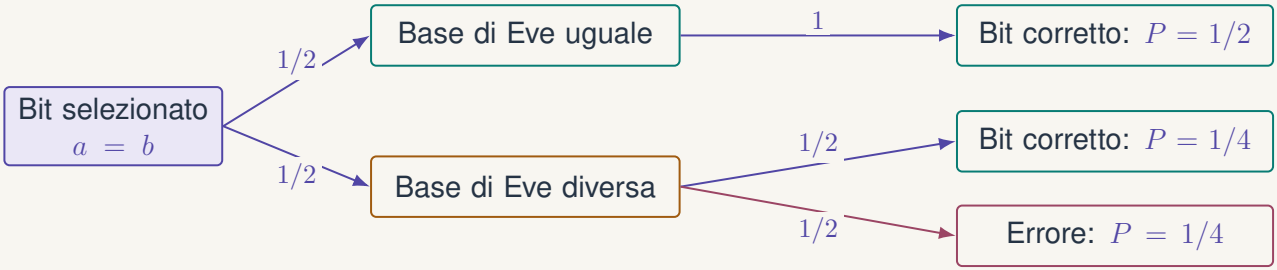
Richiami Il calcolo seguente riguarda l'attacco intercetta–misura–reinvia con scelta uniforme delle basi.

Da dove viene il tasso di errore del 25%

Limitiamoci alle posizioni conservate, per le quali $a = b$, e supponiamo che Eve intercetti ogni qubit. Nella metà dei casi sceglie la base giusta e il bit arriva integro. Nell'altra metà prepara uno stato che Bob legge correttamente soltanto con probabilità $1/2$.

$$P(\text{errore} \mid a = b) = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}.$$

Il 25% nasce dunque da due eventi successivi: la base sbagliata di Eve e il risultato casuale della misura di Bob.



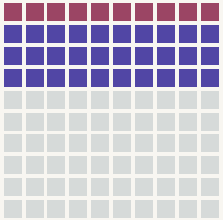
Richiami Attacco intercetta–misura–reinvia, basi equiprobabili e apparati ideali. La percentuale riguarda i bit selezionati.

Intercettare soltanto una frazione dei qubit

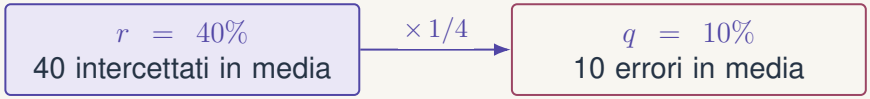
Eve può ridurre il disturbo intercettando una frazione r dei qubit, scelta indipendentemente dalle basi. Nel collegamento ideale la parte intercettata contribuisce con tasso d'errore $1/4$, mentre la parte restante conserva il bit:

$$q = r \cdot \frac{1}{4} + (1 - r) \cdot 0 = \frac{r}{4}.$$

Con $r = 0{,}40$, il disaccordo atteso è il 10% dei bit selezionati. Per esempio, su 100 bit selezionati ci attendiamo in media 10 disaccordi.



100 bit selezionati



Viola: intercettati con bit corretto. Rosa: disaccordi.
Grigio: qubit che proseguono senza intercettazione.

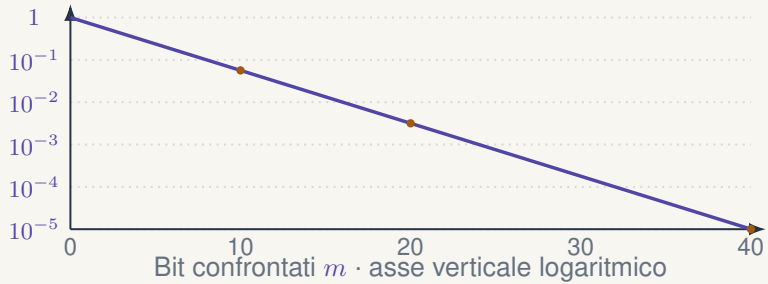
Richiami La relazione assume apparati ideali e considera come unica causa di errore l'attacco intercetta–misura–reinvia.

Dimensione del campione e rilevazione dell’attacco

Anche in presenza di intercettazione totale, alcuni confronti danno risultati uguali. Per ogni bit la probabilità è $3/4$. Se il campione contiene m bit indipendenti, tutti i confronti coincidono con probabilità

$$P(\text{attacco non rilevato}) = \left(\frac{3}{4}\right)^m .$$

Passando da 10 a 40 bit di controllo, il rischio scende da circa $5{,}6\%$ a circa $0{,}001\%$. Un campione più ampio rende più difficile che il disturbo sfugga alla verifica.



$m = 10 \quad P = 0{,}0563$

$m = 20 \quad P = 0{,}00317$

$m = 40 \quad P = 0{,}0000101$

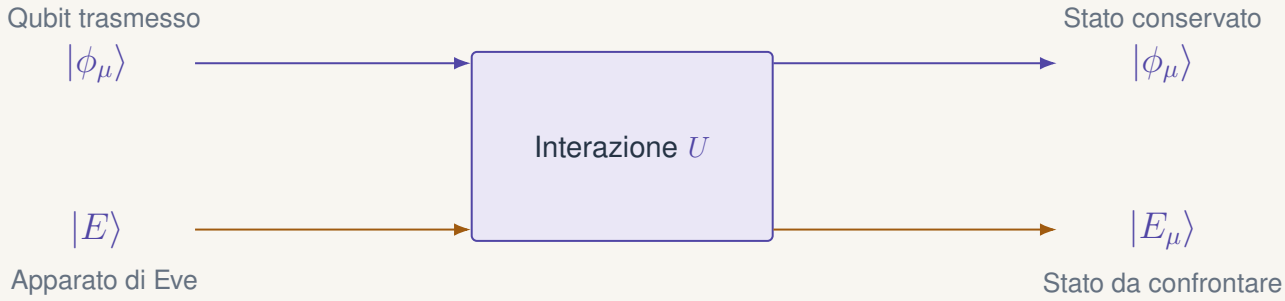
Richiami Attacco totale intercetta–misura–reinvia, campione di bit indipendenti e apparati ideali: ciascun confronto passa con probabilità $3/4$.

Informazione acquisita e disturbo prodotto

Un'interazione più generale può coinvolgere il qubit e un apparato di Eve inizialmente in $|E\rangle$. Supponiamo che l'interazione lasci intatto ciascuno dei quattro stati trasmessi:

$$U(|\phi_\mu\rangle|E\rangle) = |\phi_\mu\rangle|E_\mu\rangle, \qquad |\phi_\mu\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}.$$

Per ricavare informazione, Eve avrebbe bisogno di stati finali $|E_\mu\rangle$ distinguibili. L'unitarietà dell'interazione vincola proprio questa possibilità, perché conserva i prodotti scalari.



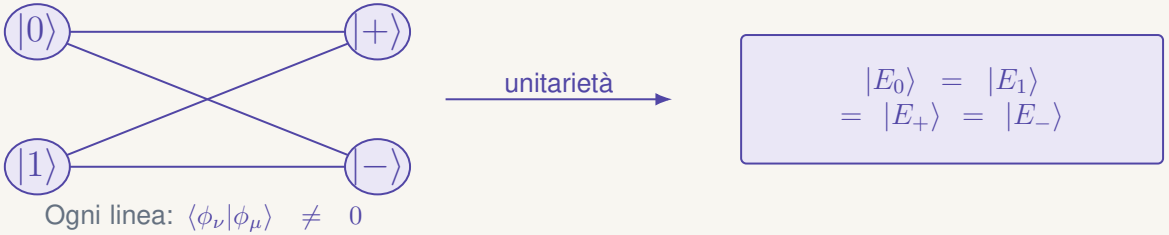
Richiami Un operatore unitario soddisfa $\langle Uv|Uw\rangle = \langle v|w\rangle$.

La conservazione dei prodotti scalari

Consideriamo, per esempio, le preparazioni $|0\rangle$ e $|+\rangle$. Il loro prodotto scalare è $1/\sqrt{2}$. Poiché l'interazione conserva entrambi gli stati, l'unitarietà impone

$$\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}}\langle E_0|E_+\rangle \quad \Longrightarrow \quad \langle E_0|E_+\rangle = 1.$$

Due vettori normalizzati con prodotto scalare 1 coincidono. Lo stesso argomento vale per le altre coppie collegate nel diagramma: tutti gli stati finali dell'apparato sono uguali. Eve ottiene quindi la stessa descrizione del proprio apparato per ogni bit e per ogni base.



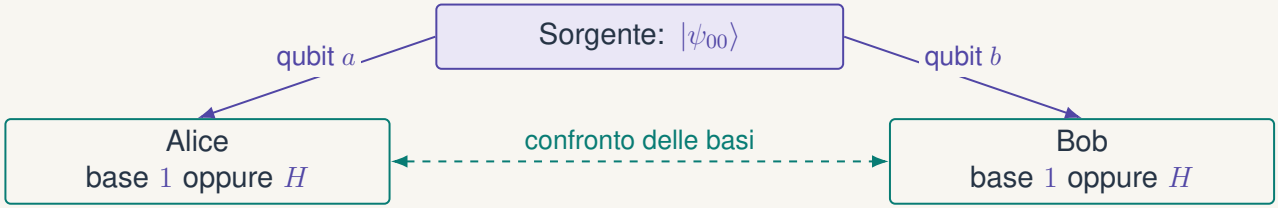
Richiami Se tutti gli stati trasmessi restano intatti, l'apparato di Eve termina nello stesso stato per ogni preparazione: nessuna scelta del bit vi rimane registrata.

La versione con coppie entangled

La stessa correlazione può essere ottenuta distribuendo una coppia di Bell, con un qubit ad Alice e uno a Bob. Ciascuno sceglie indipendentemente la base 1 oppure H. L'identità

$$(H \otimes H)|\psi_{00}\rangle = |\psi_{00}\rangle$$

garantisce bit uguali quando le basi coincidono. Se Alice misura per prima, il suo risultato prepara sul qubit di Bob uno dei quattro stati di BB84. La selezione delle basi e il controllo del campione procedono quindi nello stesso modo.



Basi uguali $\Longrightarrow$ bit uguali: 00 oppure 11, con probabilità $1/2$

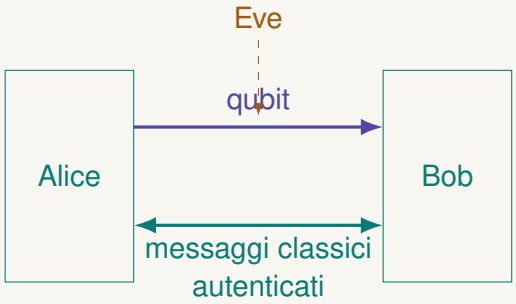
Richiami $|\psi_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ dà correlazioni uguali nelle basi 1 e H.

BB84 nel sistema di comunicazione

La selezione delle basi produce una sequenza candidata. Il campione di controllo stima i disaccordi; i valori pubblicati vengono eliminati. Nel modello ideale senza disturbo, le sequenze rimaste ad Alice e Bob coincidono.

La probabilità $(3/4)^m$ riguarda l'attacco intercetta–misura–reinvia studiato. Per un collegamento rumoroso, la scelta di accettare o scartare i dati richiede un'analisi di sicurezza e un'elaborazione classica adeguate.

La chiave viene poi utilizzata in un servizio che deve autenticare gli interlocutori, custodire i segreti e cifrare i messaggi. Sono questi i requisiti esaminati nella sezione seguente.



Il canale quantistico e quello classico svolgono funzioni complementari.

Richiami La parte su BB84 sviluppa il modello introduttivo e l'attacco intercetta–misura–reinvia; la sicurezza di un sistema completo richiede anche il trattamento del rumore.

CAPITOLO 02

La QKD nelle comunicazioni protette

Autenticazione, protezione dei dati e condizioni operative della rete

Impieghi governativi e militari • Valutazione dell’11 agosto 2026

Dalla chiave alla sicurezza dell'intero servizio

Proteggere una comunicazione richiede quattro proprietà. La **riservatezza** limita la lettura del contenuto ai destinatari autorizzati. L'**integrità** permette di rilevare modifiche. L'**autenticità** consente di verificare l'origine dei messaggi. La **disponibilità** permette agli utenti di usare il servizio quando occorre.

La QKD fornisce chiavi da consegnare agli apparati di cifratura. Il servizio comprende anche generatori casuali, autenticazione e gestione dei segreti. Una debolezza in una di queste componenti può compromettere la comunicazione pur lasciando corretto lo scambio quantistico.

La valutazione delle informazioni classificate riguarda perciò tutte le componenti attraversate dai dati.



