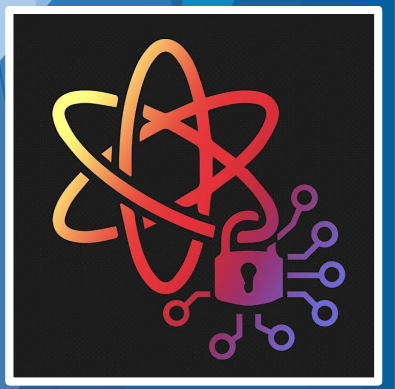
INFN CNAF Istituto Nazionale di Fisica Nucleare
Centro Nazionale per la Ricerca e lo Sviluppo nelle Tecnologie Informatiche e Telematiche

Quantum Cryptography

Introduzione alla Crittografia Quantistica

Algoritmo BB84 di QKD (Quantum-Key-Distribution)



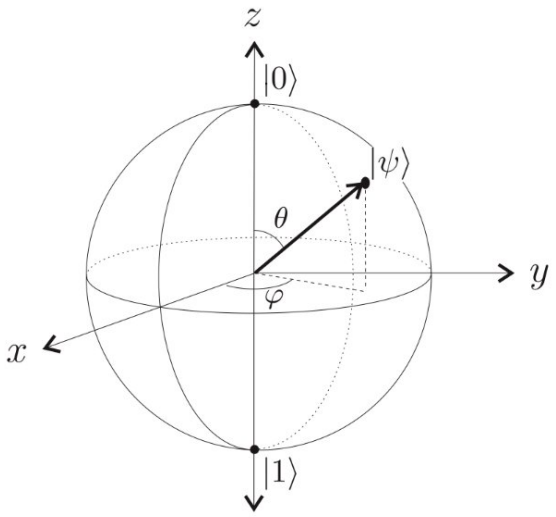
Francesco Amori

Sommario

- Quantum Computing
  - Sovrapposizione ed Entanglement
  - Misurazione
  - Circuito Quantistico
- Quantum-Key-Distribution
  - Protocollo BB84
  - Algoritmo
  - Simulazione in Python
  - Sicurezza dei dati
  - Accenni relativi a Ekert-91
- Conclusioni

Quantum Computing

- I computer quantistici sono delle nuove tipologie di dispositivi che non consentono di rappresentare e manipolare l'informazione attraverso i classici bit: "0" e "1"
- Utilizzano i quantum bit o qubit, oggetti più complessi che sfruttano proprietà della fisica quantistica: la sovrapposizione di stati e l'entanglement



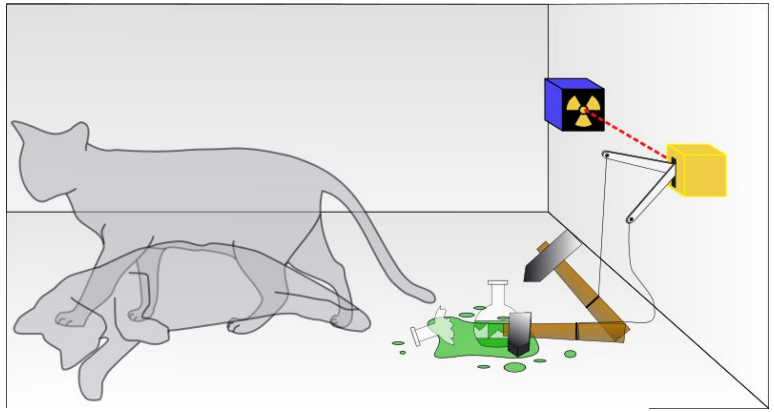
Un qubit è definito come:

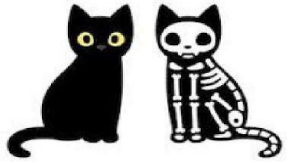
$$|\psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$$

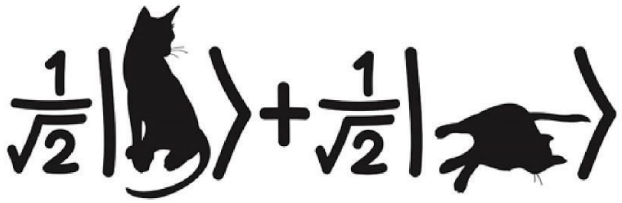
I possibili stati di un qubit sono tutti i punti della superficie della sfera