La chiave entra in un servizio che deve garantire tutte e quattro le proprietà.

Richiami Il criterio di valutazione comprende riservatezza, integrità, autenticità e disponibilità.

La raccolta dei dati e la decifrazione futura

La minaccia quantistica riguarda i sistemi asimmetrici la cui sicurezza dipende da problemi risolvibili da un computer quantistico sufficientemente potente. La sigla CRQC, da *Cryptographically Relevant Quantum Computer*, indica un computer quantistico capace di compromettere i sistemi crittografici considerati.

L'attacco può iniziare prima che tale capacità sia disponibile. Un avversario intercetta i dati cifrati, li conserva e attende di poterli decifrare. È lo scenario chiamato *store-now, decrypt-later*.

Di conseguenza, la durata richiesta della riservatezza entra nella scelta dei tempi di migrazione. Un messaggio che deve rimanere segreto a lungo va protetto considerando anche le capacità future dell'avversario.



Richiami La riservatezza richiesta nel tempo lega la scelta della protezione alle capacità future dell'avversario.

PQC, QKD e chiavi precondivise

La **crittografia post-quantistica** (PQC) usa problemi matematici ritenuti difficili anche per un avversario quantistico. Comprende due funzioni distinte: i meccanismi di incapsulamento stabiliscono un segreto condiviso; le firme digitali autenticano messaggi e certificati.

La **distribuzione quantistica di chiavi** (QKD) combina stati inviati su un canale quantistico e messaggi classici autenticati. La garanzia sul segreto dipende dalle ipotesi fisiche e dai controlli del protocollo.

Con la **precondivisione**, gli interlocutori ricevono una chiave simmetrica attraverso un mezzo sicuro prima di comunicare. L'organizzazione deve provvedere alla distribuzione e alla custodia dei segreti.

PQC
Problemi matematici; chiavi e firme

QKD
Stati quantistici; chiave condivisa

Precondivisione
Distribuzione preventiva dei segreti

Richiami La scelta comprende il metodo di formazione della chiave e il modo in cui si verificano le identità.

1. L’identità degli interlocutori

Durante BB84, Alice e Bob rendono pubbliche le basi e le informazioni destinate al controllo. Per fidarsi del confronto, ciascuno deve poter stabilire che i messaggi provengano dall’altro. La segretezza della chiave e l’identità di chi la condivide sono proprietà distinte.

Un avversario che sostituisce gli interlocutori può aprire due scambi separati, uno con Alice e uno con Bob. Ciascun utente dialoga allora con l’avversario, pur credendo di dialogare con l’altro.

L’autenticazione del canale classico serve a impedire questa sostituzione. Occorre quindi un punto di fiducia iniziale: un segreto già condiviso oppure una struttura di certificati verificabili.

Due scambi con un intermediario



Autenticazione
Verifica l’origine dei messaggi classici

Richiami Un canale pubblico può essere autenticato: i messaggi restano leggibili, mentre la loro origine è verificabile.

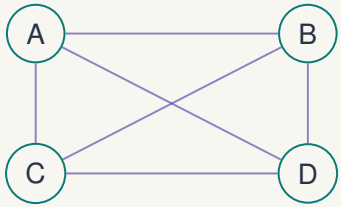
2. La fiducia iniziale e la crescita della rete

Un segreto già condiviso permette ad Alice e Bob di autenticare i messaggi di BB84. All'aumentare delle sedi cresce il numero di segreti da distribuire e custodire. Nell'esempio, quattro sedi che comunicano tutte a coppie richiedono sei relazioni di fiducia.

Un certificato collega invece un'identità a una chiave pubblica mediante la firma di un'autorità fidata. Gli utenti verificano quella firma attraverso una struttura comune. Per resistere alla minaccia quantistica, le firme dei certificati devono essere post-quantistiche.

Queste due scelte assegnano la fiducia iniziale a risorse diverse: segreti custoditi dalle coppie di utenti oppure chiavi pubbliche e autorità di certificazione.

Segreti condivisi fra coppie



Quattro sedi, sei segreti condivisi.

Certificati e autorità fidata
Firme resistenti agli attacchi quantistici

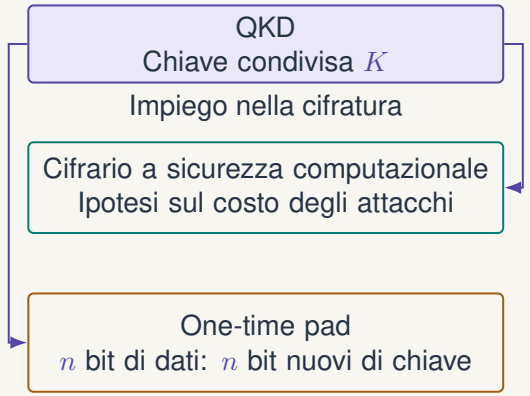
Richiami La scalabilità riguarda anche la distribuzione iniziale, la conservazione e l'aggiornamento dei segreti.

3. La chiave distribuita e i dati cifrati

La sicurezza **informazionale** riguarda anche un avversario con risorse di calcolo illimitate. Quella **computazionale** dipende dalla difficoltà dei problemi su cui si basa il cifrario. Una chiave ottenuta con QKD mantiene distinto il problema dello scambio da quello della cifratura dei dati.

Il one-time pad offre segretezza informazionale quando la chiave è uniforme, indipendente dal messaggio, segreta e usata una sola volta. Per cifrare n bit servono n nuovi bit di chiave.

Per i volumi di comunicazioni classificate considerati nella valutazione dell'11 agosto 2026, questo consumo rende impraticabile un impiego generalizzato. Il numero di bit segreti prodotti dal collegamento deve essere confrontato con il volume dei dati da proteggere.



Due impieghi alternativi della chiave, con garanzie e consumi diversi.

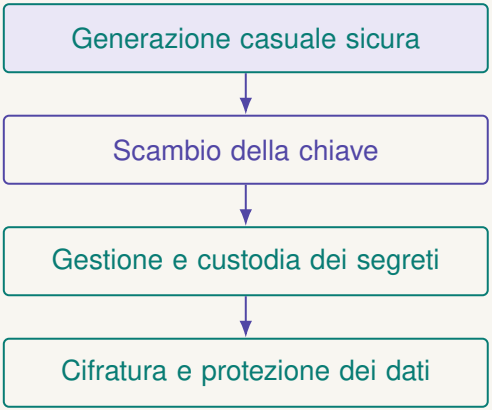
Richiami La sicurezza dello scambio della chiave e quella dell'algoritmo di cifratura devono essere valutate separatamente.

4. Generazione casuale e gestione dei segreti

Le basi e i bit di BB84 devono essere scelti con la casualità prevista dal protocollo. Se queste scelte diventano prevedibili, cambiano le condizioni da cui dipende la sicurezza dello scambio.

La chiave ottenuta deve poi raggiungere gli apparati di cifratura e rimanere segreta durante la custodia e l'uso. Chi accede alla chiave in una di queste fasi può sfruttarla anche se lo scambio sul canale quantistico è avvenuto correttamente.

Occorre quindi controllare i generatori casuali, il trasferimento interno delle chiavi e le componenti che le conservano. La protezione deve accompagnare il segreto dalla generazione al suo impiego.



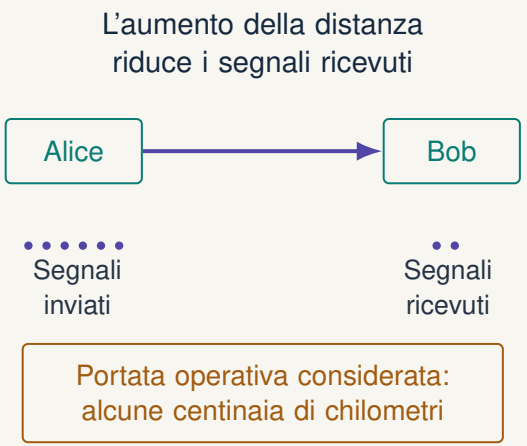
Richiami La gestione delle chiavi comprende generazione, consegna agli apparati, custodia e uso controllato.

5. Le perdite nel collegamento ottico

Durante la propagazione in fibra, una parte dei segnali viene persa. All'aumentare della distanza, Bob riceve meno eventi utili per costruire la sequenza condivisa e per svolgere i controlli. La portata del collegamento è quindi legata alle perdite del canale.

Nella valutazione tecnologica dell'11 agosto 2026, la connessione diretta dei sistemi più avanzati è collocata nell'ordine di alcune centinaia di chilometri. Questa portata condiziona la disposizione dei terminali e la progettazione della rete.

Per raggiungere sedi più lontane occorre cambiare architettura. Le possibilità includono nodi intermedi, ripetitori quantistici e collegamenti satellitari, ciascuno con proprie condizioni di fiducia e di funzionamento.



Richiami Limite tecnologico e operativo. I segnali nel diagramma rappresentano schematicamente le perdite, senza una scala quantitativa.

6. La fiducia nei nodi intermedi

Un nodo fidato T unisce due collegamenti: Alice condivide con il nodo la chiave di tratta K_{AT}, mentre il nodo condivide con Bob K_{TB}. Le due tratte permettono di raggiungere una distanza maggiore.

Il nodo gestisce segreti necessari alla comunicazione e deve essere protetto insieme ai terminali. La riservatezza fra Alice e Bob dipende quindi anche dalla sicurezza del sito intermedio.

La protezione delle singole tratte lascia al nodo un ruolo di fiducia. Per valutare l'intero percorso occorre considerare tutti i siti che gestiscono le chiavi, compresi quelli aggiunti per estendere la rete.

Una rete di tratte con nodi fidati



La fiducia comprende anche il sito intermedio.

Protezione dei terminali + protezione dei nodi attraversati

Richiami L'estensione mediante nodi fidati introduce dipendenze dai siti intermedi nella sicurezza end-to-end.

7. Ripetitori e collegamenti satellitari

Un ripetitore quantistico dovrebbe estendere la distanza mediante operazioni sugli stati quantistici, mantenendo la protezione del collegamento complessivo. Nella valutazione tecnologica dell'11 agosto 2026, questa soluzione resta teorica e la realizzazione pratica è indicata come incerta.

Il collegamento satellitare segue un'altra architettura: la trasmissione ottica passa attraverso un satellite. Il suo impiego dipende dalla disponibilità del collegamento e dalle condizioni meteorologiche.

Per progettare una comunicazione occorre quindi conoscere sia la distanza raggiungibile sia i periodi nei quali il collegamento può effettivamente funzionare.

Ripetitori quantistici
Estensione del collegamento con operazioni quantistiche

Realizzazione pratica incerta

Collegamenti satellitari
Trasmissione attraverso un collegamento ottico

Disponibilità del collegamento e condizioni meteorologiche

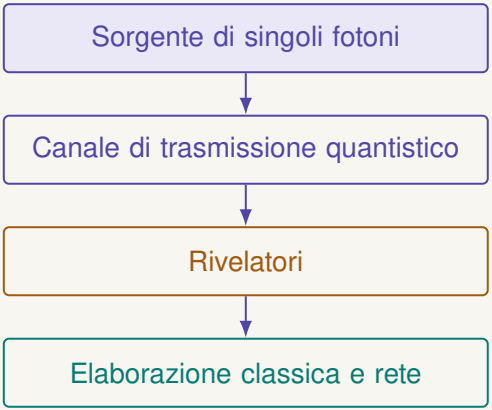
Richiami Valutazione tecnologica riferita all'11 agosto 2026: ripetitori e satelliti rientrano nei limiti attuali.

8. Apparati specializzati e integrazione

La QKD richiede sorgenti e rivelatori adatti agli stati ottici usati dal protocollo. I dispositivi vanno collegati al canale quantistico e sincronizzati con i messaggi classici di controllo.

L'installazione introduce apparati da integrare e mantenere: terminali ottici, collegamenti e sistemi di elaborazione. Il costo riguarda sia l'acquisto sia il loro inserimento nella rete esistente.

La PQC viene eseguita mediante algoritmi su hardware di calcolo ordinario. Le due opzioni comportano quindi interventi diversi sull'infrastruttura; per la QKD, gli apparati ottici costituiscono una voce specifica del progetto.



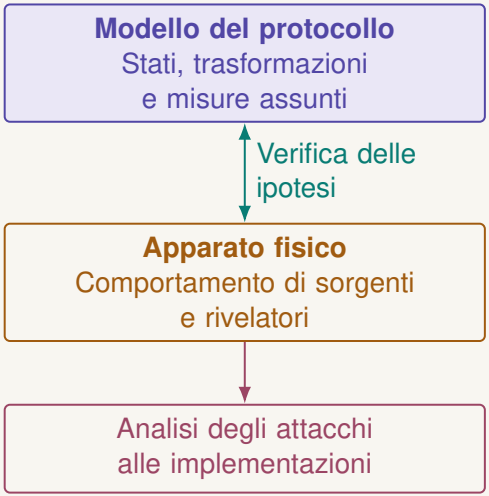
Richiami Il costo della soluzione include gli apparati specializzati e la loro integrazione nella rete.

9. La sicurezza dell’implementazione

La descrizione di BB84 assegna alle preparazioni e alle misure un comportamento preciso. Un apparato reale deve essere esaminato rispetto a queste ipotesi, perché la sua risposta fisica determina quali informazioni possono diventare accessibili a un avversario.

Gli attacchi alle implementazioni riguardano proprio i dispositivi utilizzati per eseguire il protocollo. La valutazione di sicurezza deve quindi comprendere sorgenti, rivelatori e condizioni di funzionamento, oltre alla descrizione matematica dello scambio.

Nel quadro considerato, la comprensione degli attacchi fisici ai sistemi QKD resta parziale. Questa incertezza richiede analisi specifiche prima di affidare agli apparati la protezione di informazioni classificate.



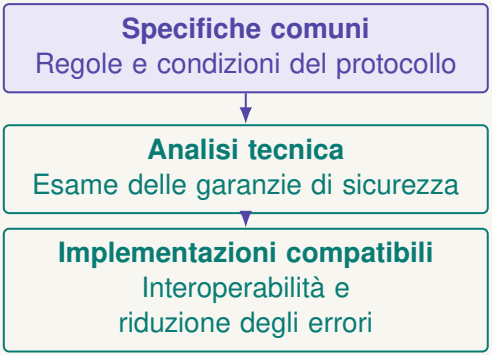
Richiami La verifica riguarda il legame fra le ipotesi del protocollo e il comportamento dell’apparato.

10. Standardizzazione e interoperabilità

Uno standard specifica quali stati preparare, quali messaggi scambiare e quali condizioni controllare. Gli esperti possono esaminare una procedura definita e confrontare le sue garanzie con le ipotesi richieste.

Le stesse specifiche permettono a dispositivi di produttori diversi di comunicare. Regole condivise riducono inoltre le divergenze fra implementazioni e il rischio di errori introdotti durante la realizzazione.

Per valutare una rete QKD occorre quindi esaminare le specifiche disponibili, la loro analisi di sicurezza e la compatibilità degli apparati che dovranno lavorare insieme.



Richiami Standardizzazione significa rendere comuni e verificabili le specifiche su cui si fondano le implementazioni.

11. La disponibilità del collegamento

Un attacco di *negazione del servizio*, o *denial of service*, impedisce agli utenti autorizzati di usare il collegamento. Nei sistemi QKD può interrompere o disturbare i segnali necessari a produrre nuove chiavi.

Quando la distribuzione si arresta, il servizio perde il rifornimento regolare di materiale segreto. Questa interruzione riguarda la disponibilità, mentre la segretezza delle chiavi già custodite costituisce una proprietà distinta.

La valutazione delle comunicazioni governative e militari deve perciò considerare anche la continuità dello scambio nelle condizioni operative previste.



Interruzione o disturbo del collegamento

Produzione regolare di nuove chiavi compromessa

La disponibilità è una proprietà del servizio.

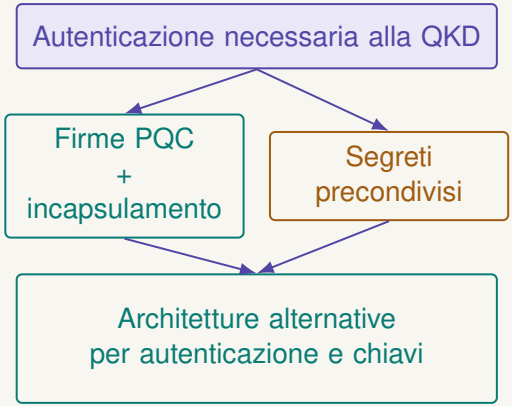
Richiami Gli attacchi di negazione del servizio colpiscono la disponibilità della soluzione di sicurezza.

12. Autenticazione e alternative alla QKD

Per autenticare la QKD servono segreti precondivisi oppure certificati con firme resistenti agli attacchi quantistici. Queste risorse devono essere predisposte prima di affidarsi allo scambio quantistico.

Una soluzione basata su PQC può affiancare alle firme un meccanismo di incapsulamento per stabilire le chiavi. Una soluzione basata sulla distribuzione preventiva può fornire direttamente segreti simmetrici agli interlocutori. Firme e formazione della chiave restano funzioni distinte.

Il confronto fra architetture deve quindi stabilire quale contributo aggiuntivo porti la QKD, tenendo conto degli apparati richiesti, dei siti fidati e della continuità del servizio.



Richiami La valutazione riguarda il contributo della QKD all'architettura completa, comprese le alternative per autenticazione e chiavi.

La scelta per le comunicazioni classificate

Le criticità si dividono in due gruppi. I limiti intrinseci riguardano le funzioni che devono accompagnare lo scambio quantistico, a partire dall'autenticazione. I limiti attuali riguardano invece la portata, la realizzazione degli apparati e le condizioni operative.

Un miglioramento tecnologico può intervenire sul secondo gruppo. Rimane comunque necessario integrare la QKD in una soluzione che garantisca riservatezza, integrità, autenticità e disponibilità.

Per la migrazione delle comunicazioni NATO, la priorità è l'adozione della PQC. L'impiego della QKD è sconsigliato nelle applicazioni governative e militari e, in particolare, per la trasmissione delle informazioni classificate considerate.

Limiti intrinseci
Autenticazione e funzioni di sicurezza aggiuntive

Limiti attuali
Portata, apparati, attacchi e disponibilità

Priorità di migrazione
Crittografia post-quantistica

Richiami Ambito della valutazione: comunicazioni governative, militari e classificate NATO; 11 agosto 2026.

CAPITOLO 03

Codifica superdensa

Due bit per qubit trasmesso
Entanglement ed entropia condizionata

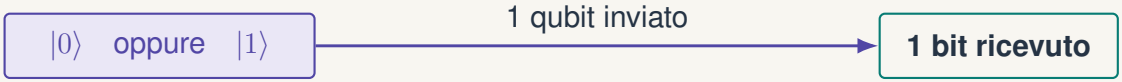
Stati di Bell, capacità e informazione condivisa

Il vantaggio: due bit per qubit trasmesso

Alice deve comunicare un messaggio di due bit: 00, 01, 10 oppure 11. Un qubit usato da solo offre al massimo due stati perfettamente distinguibili; per trasmettere uno dei quattro messaggi occorrono quindi due invii sul canale a qubit.

Con una coppia di Bell già condivisa, Alice può scegliere fra quattro stati ortogonali della coppia agendo sul proprio qubit. Le basta inviarlo a Bob, che legge i due bit mediante una misura congiunta. **Il rendimento della fase di comunicazione passa da uno a due bit per qubit inviato.**

Un qubit usato da solo



Una coppia di Bell già condivisa



Nel secondo caso Bob misura il qubit ricevuto insieme a quello già in suo possesso.

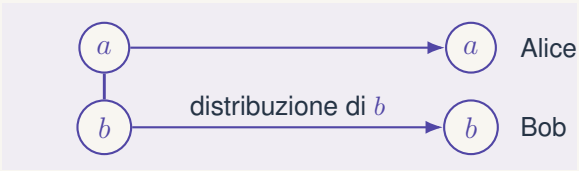
Richiami Una coppia di Bell condivisa costituisce un ebit: una risorsa di entanglement consumata da ciascuna esecuzione.

Preparare prima, comunicare dopo

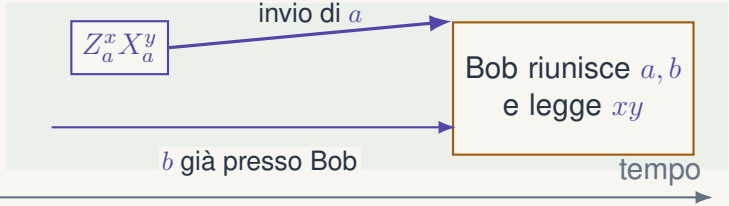
L'entanglement permette di anticipare una parte del lavoro. Alice può preparare la coppia, inviare b e conservare a quando il messaggio è ancora da scegliere. Al momento della comunicazione codifica xy su a e compie un solo nuovo invio.

Con la coppia preparata da Alice, i trasferimenti complessivi sono due: prima b, poi a. Il vantaggio è concentrare un solo invio dopo la scelta del messaggio, usando una coppia distribuita e conservata in anticipo.

Prima della scelta del messaggio



Dopo la scelta di xy



Esempio ideale. Con 1000 coppie già disponibili, 1000 invii nella fase di comunicazione trasferiscono 2000 bit. Il canale usato senza entanglement ne trasferisce 1000.

Richiami Il vantaggio è utile quando gli invii durante la comunicazione sono la risorsa limitata e le coppie si possono preparare in anticipo.

Quattro messaggi nelle correlazioni

La coppia iniziale è $|\psi_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, con a presso Alice e b presso Bob. I due bit comandano due porte locali: y decide se applicare X_a; x decide se applicare successivamente Z_a.

L'operazione $Z_a^x X_a^y$ produce lo stato $|\psi_{xy}\rangle$. Il messaggio è così associato a uno dei quattro stati ortogonali della coppia, tutti raggiungibili agendo sul solo qubit a.

Messaggio 00	**Messaggio 01**	**Messaggio 10**	**Messaggio 11**
I su a	X su a	Z su a	ZX su a
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$\|\psi_{00}\rangle$	$\|\psi_{01}\rangle$	$\|\psi_{10}\rangle$	$\|\psi_{11}\rangle$
$\dfrac{\|00\rangle + \|11\rangle}{\sqrt{2}}$	$\dfrac{\|01\rangle + \|10\rangle}{\sqrt{2}}$	$\dfrac{\|00\rangle - \|11\rangle}{\sqrt{2}}$	$\dfrac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

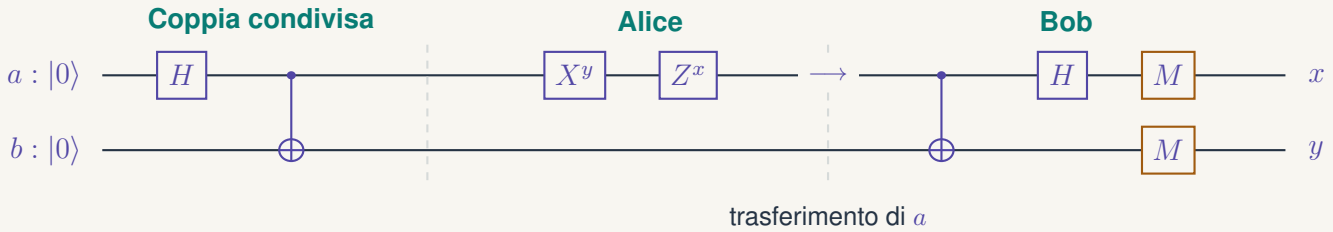
y sceglie la parità delle etichette; x sceglie il segno relativo.

Richiami $y = 0$ seleziona le etichette uguali $00, 11$; $y = 1$ quelle diverse $01, 10$. Il bit x sceglie il segno $+$ oppure $-$.

Come Bob recupera i due bit

Ricevuto a, Bob applica C_{ab}: la parità diventa il valore y del secondo qubit. Sul primo resta $H|x\rangle$, cioè $|+\rangle$ oppure $|-\rangle$. La successiva Hadamard trasforma il segno relativo nel valore leggibile x. Le due misure restituiscono xy.

$$|\psi_{xy}\rangle \xrightarrow{C_{ab}} H|x\rangle_a|y\rangle_b \xrightarrow{H_a} |x\rangle_a|y\rangle_b.$$



Per il messaggio 11**:** Alice applica X_a e poi Z_a. Bob decodifica

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \xrightarrow{C_{ab}} |-\rangle|1\rangle \xrightarrow{H_a} |11\rangle.$$

Richiami $C_{ab}|01\rangle = |01\rangle$ e $C_{ab}|10\rangle = |11\rangle$: per il messaggio 11 si ottiene $(|0\rangle - |1\rangle)|1\rangle/\sqrt{2} = |-\rangle|1\rangle$.