Sovrapposizione degli stati

Il gatto di Schrödinger







Entanglement Quantistico

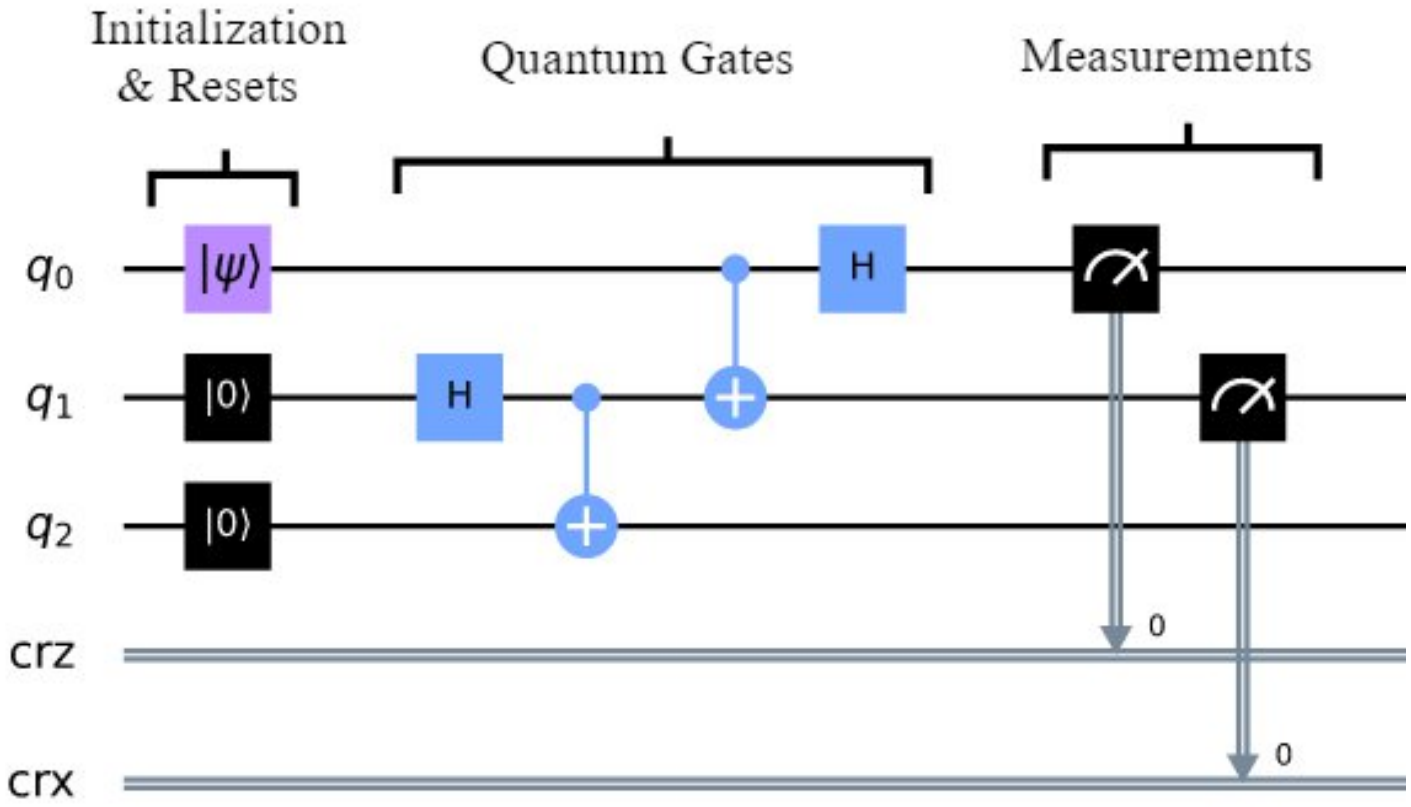
- L'entanglement quantistico è un fenomeno per cui, in determinate condizioni, due o più sistemi fisici rappresentano sottosistemi di un sistema più ampio, il cui stato quantico non è descrivibile singolarmente, ma esprimibile solo come sovrapposizione di più stati
- Questo vuol dire che misurando lo stato di un sistema (quindi osservandolo) si possa determinare simultaneamente il valore anche per gli altri stati