La matrice densità e il qubit di Bob

Uno **stato puro** è descritto da un vettore normalizzato $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. La **matrice densità** raccoglie le stesse ampiezze in una forma utile anche per descrivere parti di un sistema:

$$\rho_\phi = |\phi\rangle\langle\phi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}.$$

Gli elementi diagonali sono le probabilità nella base $0, 1$; quelli fuori diagonale conservano la coerenza fra le componenti. Per il solo qubit di Bob, una coppia di Bell dà invece

$$\rho_B = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} = I_2/2.$$

Questo è uno **stato misto**: le statistiche locali equivalgono a una miscela equiprobabile di $|0\rangle$ e $|1\rangle$. La matrice locale è uguale per tutti i messaggi xy; Bob può distinguerli quando riceve anche a e misura la coppia.

Richiami β^* è il complesso coniugato di β; I_2 è l'identità 2×2. A e B indicano i sistemi associati ai qubit a e b.

L’entropia di uno stato quantistico

Per calcolare l’**entropia di von Neumann** si usano gli autovalori λ_j della matrice densità. Sono numeri positivi o nulli, con somma uno. Nella base degli autovettori rappresentano i pesi dei diversi stati ortogonali:

$$S(\rho) = -\sum_j \lambda_j \log_2 \lambda_j, \qquad 0 \log_2 0 := 0.$$

Stato puro $|+\rangle$

$$\rho_+ = \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Autovalori: $1, 0$

$$S = -1 \log_2 1 = 0$$

Stato misto $I_2/2$

$$\rho_{\text{mista}} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

Autovalori: $1/2, 1/2$

$$S = -2(\tfrac{1}{2} \log_2 \tfrac{1}{2}) = 1$$

Entrambi gli esempi danno 0 e 1 con probabilità $1/2$ nella base computazionale. Nella base H, invece, $|+\rangle$ dà sempre 0, mentre $I_2/2$ resta equiprobabile. L’entropia descrive lo stato; la casualità degli esiti dipende anche dalla base di misura.

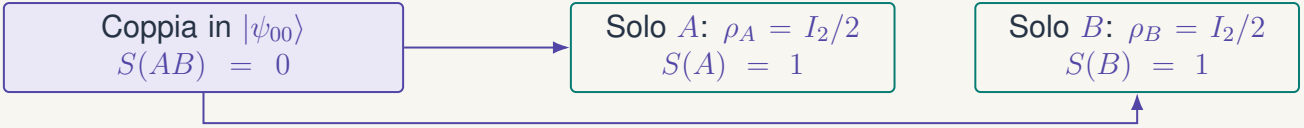
Richiami Un autovettore $|v\rangle$ soddisfa $\rho|v\rangle = \lambda|v\rangle$. I logaritmi in base 2 esprimono S in bit; uno stato puro ha autovalori $1, 0, \ldots, 0$.

La coppia è pura; ciascuna parte è mista

Per la coppia $|\psi_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, il prodotto $|\psi_{00}\rangle\langle\psi_{00}|$ dà

$$\rho_{AB} = \tfrac{1}{2}\Big(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\Big).$$

La descrizione del solo B si ottiene sommando sui due valori del sistema A: questa operazione è la **traccia parziale**. I due termini incrociati si annullano perché $\langle 0|1\rangle = 0$. Restano $\rho_B = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. Per A vale lo stesso calcolo.



La coppia ha uno stato puro, con autovalori $1, 0, 0, 0$ ed entropia zero. Ogni parte ha invece due autovalori $1/2$ ed entropia un bit. La coerenza dei termini incrociati appartiene alla descrizione congiunta.

Richiami Si scrive $\rho_B = \mathrm{Tr}_A\, \rho_{AB}$. La traccia parziale conserva le probabilità di tutte le misure sul sottosistema B.

L’entropia condizionata negativa

Per due variabili classiche, l’entropia condizionata misura l’incertezza che rimane sulla prima quando si conosce la seconda. Se i due bit sono sempre uguali, conoscere uno permette di ricostruire l’altro e l’incertezza residua è zero.

Per due sistemi quantistici si definisce invece la differenza

$$S(A|B) = S(AB) - S(B).$$

Preparazione della coppia	$S(AB)$	$S(B)$	$S(A\|B)$
00 oppure 11, scelti a caso	1	1	0
$(\|00\rangle + \|11\rangle)/\sqrt{2}$	0	1	-1

Nel secondo caso B resta una **memoria quantistica**. Misurare entrambi i qubit nella base computazionale produce due bit classici uguali e riporta al primo caso. Il valore -1 descrive la coppia prima di quella misura, con la sua coerenza ancora disponibile.

Richiami Per la coppia di Bell: $S(A) = S(B) = 1$, $S(AB) = 0$. È la differenza $S(A|B) = 0 - 1$ a essere negativa.

Il bit aggiuntivo viene dall'entanglement

La **capacità** è il numero di bit classici trasmessi per invio nel limite di molte esecuzioni. Ogni esecuzione usa una nuova coppia nello stesso stato ρ_{AB}. Se Alice codifica con porte unitarie sul proprio qubit e Bob riceve attraverso un canale ideale, vale

$$C_U = 1 + S(B) - S(AB) = 1 - S(A|B).$$

Il confronto con l'invio ordinario di un qubit, che offre un bit, dà un incremento di $-S(A|B)$. Una coppia con entropia condizionata negativa aumenta quindi la capacità della comunicazione.

Capacità ordinaria	Incremento $-S(A\|B)$
1 bit	1 bit

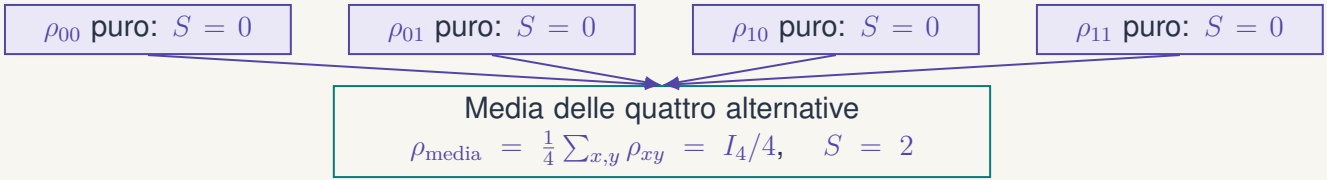
Coppia di Bell: 2 bit per qubit inviato

Per una coppia di Bell, $C_U = 1 - (-1) = 2$. Qui i quattro messaggi sono già distinguibili in una singola esecuzione: l'esempio realizza subito il valore della capacità.

Richiami Il pedice U indica il vincolo alle codifiche unitarie sulla coppia disponibile. La formula è il risultato teorico richiamato in calce.

Quattro stati puri, due bit da leggere

Per ciascun messaggio xy, la coppia ha uno stato puro $\rho_{xy} = |\psi_{xy}\rangle\langle\psi_{xy}|$. Bob considera quattro alternative equiprobabili. La loro media ha quattro autovalori $1/4$ ed entropia $\log_2 4 = 2$:



La **quantità di Holevo** limita superiormente l'informazione classica ricavabile dalla misura dell'insieme di stati:

$$\chi = S(\rho_{\text{media}}) - \frac{1}{4}\sum_{x,y} S(\rho_{xy}) = 2 - 0 = 2 \text{ bit}.$$

La misura di Bell raggiunge il limite perché distingue le quattro alternative. L'entropia 2 riguarda la media dei messaggi; ciascuno stato di Bell fissato ha invece entropia 0.

Richiami I_4 è l'identità nello spazio dei due qubit. Il bilancio resta: una coppia condivisa, un qubit trasmesso, due bit recuperati.

CAPITOLO 04

Correzione degli errori quantistici

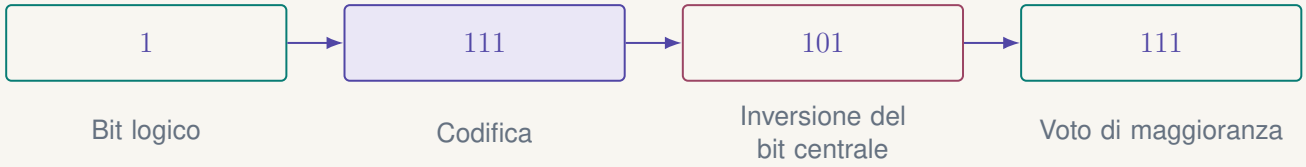
Ridondanza, sindromi e recupero
Le operazioni sui qubit logici

Mermin, cap. 5 e app. N

La ridondanza nel caso classico

Per proteggere un bit classico si può ripeterlo tre volte: $0 \mapsto 000$ e $1 \mapsto 111$. Se una sola posizione viene invertita, le altre due conservano il valore iniziale. La maggioranza identifica quindi il bit da ripristinare.

Per esempio, 101 viene ricondotto a 111. Con un qubit occorre proteggere anche le ampiezze e le fasi di una sovrapposizione: la ridondanza deve permettere di diagnosticare l'errore conservando questi coefficienti.



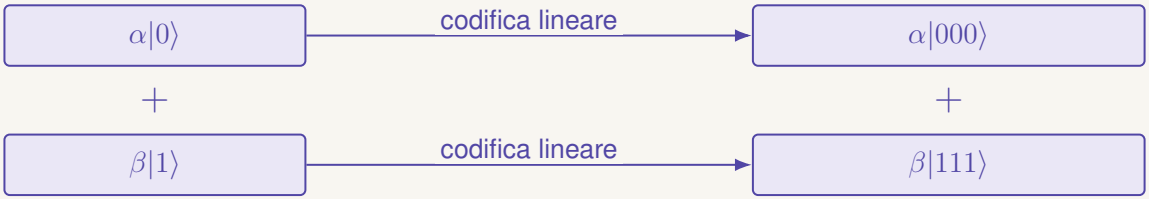
Richiami Un codice associa a ciascun valore logico una parola composta da più bit o qubit fisici.

Codificare un qubit mediante linearità

La codifica manda $|0\rangle$ in $|0_L\rangle = |000\rangle$ e $|1\rangle$ in $|1_L\rangle = |111\rangle$. Gli stati $|0_L\rangle$ e $|1_L\rangle$ rappresentano i due valori del **qubit logico**, conservato su tre qubit fisici. Per linearità,

$$\alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|000\rangle + \beta|111\rangle.$$

Le ampiezze restano α e β e accompagnano due stati del registro. Tre copie del qubit iniziale darebbero invece un prodotto con otto termini, fra cui coefficienti α^3 e $\alpha^2\beta$: si tratterebbe di un'altra trasformazione.



Gli stessi coefficienti accompagnano le due componenti.

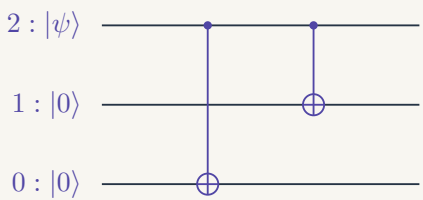
Richiami La codifica è un'operazione lineare applicata al qubit iniziale e a due ausiliari preparati in $|0\rangle$.

Il circuito di codifica a tre qubit

La codifica si realizza usando il qubit iniziale come controllo di due CNOT. Esso occupa il filo 2; i fili 1 e 0 vengono preparati in zero e fungono da bersagli:

$$C_{21}C_{20}(\alpha|0\rangle + \beta|1\rangle)|00\rangle = \alpha|000\rangle + \beta|111\rangle.$$

Il circuito manda $|000\rangle$ in $|000\rangle$ e $|100\rangle$ in $|111\rangle$. La linearità garantisce lo stesso comportamento per ogni scelta di α e β.



Le due CNOT hanno lo stesso controllo e bersagli diversi. Il loro ordine è intercambiabile.

Richiami Il filo 2 è quello più in alto; le stringhe sono scritte nell'ordine $x_2x_1x_0$.

Le tre possibili inversioni di bit

Supponiamo che fra due controlli si verifichi al massimo un'inversione. Le possibilità sono allora I, X_0, X_1, X_2. Ciascuna porta le componenti $|000\rangle$ e $|111\rangle$ in una coppia diversa di stati di base.

Le quattro coppie individuano quattro sottospazi ortogonali, ciascuno di dimensione 2. La diagnosi può stabilire in quale sottospazio si trovi lo stato, lasciando al suo interno la combinazione con coefficienti α e β.

Errore I	Errore X_0	Errore X_1	Errore X_2
$\alpha\|000\rangle + \beta\|111\rangle$	$\alpha\|001\rangle + \beta\|110\rangle$	$\alpha\|010\rangle + \beta\|101\rangle$	$\alpha\|100\rangle + \beta\|011\rangle$
Sindrome 00	Sindrome 01	Sindrome 11	Sindrome 10

Richiami Le due parità $s_{21} = x_2 \oplus x_1$ e $s_{10} = x_1 \oplus x_0$ formano la sindrome: un'etichetta che distingue i quattro casi del diagramma.

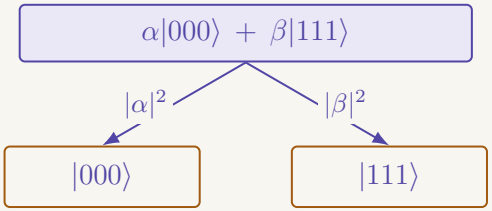
Leggere un dato e leggere una relazione

Una misura diretta di un qubit distinguerebbe $|000\rangle$ da $|111\rangle$ e selezionerebbe una sola componente. La diagnosi cerca invece le relazioni fra posizioni adiacenti, espresse dalle parità:

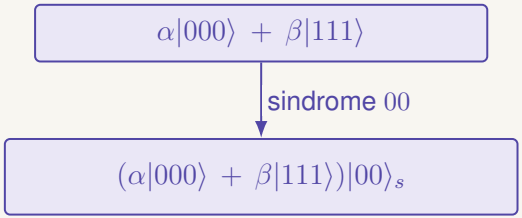
$$s_{21} = x_2 \oplus x_1, \qquad s_{10} = x_1 \oplus x_0.$$

Per un dato errore, le due componenti logiche hanno le stesse parità. La misura può quindi identificarne il sottospazio comune conservando la sovrapposizione.

Misura di un qubit dei dati



Misura delle parità



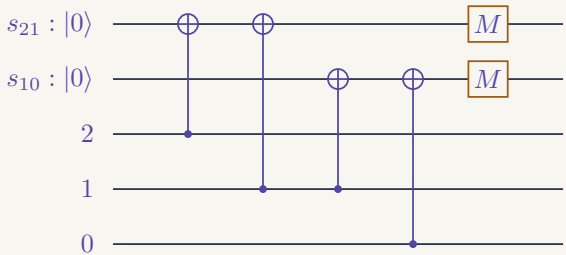
Richiami Le x_i sono le etichette di ciascun termine della sovrapposizione. La parità vale 0 per etichette uguali e 1 per etichette diverse.

Registrare le parità su due ausiliari

Per leggere le parità introduciamo due ausiliari inizialmente a zero. Due CNOT sommano sul primo i valori dei qubit 2 e 1; altre due sommano sul secondo i valori dei qubit 1 e 0.

I tre qubit dei dati fungono da controlli. Le misure vengono eseguite sugli ausiliari. La coppia di risultati costituisce la sindrome dell'errore.

$$|x_2x_1x_0\rangle|00\rangle \longmapsto |x_2x_1x_0\rangle|s_{21}s_{10}\rangle.$$



Le misure dei due fili superiori danno la sindrome. Le ampiezze restano sui tre fili dei dati.

Richiami Per ciascun termine, due CNOT sul bersaglio inizializzato a zero calcolano lo XOR. Nella formula i dati precedono gli ausiliari.

La tabella delle sindromi

Calcoliamo le due parità per ciascuno dei quattro casi. Per ogni riga, i due termini della sovrapposizione producono la stessa sindrome.

Errore	Etichette coinvolte	$s_{21}s_{10}$	Recupero
I	$000, 111$	00	I
X_0	$001, 110$	01	X_0
X_1	$010, 101$	11	X_1
X_2	$100, 011$	10	X_2

Dopo la diagnosi, applicare una seconda X al qubit individuato ripristina la parola: $X_i^2 = I$. La sindrome determina la correzione per ogni scelta di α e β.

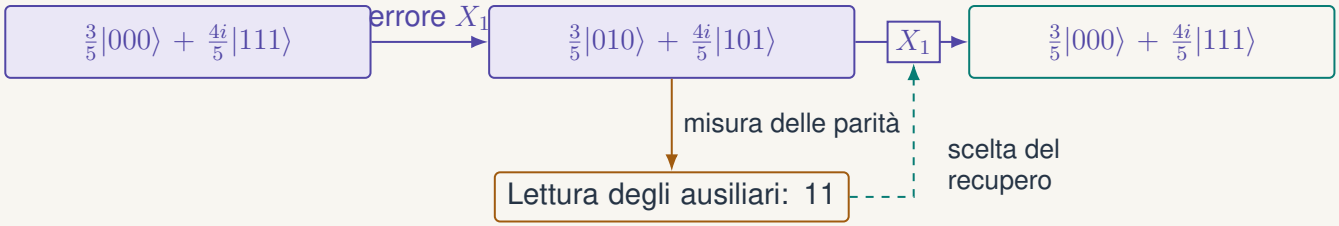
Richiami La tabella assume un errore di tipo X su al massimo un qubit della parola.

Un recupero calcolato dall'inizio alla fine

Consideriamo $|\psi_L\rangle = (3/5)|000\rangle + (4i/5)|111\rangle$ e un errore X_1 sul qubit centrale. Le etichette diventano 010 e 101; entrambe hanno sindrome 11. L'estrazione produce

$$\left(\frac{3}{5}|010\rangle + \frac{4i}{5}|101\rangle\right)|11\rangle_s.$$

La lettura degli ausiliari individua il qubit centrale. Applicando X_1 una seconda volta si recuperano le etichette iniziali e la fase relativa i, che è rimasta nei coefficienti.



Richiami $|3/5|^2 + |4i/5|^2 = 1$. Il recupero deve conservare ampiezze complesse arbitrarie.

Perché le ampiezze vengono preservate

Per un errore ammesso $E \in \{I, X_0, X_1, X_2\}$, le componenti $E|0_L\rangle$ ed $E|1_L\rangle$ producono la stessa sindrome $s(E)$. Dopo l'estrazione lo stato si fattorizza:

$$\Big(\alpha E|0_L\rangle + \beta E|1_L\rangle\Big)|s(E)\rangle.$$

La misura agisce sul secondo fattore. Poiché quel fattore è comune alle due componenti, i coefficienti α e β restano nei dati. Il recupero E^{-1} riporta le due componenti nel codice.

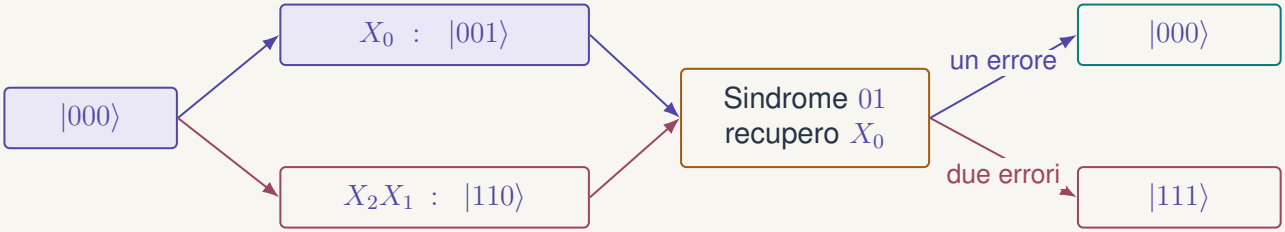
Anche per uno stato entangled $\alpha|0_L\rangle|A\rangle + \beta|1_L\rangle|B\rangle$, lo stesso fattore di sindrome accompagna entrambi i termini. I registri esterni $|A\rangle, |B\rangle$ e le loro correlazioni vengono preservati.

Richiami Il recupero conserva anche uno stato del tipo $\alpha|0_L\rangle|A\rangle + \beta|1_L\rangle|B\rangle$.

Che cosa accade con due inversioni

La stessa sindrome può corrispondere a errori diversi quando si esce dal modello previsto. Due inversioni X_2X_1 portano $|000\rangle$ in $|110\rangle$, che ha sindrome 01, uguale a quella dell'errore singolo X_0.

Il recupero applica allora X_0 e ottiene $|111\rangle$. Sullo stato generico il risultato è $\alpha|111\rangle + \beta|000\rangle$: il qubit logico è stato invertito. La frequenza dei controlli deve rendere rari questi errori multipli.



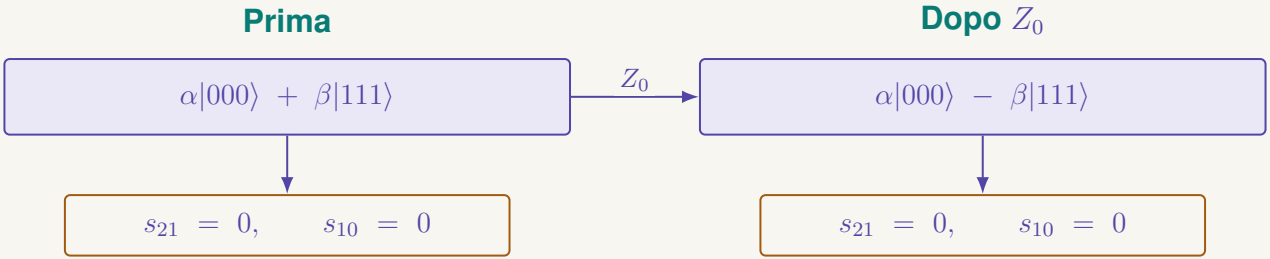
Richiami Il recupero interpreta la sindrome attraverso il modello di errore per cui il codice è stato costruito.

Un errore può cambiare la fase

Un'inversione di fase mostra un altro limite del codice di ripetizione. Applicando Z_0 si ottiene

$$Z_0|\psi_L\rangle = \alpha|000\rangle - \beta|111\rangle.$$

Le due etichette conservano le parità zero, perciò la sindrome resta 00. È però cambiata la fase relativa che determina l'interferenza. La protezione di un qubit arbitrario richiede dunque controlli capaci di riconoscere anche questo genere di alterazione.



Richiami Z modifica una fase relativa; $HXH = Z$ collega errori di bit ed errori di fase.

Un errore combinato di bit e fase

Una singola posizione può subire sia un'inversione di bit sia un cambio di fase. Indichiamo con $Y = ZX$ la loro composizione, applicando prima X e poi Z:

$$Y = ZX = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad Y|0\rangle = -|1\rangle, \qquad Y|1\rangle = |0\rangle.$$

Questa convenzione soddisfa $Y = i\sigma_y$, dove σ_y è la consueta matrice di Pauli. Il fattore i diventa una fase globale quando la porta agisce sullo stato. Per seguire esattamente il recupero conviene usare l'inversa:

$$Y^2 = -I, \qquad Y^\dagger = XZ = -Y, \qquad Y^\dagger Y = I.$$

Dopo un errore Y_i, l'operazione $X_i Z_i$ ricostruisce quindi lo stato iniziale.

Richiami $Y = ZX$ è la convenzione usata qui. Il simbolo † indica la trasposta coniugata; per una porta unitaria coincide con l'inversa.

L’interazione del qubit con l’ambiente

Il rumore può nascere dall’interazione del qubit con altri sistemi, detti **ambiente**. Gli operatori I, X, Y, Z formano una base: ogni matrice 2×2 è una loro combinazione. L’interazione si scrive quindi

$$U(|\psi\rangle|e\rangle) = |\psi\rangle|d\rangle + X|\psi\rangle|a\rangle + Y|\psi\rangle|b\rangle + Z|\psi\rangle|c\rangle.$$

I vettori ambientali incorporano i coefficienti. Un codice che associa sindromi riconoscibili ai quattro contributi, conservando le ampiezze logiche in ciascuno, può correggere la loro somma coerente. La correzione degli errori di base comprende così un errore generale su un qubit.

Identità		**Bit**		**Bit e fase**		**Fase**
$\|\psi\rangle \otimes \|d\rangle$	+	$X\|\psi\rangle \otimes \|a\rangle$	+	$Y\|\psi\rangle \otimes \|b\rangle$	+	$Z\|\psi\rangle \otimes \|c\rangle$

I quattro contributi si sommano nello stato del sistema e dell’ambiente.

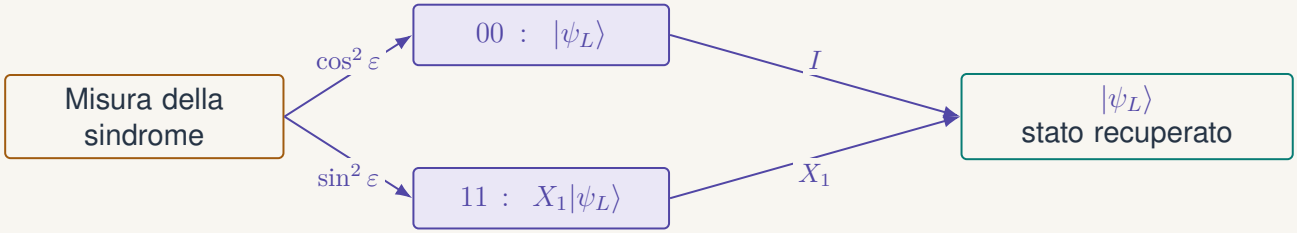
Richiami I vettori ambientali possono essere non ortogonali e non normalizzati: i loro coefficienti fanno già parte dello stato congiunto.