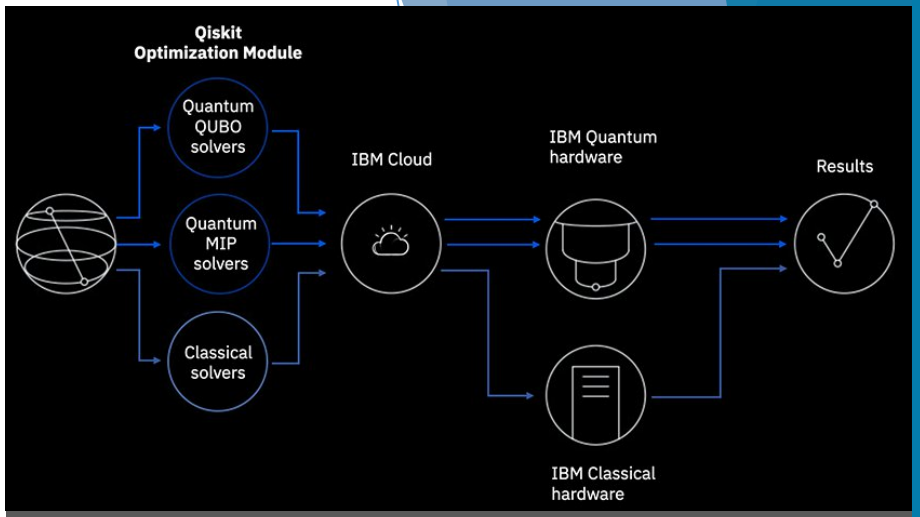
Misurazione

- Misurare uno stato vuol dire osservare il sistema in un determinato momento
- Il problema della misurazione quantistica introduce una distinzione tra due fasi: ***il prima ed il dopo la misurazione*** (rispetto alla funzione d'onda)
- Prima della misurazione la funzione d'onda, secondo l'equazione di Schrödinger, evolve tranquillamente
  - Equazione di Schrödinger: $i\hbar\frac{\partial}{\partial t}\Psi = H\Psi$
- Appena il ricercatore effettua la misurazione, l'equazione di Schrödinger viene messa da parte ed avviene il **collasso** della funzione d'onda.
- Quindi è l'azione di misurare che «fa qualcosa» al sistema

Circuito Quantistico

Un circuito quantistico è un modello per l'esecuzione di processi quantistici dati da una sequenza di porte, misurazioni e inizializzazioni di qubit





- Sono scritti in modo tale che l'asse orizzontale sia il tempo
- Il circuito inizia a sinistra e finisce a destra
- Le linee orizzontali sono qubit
- Le linee doppie rappresentano i bit classici
- Gli elementi che sono collegati a queste linee sono operazioni che vengono eseguite sui qubit, come misurazioni o attività delle porte
- Queste linee, inoltre, definiscono la *sequenza degli eventi*

Dalla crittografia classica alla QKD

- La maggior parte dei nostri protocolli di comunicazione si basa principalmente su tre funzionalità crittografiche fondamentali:
  - Crittografia a Chiave Pubblica
  - Firma Digitale
  - Scambio delle Chiavi.
- Si basano su determinati problemi computazionali:
  - La fattorizzazione dei numeri interi
  - Il logaritmo discreto.
- L'algoritmo di Shor è in grado di "rompere" i sistemi crittografici a chiave pubblica perché riesce a eseguire il processo di fattorizzazione in un tempo polinomiale sotto condizioni che il Circuito Quantistico abbia:
  - Qubit Logici = 4700 e Profondità di Circuito = $8 * 10^9$

QUESTI ALGORTIMI NON SONO PIU SICURI PER VIA DEI COMPUTER QUANTISTICI

Cos’è una Quantum-Key-Distribution

- La Quantum Key Distribution (QKD) è una tecnologia di crittografia a chiave quantistica che utilizza la meccanica quantistica per generare e distribuire una chiave crittografica sicura tra due parti.