Un errore continuo e una sindrome discreta

Consideriamo una rotazione di parametro reale ε sul qubit centrale del codice a tre qubit. Poiché $X_1^2 = I$, si ha

$$e^{i\varepsilon X_1} = \cos\varepsilon\, I + i \sin\varepsilon\, X_1.$$

L'estrazione produce $\cos\varepsilon|\psi_L\rangle|00\rangle_s + i\sin\varepsilon X_1|\psi_L\rangle|11\rangle_s$. Le sindromi sono ortogonali, quindi hanno probabilità $\cos^2\varepsilon$ e $\sin^2\varepsilon$. Il recupero applica I oppure X_1 e restituisce in entrambi i casi lo stato logico, a meno di una fase globale.



Richiami Una misura della sindrome seleziona un sottospazio d'errore; il recupero riporta quel sottospazio nel codice.

Le parità come osservabili

Un'**osservabile** associa a una misura un operatore hermitiano. Per leggere una parità usiamo il prodotto di due porte Z, i cui autovalori sono $+1$ per etichette uguali e -1 per etichette diverse:

$$Z_i Z_j |x_i x_j\rangle = (-1)^{x_i \oplus x_j} |x_i x_j\rangle.$$

Nel codice a tre qubit, i controlli sono $S_1 = Z_2 Z_1$ e $S_2 = Z_1 Z_0$. Tutti gli stati del codice hanno autovalore $+1$ per entrambi. La lettura $+1$ si registra come bit 0; la lettura -1 come bit 1.

Se un errore E anticommuta con S, vale $SE = -ES$. Dall'identità $S|\psi_L\rangle = |\psi_L\rangle$ segue $SE|\psi_L\rangle = -E|\psi_L\rangle$: l'errore cambia il segno letto dal controllo.

Richiami Se $S|\psi_L\rangle = |\psi_L\rangle$ e $SE = -ES$, allora $SE|\psi_L\rangle = -E|\psi_L\rangle$.

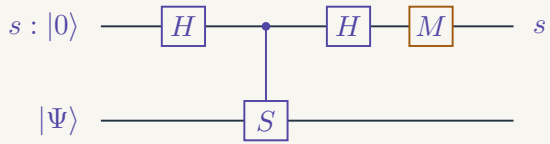
Il circuito per misurare un'osservabile

Un operatore hermitiano soddisfa $S^\dagger = S$. Se inoltre $S^2 = I$, i suoi autovalori sono $+1$ e -1. Il circuito misura questo segno mediante un qubit ausiliario.

Per un autostato dei dati, $S|\Psi\rangle = \lambda|\Psi\rangle$, la prima Hadamard prepara $|+\rangle$. La porta controllata produce

$$\frac{|0\rangle|\Psi\rangle + |1\rangle S|\Psi\rangle}{\sqrt{2}} = \frac{|0\rangle + \lambda|1\rangle}{\sqrt{2}}|\Psi\rangle.$$

L'ausiliario è quindi $|+\rangle$ per $\lambda = +1$ e $|-\rangle$ per $\lambda = -1$. La seconda Hadamard li trasforma in $|0\rangle$ e $|1\rangle$, e la misura restituisce il bit della sindrome.



$$\lambda = (-1)^s$$

Il filo inferiore può rappresentare un intero registro di dati; S agisce su quel registro.

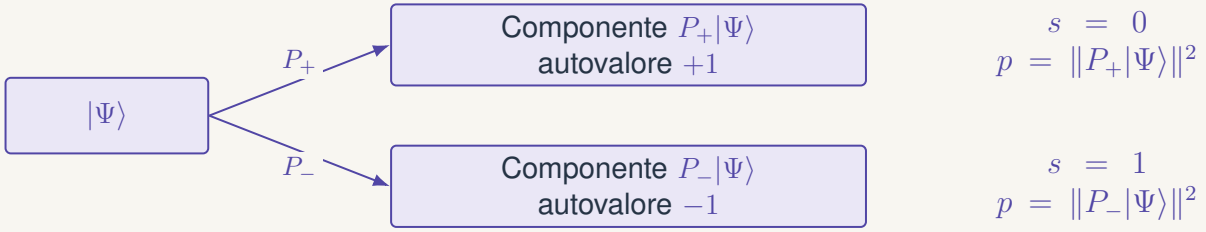
Richiami La misurazione di S è realizzata da una misura ordinaria su un qubit ausiliario.

La misura come proiezione su due sottospazi

Per uno stato qualunque $|\Psi\rangle$, definiamo $P_+ = (I + S)/2$ e $P_- = (I - S)/2$. Questi proiettori estraggono rispettivamente la componente con autovalore $+1$ e quella con autovalore -1. Il circuito della slide 73 dà

$$|0\rangle P_+|\Psi\rangle + |1\rangle P_-|\Psi\rangle.$$

La probabilità della lettura 0 è $p_+ = \|P_+|\Psi\rangle\|^2$; dopo la lettura, i dati sono nello stato $P_+|\Psi\rangle/\sqrt{p_+}$. Per la lettura 1 si usa lo stesso calcolo con P_-. La divisione ripristina la norma unitaria del ramo selezionato.



Richiami La formula del ramo selezionato si usa quando la sua probabilità è positiva. $P_+ + P_- = I$, $P_+P_- = 0$ e $P_\pm^2 = P_\pm$.

Più controlli compatibili

Per distinguere più errori si misurano r controlli $S_1, \ldots, S_r$ hermitiani, con $S_j^2 = I$. Essi commutano a coppie: $S_i S_j = S_j S_i$. Ogni sottospazio può così avere un autovalore definito per tutti i controlli.

La sindrome è la sequenza $s = (s_1, \ldots, s_r)$. Il proiettore sul sottospazio individuato dalla lettura è

$$P_s = \prod_{j=1}^{r} \frac{I + (-1)^{s_j} S_j}{2}.$$

Gli stati del codice hanno sempre autovalore $+1$, cioè sindrome nulla. Per questo i controlli sono detti **stabilizzatori**. Un errore di base lascia $s_j = 0$ se commuta con S_j e produce $s_j = 1$ se anticommuta. Quando i casi ammessi hanno sindromi distinguibili, la lettura individua il recupero.

Richiami La commutazione rende compatibili le misure dei diversi controlli.

Quante dimensioni occorrono

Per proteggere un qubit logico servono due dimensioni. Se vogliamo distinguere lo stato corretto e i $3n$ errori singoli X_i, Y_i, Z_i mediante sottospazi ortogonali, lo spazio fisico deve soddisfare

$$2(1 + 3n) \leq 2^n.$$

Quattro qubit offrono 16 dimensioni contro le 26 richieste. Con cinque qubit le quantità coincidono: $2(1 + 15) = 32$. Cinque è il primo numero compatibile con questo conteggio. La costruzione dei controlli nelle slide successive mostra che un codice con queste dimensioni esiste.



Richiami Il conteggio assume sottospazi distinti e ortogonali per gli errori singoli: è il caso del codice a cinque qubit.

I quattro controlli del codice a cinque qubit

Il codice a cinque qubit usa quattro controlli. Ogni riga del diagramma rappresenta un prodotto di operatori locali; ogni colonna corrisponde a un qubit fisico. Gli stati logici soddisfano

$$M_j|\psi_L\rangle = |\psi_L\rangle, \qquad j = 0, 1, 2, 3.$$

Le misure producono quattro bit nell'ordine M_0, M_1, M_2, M_3. Le sedici combinazioni distinguono il sottospazio del codice e i quindici sottospazi associati agli errori singoli.

	Qubit 0	Qubit 1	Qubit 2	Qubit 3	Qubit 4
M_0	I	Z	X	X	Z
M_1	Z	I	Z	X	X
M_2	X	Z	I	Z	X
M_3	X	X	Z	I	Z

Richiami La griglia elenca i qubit per indice crescente; le stringhe restano ordinate $x_4 \cdots x_0$. Un segno $+1$ dà il bit 0, un segno -1 dà il bit 1.

Perché i controlli commutano

Due controlli possono contenere operatori locali che anticommutano e tuttavia commutare nel loro insieme. Nel prodotto $M_0 M_1$ le anticommutazioni sono due, sui qubit 2 e 4: i segni si compensano. Lo stesso accade per ogni coppia.

Il quinto operatore della sequenza ciclica, $M_4 = Z_0 X_1 X_2 Z_3$, è già determinato dai primi quattro:

$$M_0 M_1 M_2 M_3 M_4 = I, \qquad M_4 = M_0 M_1 M_2 M_3.$$

	Qubit 0	Qubit 1	Qubit 2	Qubit 3	Qubit 4
M_0	I	Z	X	X	Z
M_1	Z	I	Z	X	X
	$+1$	$+1$	-1	$+1$	-1

Due anticommutazioni locali: $(-1) \cdot (-1) = +1$

Richiami Operatori su qubit diversi commutano. Sullo stesso qubit vale $XZ = -ZX$.

Le due parole logiche del codice

Possiamo definire le parole logiche applicando a $|00000\rangle$ e $|11111\rangle$ i fattori che selezionano l'autovalore positivo dei controlli.

$$|0_L\rangle = \frac{1}{4}(I + M_0)(I + M_1)(I + M_2)(I + M_3)|00000\rangle,$$
$$|1_L\rangle = \frac{1}{4}(I + M_0)(I + M_1)(I + M_2)(I + M_3)|11111\rangle.$$

Lo sviluppo produce 16 etichette distinte, ciascuna con coefficiente $+1$ oppure -1. La norma al quadrato è quindi 16; moltiplicando per $1/4$ si ottiene norma uno. Ogni M_j inverte due qubit, quindi $|0_L\rangle$ contiene etichette con un numero pari di 1 e $|1_L\rangle$ etichette con un numero dispari di 1.

Le due parole sono ortogonali. Una loro combinazione $\alpha|0_L\rangle + \beta|1_L\rangle$ è conservata da tutti i quattro controlli.

Richiami $M_j(I + M_j) = I + M_j$: ogni fattore seleziona l'autovalore $+1$.

Sedici sindromi per sedici casi

Confrontando ogni errore con i quattro controlli otteniamo la tabella delle sindromi. Il bit 0 indica commutazione, il bit 1 anticommutazione. Tutte le righe sono diverse: la lettura identifica un unico errore ammesso.

Errore	$s_0 s_1 s_2 s_3$	Errore	$s_0 s_1 s_2 s_3$
I	0000	Y_2	1101
X_0	0100	Z_2	1000
Y_0	0111	X_3	0010
Z_0	0011	Y_3	1110
X_1	1010	Z_3	1100
Y_1	1011	X_4	1001
Z_1	0001	Y_4	1111
X_2	0101	Z_4	0110

A ogni sindrome corrisponde un recupero: I, X_i, Z_i oppure $Y_i^\dagger$.

Richiami La sindrome è ordinata come M_0, M_1, M_2, M_3; questa convenzione va mantenuta nel recupero.

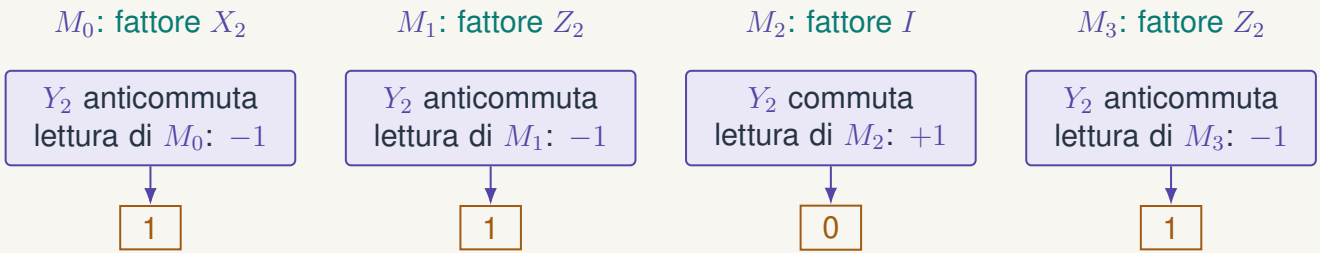
Esempio: un errore combinato sul qubit 2

L'errore $Y_2 = Z_2X_2$ anticommuta con M_0, M_1, M_3 e commuta con M_2. La sindrome è quindi 1101.

Il recupero applica $Y_2^\dagger = X_2Z_2$:

$$(X_2Z_2)(Z_2X_2)|\psi_L\rangle = |\psi_L\rangle.$$

La stessa correzione vale per ogni scelta delle ampiezze logiche.



Richiami Con $Y = ZX$, il recupero è $Y^{-1} = Y^\dagger = XZ$: nel circuito si applica prima Z e poi X.

Preparare una parola logica a cinque qubit

I quattro controlli $M_0, \ldots, M_3$ selezionano il sottospazio della sindrome. L'osservabile logica $\overline{Z} = Z_0 Z_1 Z_2 Z_3 Z_4$ distingue poi le parole del codice: $\overline{Z}|0_L\rangle = |0_L\rangle$ e $\overline{Z}|1_L\rangle = -|1_L\rangle$.

Per inizializzare il registro in $|0_L\rangle$, misuriamo i controlli, applichiamo il recupero della tabella e misuriamo $\overline{Z}$. Se l'esito è $+1$ abbiamo $|0_L\rangle$; se è -1, applichiamo

$$\overline{X} = X_0 X_1 X_2 X_3 X_4, \qquad \overline{X}|1_L\rangle = |0_L\rangle.$$

La procedura prepara uno stato logico fissato. Per codificare un ingresso $\alpha|0\rangle + \beta|1\rangle$ occorre invece un circuito unitario che trasferisca entrambe le ampiezze nella parola logica.

Richiami Preparare una parola logica fissata e codificare un qubit arbitrario sono operazioni distinte: la seconda deve preservare le ampiezze dell'ingresso.

I sei controlli del codice di Steane

Nel codice di Steane, un qubit logico occupa sette qubit fisici. Usiamo nuovi controlli M_0, M_1, M_2 composti da X e N_0, N_1, N_2 composti da Z. Ogni riga della griglia è un operatore; per esempio, $M_0 = X_0X_4X_5X_6$ e $N_0 = Z_0Z_4Z_5Z_6$.

Le posizioni comuni a un controllo M_i e a un controllo N_j sono due oppure quattro. Le anticommutazioni locali producono quindi un segno complessivo positivo: tutti i controlli commutano. Gli stati del codice hanno autovalore $+1$ per tutte le sei righe.

	q_0	q_1	q_2	q_3	q_4	q_5	q_6
M_0	X	I	I	I	X	X	X
M_1	I	X	I	X	I	X	X
M_2	I	I	X	X	X	I	X
N_0	Z	I	I	I	Z	Z	Z
N_1	I	Z	I	Z	I	Z	Z
N_2	I	I	Z	Z	Z	I	Z

Richiami Nelle righe M si moltiplicano le X indicate; nelle righe N si moltiplicano le Z. I lascia invariato il qubit della colonna.

Costruire gli stati logici di Steane

Ogni fattore $I + M_j$ aggiunge allo stato il risultato di applicare M_j. I tre fattori producono $2^3 = 8$ combinazioni: applicandole a $|0000000\rangle$ si ottengono otto etichette distinte con la stessa ampiezza.

$$|0_L\rangle = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|0000000\rangle.$$

La parola logica uno è ottenuta invertendo tutti i sette qubit:

$$|1_L\rangle = \overline{X}|0_L\rangle, \qquad \overline{X} = X_0X_1X_2X_3X_4X_5X_6.$$

Le otto etichette di $|0_L\rangle$ hanno peso pari, dove il peso è il numero di bit uguali a 1. Le loro complementari hanno peso dispari e formano $|1_L\rangle$. Le due parole sono quindi ortogonali.

Richiami Le otto componenti di ciascuna parola logica hanno ampiezza $1/\sqrt{8}$.

Le componenti delle due parole logiche

Sviluppiamo il prodotto precedente. Le stringhe sono scritte nell'ordine $x_6x_5\cdots x_0$. Ogni riga compare con ampiezza $1/\sqrt{8}$ nella parola corrispondente.

In $\lvert 0_L\rangle$	Peso	In $\lvert 1_L\rangle$	Peso
0000000	0	1111111	7
0011011	4	1100100	3
0101101	4	1010010	3
0110110	4	1001001	3
1000111	4	0111000	3
1011100	4	0100011	3
1101010	4	0010101	3
1110001	4	0001110	3

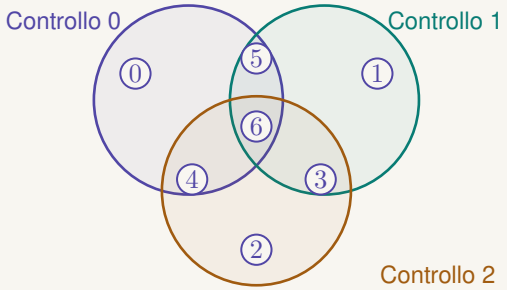
Ogni parola ha norma 1: otto probabilità uguali a $1/8$ sommano a 1.

Richiami Il complemento di una stringa si ottiene applicando X a tutte le sue posizioni.

La posizione dell’errore in tre bit

Nel codice di Steane, ogni posizione compare in una combinazione diversa dei tre controlli. La colonna h_j registra queste appartenenze: il bit i vale 1 se il qubit j compare nel controllo i.

Un errore X_j lascia la firma h_j nei controlli N_i, mentre un errore Z_j la lascia nei controlli M_i. Le sette colonne distinte permettono di localizzare l’errore. Per esempio, il qubit 5 appartiene ai controlli 0 e 1, dunque $h_5 = 110$.



$$
\begin{array}{ll}
j = 0 & h_j = 100 \\
j = 1 & h_j = 010 \\
j = 2 & h_j = 001 \\
j = 3 & h_j = 011 \\
j = 4 & h_j = 101 \\
j = 5 & h_j = 110 \\
j = 6 & h_j = 111
\end{array}
$$

Qubit 5
controlli 0 e 1
$h_5 = 110$

Richiami La firma h_j registra le appartenenze ai controlli nell’ordine 0, 1, 2; j è l’etichetta del qubit, mentre h_j è la sua sindrome.

Distinguere errori di bit, fase e combinati

I sei risultati vengono divisi in due gruppi, s_M e s_N. I controlli di tipo Z, cioè gli N_i, rivelano le inversioni di bit; quelli di tipo X, cioè gli M_i, rivelano i cambi di fase.

La firma h_j stabilisce la posizione. Quando compare in entrambi i gruppi, sulla stessa posizione sono presenti entrambi gli effetti: l'errore è $Y_j = Z_j X_j$ e si recupera con $X_j Z_j$. La coppia $000, 000$ corrisponde allo stato corretto nel modello di errore singolo.

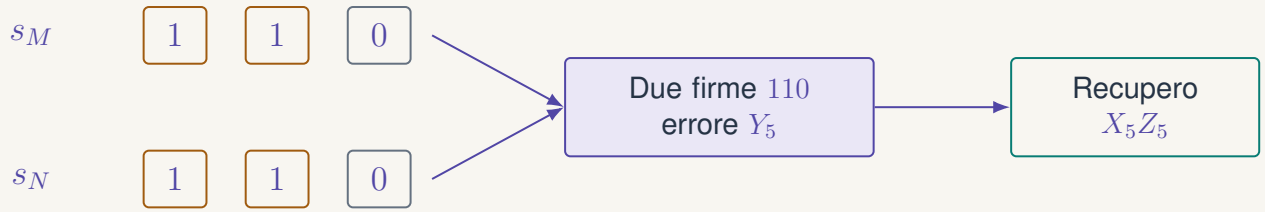
	$s_N = 000$	$s_N = h_j$
$s_M = 000$	I Recupero: I	X_j Recupero: X_j
$s_M = h_j$	Z_j Recupero: Z_j	$Y_j = Z_j X_j$ Recupero: $X_j Z_j$

Richiami La tabella copre $1 + 3 \cdot 7 = 22$ casi: lo stato corretto e tutti gli errori singoli di base.

Esempio: la firma 110 nel codice di Steane

Supponiamo di leggere $s_M = 110$ e $s_N = 110$. Entrambi i gruppi indicano un'alterazione; la firma comune individua il qubit 5. Si tratta quindi di un errore combinato Y_5.

Il recupero è $X_5 Z_5$, che annulla $Z_5 X_5$. Con $s_M = 000$ e $s_N = 110$, invece, sarebbe presente soltanto l'inversione di bit e basterebbe X_5. La lettura separa così il tipo dell'errore dalla sua posizione.



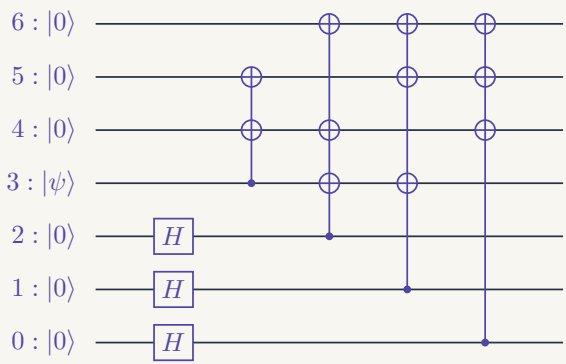
Richiami Per il qubit 5, i controlli con indice 0 e 1 contengono l'operatore locale; quelli con indice 2 lo omettono.

Il circuito di codifica a sette qubit

Il qubit da codificare occupa il filo 3; gli altri sei partono da zero. Le Hadamard sui fili 0, 1 e 2 preparano i controlli delle tre combinazioni $I + M_j$.

Il filo 3 controlla prima due inversioni sui fili 4 e 5. Seguono tre gruppi di CNOT con controlli 2, 1 e 0.

Le operazioni distribuiscono le due componenti dell'ingresso nelle corrispondenti parole logiche. Da $\alpha|0\rangle + \beta|1\rangle$ sul filo 3 si ottiene così $\alpha|0_L\rangle + \beta|1_L\rangle$ sull'intero blocco.



Un controllo collegato a più bersagli rappresenta più CNOT con lo stesso controllo.

Richiami I fili sono ordinati dall'alto verso il basso come $6, 5, 4, 3, 2, 1, 0$.

Perché il circuito prepara entrambe le parole

Con ingresso $|0\rangle$ sul filo 3, il gruppo controllato dal filo 2 crea due rami: il registro resta azzerato oppure vengono invertiti i qubit $2, 3, 4, 6$. Sullo stato iniziale la somma è quindi $(I + M_2)|0000000\rangle/\sqrt{2}$.

I gruppi con controllo 1 e 0 aggiungono allo stesso modo i fattori $(I + M_1)/\sqrt{2}$ e $(I + M_0)/\sqrt{2}$. Si ottiene la parola $|0_L\rangle$ della slide 84.

Con ingresso $|1\rangle$, le prime CNOT portano a 1 anche i fili 4 e 5. L'uscita differisce per $X_3X_4X_5$. Poiché

$$X_3X_4X_5 = \overline{X}M_0M_1M_2,$$

e gli stabilizzatori lasciano $|0_L\rangle$ invariato, l'uscita è $\overline{X}|0_L\rangle = |1_L\rangle$. La linearità estende il risultato a ogni ingresso.

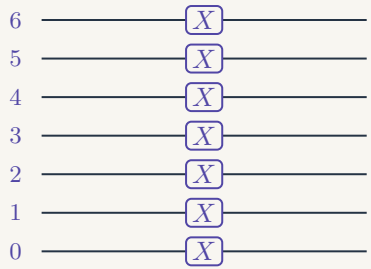
Richiami Per verificare una codifica lineare di un qubit basta verificarne l'azione su $|0\rangle$ e $|1\rangle$.

Le porte logiche X e Z

Nel codice di Steane le porte logiche $\overline{X}$ e $\overline{Z}$ si realizzano applicando la stessa porta ai sette qubit:

$$\overline{X} = X^{\otimes 7}, \qquad \overline{Z} = Z^{\otimes 7}.$$

$\overline{X}$ scambia $|0_L\rangle$ e $|1_L\rangle$. $\overline{Z}$ conserva $|0_L\rangle$ e cambia il segno di $|1_L\rangle$, perché le loro etichette hanno rispettivamente peso pari e dispari.



$$\overline{X}$$
$$|0_L\rangle \leftrightarrow |1_L\rangle$$



$$\overline{Z}$$
$$|0_L\rangle \mapsto |0_L\rangle$$
$$|1_L\rangle \mapsto -|1_L\rangle$$

Richiami Una porta logica conserva lo spazio del codice e modifica lo stato all'interno di quello spazio.