Utilizza:

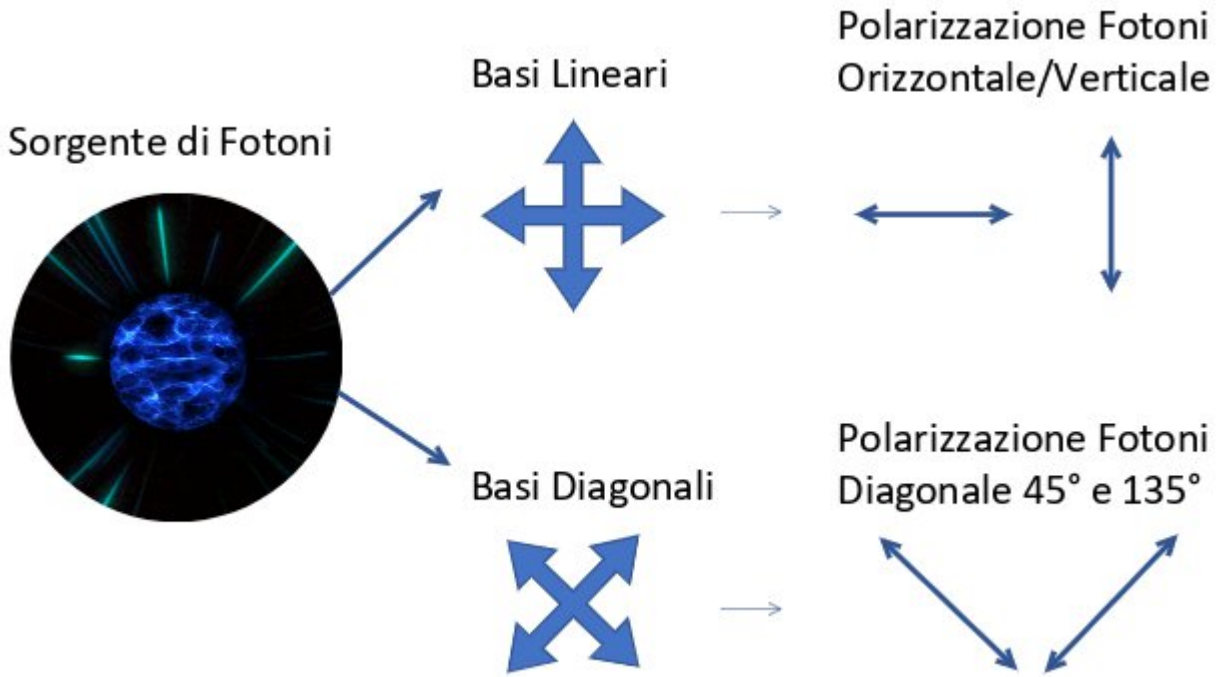
- La sovrapposizione degli stati
- L'Entanglement

Proprietà utilizzate per creare una comunicazione crittografica intrinsecamente sicura.

Necessita di una sorgente Puramente Casuale di emissione dati, come ad esempio la polarizzazione di un fotone

NOTA: *Si differenzia dalla Post-Quantum Cryptography (PQC) poiché quest’ultima utilizza alcuni algoritmi (complessi) per difendersi da attacchi di computer quantistici, mentre la QKD è utilizzata per scambiare chiavi quantistiche per criptare poi i dati (un processo analogo a quello dell’RSA ma molto più sicuro)*

Polarizzazione del Fotone



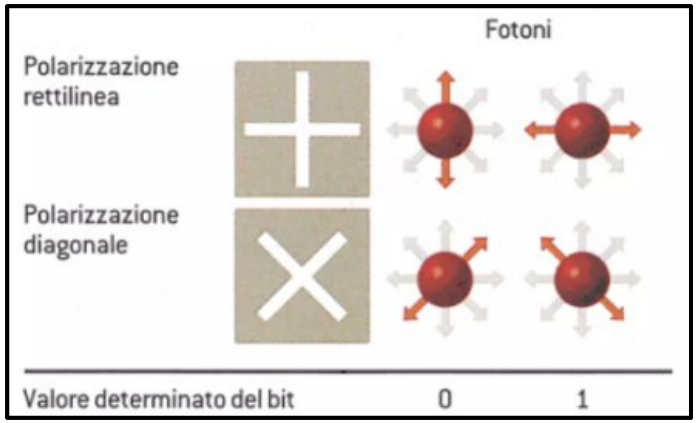
Probabilità con la quale avviene la polarizzazione di un fotone

	0° Filtro (base)	90° Filtro (base)	45° Filtro (base)	135° Filtro (base)
0° ↔	1	0	1⁄2	1⁄2
90° ↕	0	1	1⁄2	1⁄2
45° ⤢	1⁄2	1⁄2	1	0
135° ⤡	1⁄2	1⁄2	0	1