Hadamard su tutti i sette qubit

Le sette Hadamard scambiano i controlli M_i e N_i e conservano lo spazio del codice. Sugli stati logici agiscono come una Hadamard:

$$H^{\otimes 7}|0_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}}, \qquad H^{\otimes 7}|1_L\rangle = \frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}}.$$

Il blocco codificato conserva quindi la stessa trasformazione delle ampiezze di un singolo qubit: $(\alpha, \beta) \mapsto (\alpha + \beta, \alpha - \beta)/\sqrt{2}$.



sul codice

$$\overline{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Base logica: $|0_L\rangle, |1_L\rangle$

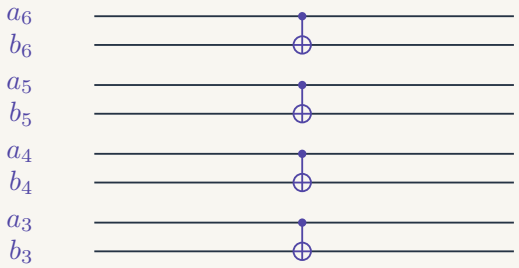
Richiami $HXH = Z$ e $HZH = X$: applicare H a ogni qubit scambia i controlli M_i e N_i e realizza la Hadamard nella base $|0_L\rangle, |1_L\rangle$.

La CNOT fra due parole logiche

Per operare su due qubit logici, colleghiamo i rispettivi blocchi con sette CNOT fra posizioni corrispondenti. Il blocco a controlla il blocco b:

$$\overline{C} = \prod_{j=0}^{6} C_{a_j b_j}, \qquad \overline{C}|x_L\rangle|y_L\rangle = |x_L\rangle|(x \oplus y)_L\rangle.$$

Le componenti di $|0_L\rangle$ producono sul bersaglio stabilizzatori, che lo lasciano invariato. Quelle di $|1_L\rangle$ aggiungono la porta logica $\overline{X}$. La linearità conserva la stessa regola sulle sovrapposizioni.





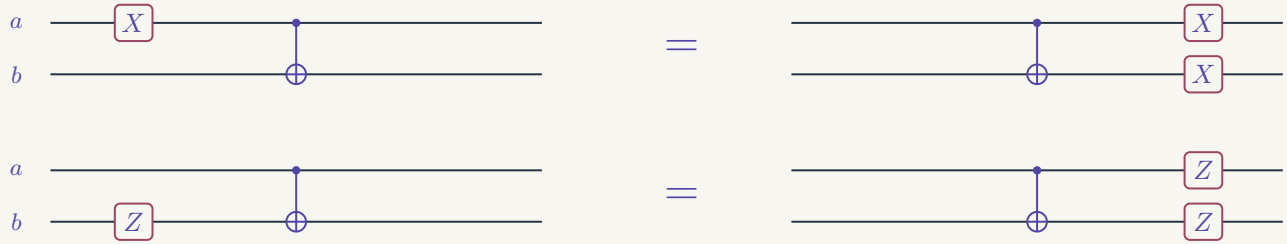
Sette CNOT su coppie disgiunte.
Ogni coppia comprende due fili distinti.

Richiami Le sette CNOT agiscono su coppie fisiche disgiunte: questa realizzazione è detta trasversale.

La propagazione degli errori attraverso CNOT

Le porte a due qubit possono propagare gli errori. Attraversando una CNOT, un errore X sul controllo raggiunge anche il bersaglio; un errore Z sul bersaglio raggiunge anche il controllo. Le altre due combinazioni, X_b e Z_a, commutano con la porta.

Nella CNOT trasversale ogni coppia fisica appartiene a due blocchi diversi. Un singolo guasto coinvolge quindi al massimo un qubit per blocco, e ciascun blocco conserva la possibilità di correggere il proprio errore.



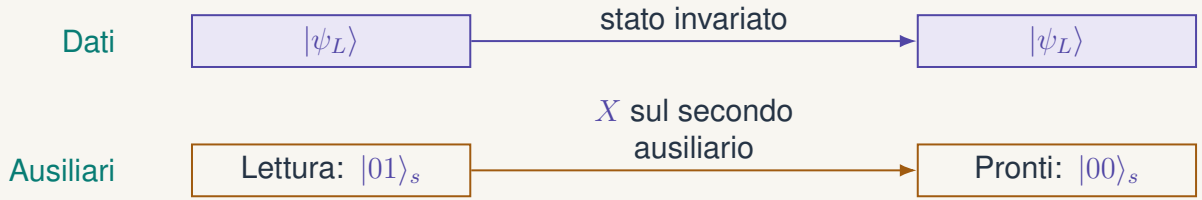
Richiami Le identità sono coniugazioni: descrivono come un errore cambia attraversando una porta.

Gli ausiliari: sindrome e successivo ripristino

La sindrome può essere misurata e usata per scegliere il recupero, oppure controllare direttamente le porte che correggono i dati. Dopo il recupero lo stato logico è separato dagli ausiliari: per un errore di base E si ha $|\psi_L\rangle|s(E)\rangle$.

Per riutilizzare gli ausiliari occorre prepararli nuovamente in zero. Si leggono i loro valori e si applica X a ciascuna posizione risultata 1. Nel codice a tre qubit, per esempio, la sindrome 01 richiede X soltanto sul secondo ausiliario.

I dati conservano $|\psi_L\rangle$ durante questo ripristino. Il registro ausiliario azzerato è pronto a registrare la sindrome del ciclo seguente.



Richiami Gli ausiliari registrano l'errore. Dopo il recupero sono separati dalle ampiezze del qubit logico e possono essere misurati e ripreparati.

Il codice di Shor: tre blocchi da tre qubit

Il codice di Shor combina tre blocchi di tre qubit. Ciascun blocco usa le due sovrapposizioni con segno opposto:

$$|G_{\pm}\rangle = \frac{|000\rangle \pm |111\rangle}{\sqrt{2}}, \qquad |0_L\rangle = |G_+\rangle^{\otimes 3}, \quad |1_L\rangle = |G_-\rangle^{\otimes 3}.$$

Le parità interne a ogni blocco individuano le inversioni di bit. Una Z su un qubit del blocco scambia invece $|G_+\rangle$ e $|G_-\rangle$: i controlli fra blocchi rilevano questo cambio di segno. La combinazione dei due livelli permette di correggere un errore arbitrario su un qubit.

$$|0_L\rangle = \boxed{|G_+\rangle \text{ tre qubit}} \otimes \boxed{|G_+\rangle \text{ tre qubit}} \otimes \boxed{|G_+\rangle \text{ tre qubit}}$$

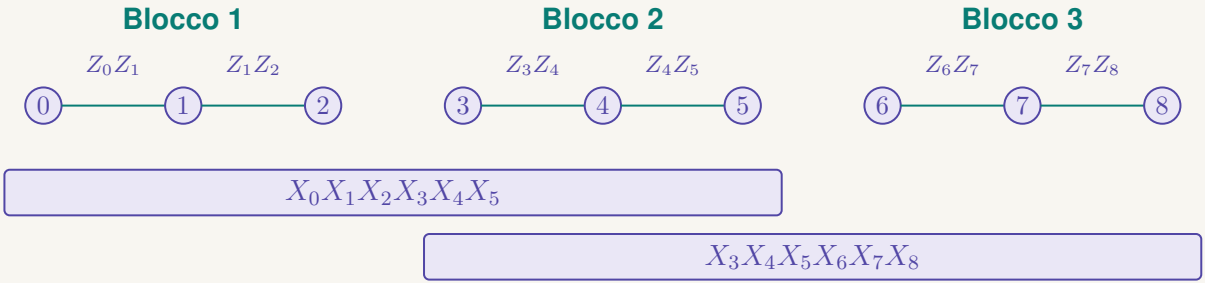
$$|1_L\rangle = \boxed{|G_-\rangle \text{ tre qubit}} \otimes \boxed{|G_-\rangle \text{ tre qubit}} \otimes \boxed{|G_-\rangle \text{ tre qubit}}$$

Richiami Le due parole di Shor sono ortogonali e normalizzate; ciascuna contiene otto etichette di base.

Otto controlli e un esempio di degenerazione

Sei controlli ZZ confrontano qubit dello stesso blocco; due controlli $X^{\otimes 6}$ confrontano blocchi adiacenti. Tutti hanno autovalore $+1$ sul codice.

Nel blocco $0, 1, 2$ vale $Z_0|\psi_L\rangle = Z_1|\psi_L\rangle = Z_2|\psi_L\rangle$. La correzione può agire su qualunque qubit del blocco individuato. Questa equivalenza fra errori fisici è la degenerazione del codice.



Richiami I casi indipendenti sono $1 + 9 + 9 + 3 = 22$: identità, nove X, nove Y e un errore Z per ciascuno dei tre blocchi.

Confrontare i codici studiati

Qubit fisici	Controlli	Errori corretti	Caratteristica
3	2	Un errore X	Parità fra coppie
5	4	Un errore arbitrario	16 sindromi distinte
7	6	Un errore arbitrario	Porte logiche trasversali
9	8	Un errore arbitrario	Tre blocchi e degenerazione

Tutti i codici della tabella proteggono un qubit logico. Il numero di qubit fisici riguarda la parola codificata; gli ausiliari necessari alla misura della sindrome sono risorse aggiuntive.

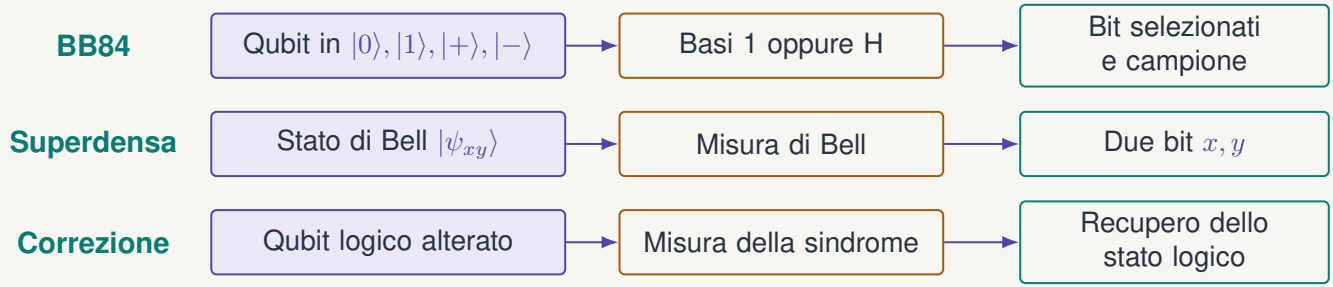
La scelta di un codice dipende dal rumore che si intende correggere e dalle operazioni da eseguire sui dati codificati. Il codice a sette qubit consente la realizzazione trasversale di X, Z, H e CNOT.

Richiami Un ciclo comprende estrazione della sindrome, misura, recupero e preparazione degli ausiliari per il ciclo seguente.

Misurare, comunicare e proteggere

In BB84, la scelta casuale delle basi costruisce correlazioni fra bit e rende osservabile il disturbo nel campione. L'uso di quelle chiavi richiede poi autenticazione, gestione dei segreti, cifratura e un collegamento disponibile.

Nella codifica superdensa, una coppia condivisa porta il rendimento a due bit per qubit inviato; l'incremento corrisponde a $-S(A|B) = 1$. Nella correzione degli errori, la misura della sindrome distingue invece sottospazi che conservano al loro interno le ampiezze del qubit logico.



Richiami Ogni procedura sceglie quali differenze rendere osservabili: il disaccordo fra bit, lo stato di Bell o il sottospazio d'errore.

Riferimenti

N. David Mermin, *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007. Cap. 1: stati, porte e misure. §§6.1–6.2: stati di Bell e BB84. §6.4: codifica superdensa. Cap. 5 e app. N: correzione degli errori.

NATO, Digital Policy Committee, *Position Paper on Quantum Key Distribution*. AC/322-D(2026)0037, 11 agosto 2026, Allegato 1. §§1–3: minaccia e strumenti crittografici; §§4–7: requisiti, limiti e valutazione dell'impiego.

N. J. Cerf e C. Adami, *Negative Entropy and Information in Quantum Mechanics*. Physical Review Letters **79**, 5194–5197 (1997). Entropia condizionata e confronto fra correlazioni classiche e quantistiche.
doi:10.1103/PhysRevLett.79.5194.

G. Bowen, *Classical Information Capacity of Superdense Coding*. Physical Review A **63**, 022302 (2001). Capacità della codifica superdensa e bilancio entropico.
doi:10.1103/PhysRevA.63.022302.

Richiami Le valutazioni di impiego della QKD sono riferite al documento dell'11 agosto 2026; le formule entropiche alle fonti aggiuntive indicate sopra.