BB84 – Protocollo Crittografico Quantistico

- Definiamo come:
  - Sistema quantistico ciò che rappresenta la chiave crittografica
  - Osservatore colui che effettua una misurazione (anche un eventuale attaccante che utilizza un attacco del tipo Man In The Middle)

- Il protocollo BB84 relativo alle QKD utilizza 2 tipi di polarizzazioni in 4 basi:

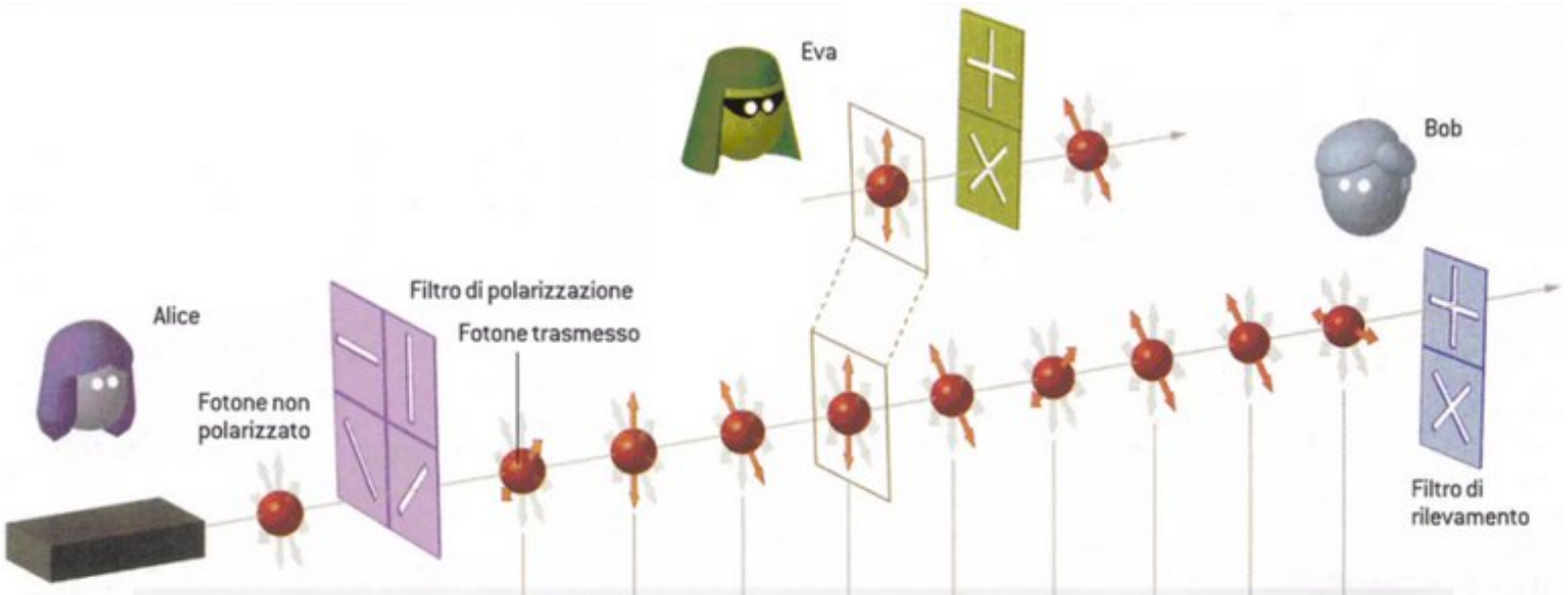


- Utilizzo di due caratteristiche fondamentali della meccanica quantistica:
  - stati non ortogonali tra di loro >> Teorema di no-cloning
    - non è possibile duplicare esattamente uno stato quantistico sconosciuto a priori
  - L'azione di misurare disturba lo stato.

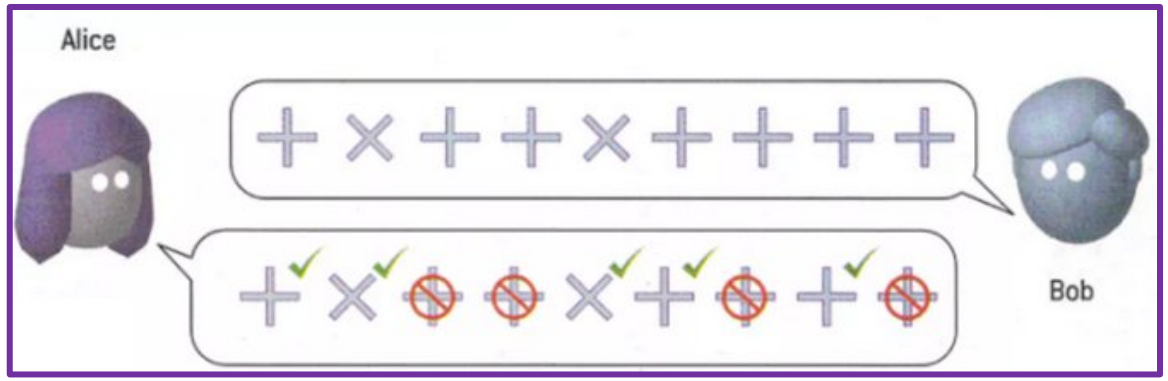
Funzionamento Algoritmo (step-by-step)

- 1. Alice sceglie una stringa casuale di bit ed una sequenza casuale di basi di polarizzazione (rettilinea, o diagonale) e manda a Bob una, sequenza di fotoni, ognuno rappresentante un bit della stringa, nella base scelta.
- 2. Bob sceglie casualmente per ogni fotone mandatogli da Alice se misurare la polarizzazione rettilinea o diagonale e interpreta ogni risultato come 0 o 1
- NOTA: tutta l'informazione è persa quando si tenta di misurare la polarizzazione rettilinea di un fotone diagonale o viceversa. Così Bob ottiene dati significativi solo dal 50% dei fotoni che ha misurato (supponendo che non vi siano state alterazioni dovute a intercettazioni)
- 3. Bob annuncia pubblicamente le basi (cioè i filtri) con cui ha analizzato i fotoni.
- 4. Alice comunica a Bob. pubblicamente, quale filtro ha scelto correttamente. Si scartano tutte le posizioni dei bit per le quali Bob ha eseguito un tipo di misurazione sbagliata o per le quali non è stato rilevato alcun fotone.
- 5. I Bit corrispondenti saranno quelli candidati a formare la chiave segreta con la quale andranno cifrati i dati (dopo una successiva verifica di corrispondenza di alcuni di questi)

Quantum Channel



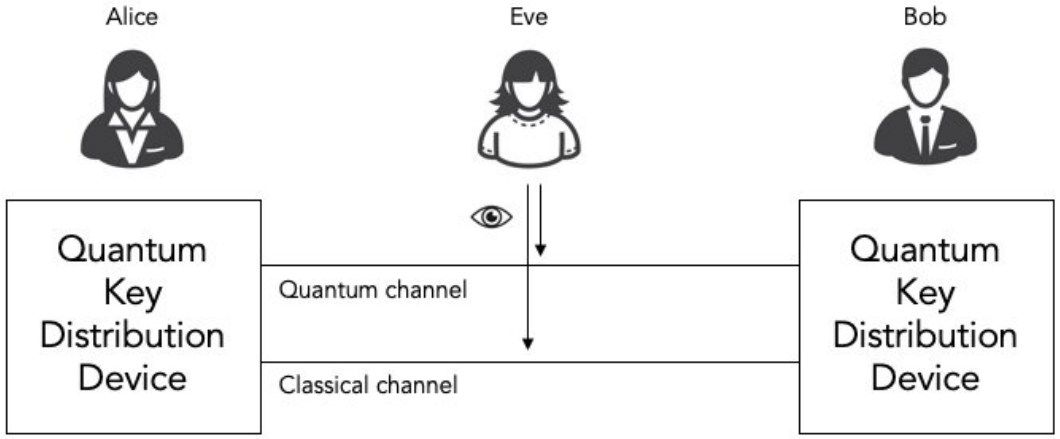
Sequenza di bit di Alice:	0	0	1	0	1	0	1	1	1
Schema di filtraggio di Alice:	/	|	\	|	\	/	\	\	–
Schema di rilevamento di Bob:	+	+	+	+	×	+	+	×	+
Misurazione dei bit di Bob:	1	0	1	0	1	0	0	1	1
Sequenza ottenuta (chiave):	–	0	–	0	1	–	–	1	1



Classic Channel

Python Simulazione

- La seguente simulazione implementata in Python mostra il funzionamento dell'algoritmo, è stato riadattato e modificato per far vedere due tipologie si situazioni, una con esito negativo e l'altra con esito positivo.
  - 1) Trasmissione **senza** Man-In-The-Middle, e quindi esito positivo della sicurezza della chiavi di Alice e Bob coincidono
  - 2) Trasmissione **con** Man-In-The-Middle, e quindi esito negativo della sicurezza della chiave, il che implica una non coincidenza nel confronto delle chiavi tra Alice e Bob



Autenticazione, Privacy e Error-Correction

- L'autenticazione è garantita da:
  - L’utilizzo di un *canale quantistico* che non può essere clonato
  - La verifica delle *proprietà di sovrapposizione* quantistica garantisce che la chiave condivisa segreta sia stata effettivamente generata attraverso il protocollo BB84
- La Privacy è garantita da:
  - La crittografia dei dati utilizzando la chiave quantistica condivisa generata.
- La Correzione degli errori avviene nel seguente modo:
  - Si misurano alcuni qubit di controllo in una base di codifica diversa da quella utilizzata per codificare il messaggio. Questi qubit di controllo vengono utilizzati per verificare che lo *stato quantistico dei qubit del messaggio* non sia stato alterato durante la trasmissione.
    - Scelta Qubit random
    - Alice codifica i qubit di controllo in una base di codifica diversa da quella utilizzata per codificare il messaggio e li invia a Bob insieme ai qubit del messaggio
    - Bob misura i qubit di controllo in entrambe le basi di codifica e lo comunica ad Alice quali basi ha utilizzato per la misura dei qubit di controllo
    - Alice comunica a Bob quali basi ha utilizzato per codificare i qubit di controllo.
    - Se Bob ha utilizzato la base corretta per la misura dei qubit di controllo, allora è probabile che i qubit del messaggio non abbiano subito errori e possono essere utilizzati per generare la chiave condivisa.
      Altrimenti, probabilmente i qubit del messaggio hanno subito errori e si scartano.

Accenni su protocolli alternativi per QKD

- PROTOCOLLO EKERT-91 (E-91)

A differenza del BB84 che sfrutta la sovrapposizione degli stati questo utilizza il concetto di Entanglement.

- Quello che avviene è l'invio di un due qubit, da una sorgente, uno verso Alice e l'altro verso Bob, i quali effettuano delle Misurazioni in basi randomiche:
- Alice sceglie tra {0, π/8 , π/4} mentre Bob tra {- π/8 , 0, π/8}, successivamente registrano il risultato della misurazione e trasmettono la base di misurazione che hanno utilizzato, attraverso il canale classico.
- Ora si creano due gruppi G_1 (esca) e G_2 (key). In G_1 misurano con delle basi diverse l'uno da l'altra, in G_2 usando la stessa base. Facendo dei test statistici sugli stati di Bell (S-Test) si può rilevare un eventuale intercettatore, se cosi fosse la connessione viene chiusa e si riapre un canale.
- Se il canale quantistico è sicuro, G_2 può essere utilizzato come chiave grezza perché Alice e Bob possono ricevere le stesse misurazioni.
- Sia Alice che Bob concordano sul fatto che la misura $|0\rangle$ rappresenta il classico bit 0 mentre la misura $|1\rangle$ rappresenta il classico bit 1, quindi ottengono la loro chiave per la cifratura.

PRO e CONTRO della QKD

- PRO
  - Assolutamente Sicuro
    - Grazie alle leggi della MQ
    - Sicuro contro attacchi quantistici
    - Indipendente dalla potenza del calcolatore

- Contro
  - Richiede linee dedicate e HW specifici
    - Aumento del costo di produzione
    - In forte via di sviluppo

NOTA:
Se leggiamo quanto scritto sopra in chiave classica vediamo che Pro e Contro si “invertono”. In breve: nel caso classico l’implementazione e l’accessibilità sono un Pro, mentre la sicurezza che è basata su problemi matematici è un Contro, poiché vulnerabile dalle leggi della MQ.

Questo indica inevitabilmente che nel momento in cui il Quantum Computing prenderà il sopravvento la sicurezza informatica verrà messa a rischio, tutti gli algoritmi ad oggi più utilizzati e diffusi saranno vulnerabili.

GRAZIE PER L'ATTENZIONE