



Quantum Key Distribution - Protocolli, Applicazioni e Realizzazione di un Simulatore

Autore

Egidio Giacoia
Matr. 0522500488

Coordinatori

Prof. Alfredo De Santis
Prof. Arcangelo Castiglione
Prof. Raffaele Pizzolante

Indice

Introduzione alla Crittografia Quantistica

- Storia della Crittografia
- Limiti della Crittografia Moderna
- La Crittografia Quantistica e QKD

Quantum Key Distribution

- Principi Fisici
- Meccanismo e Protocolli
- Sicurezza
- Attacchi
- Limiti
- Applicazioni: Quantum Network
- Overview sul futuro

BB84 Simulator

- Descrizione del tool
- Esempio di esecuzione





Introduzione alla Crittografia Quantistica

Storia della Crittografia



Cos'è la crittografia

- ▶ Possiamo definirla come: « *lo studio delle tecniche matematiche, per proteggere l'informazione digitale, i sistemi di elaborazione e le computazioni distribuite, da attacchi avversari* »

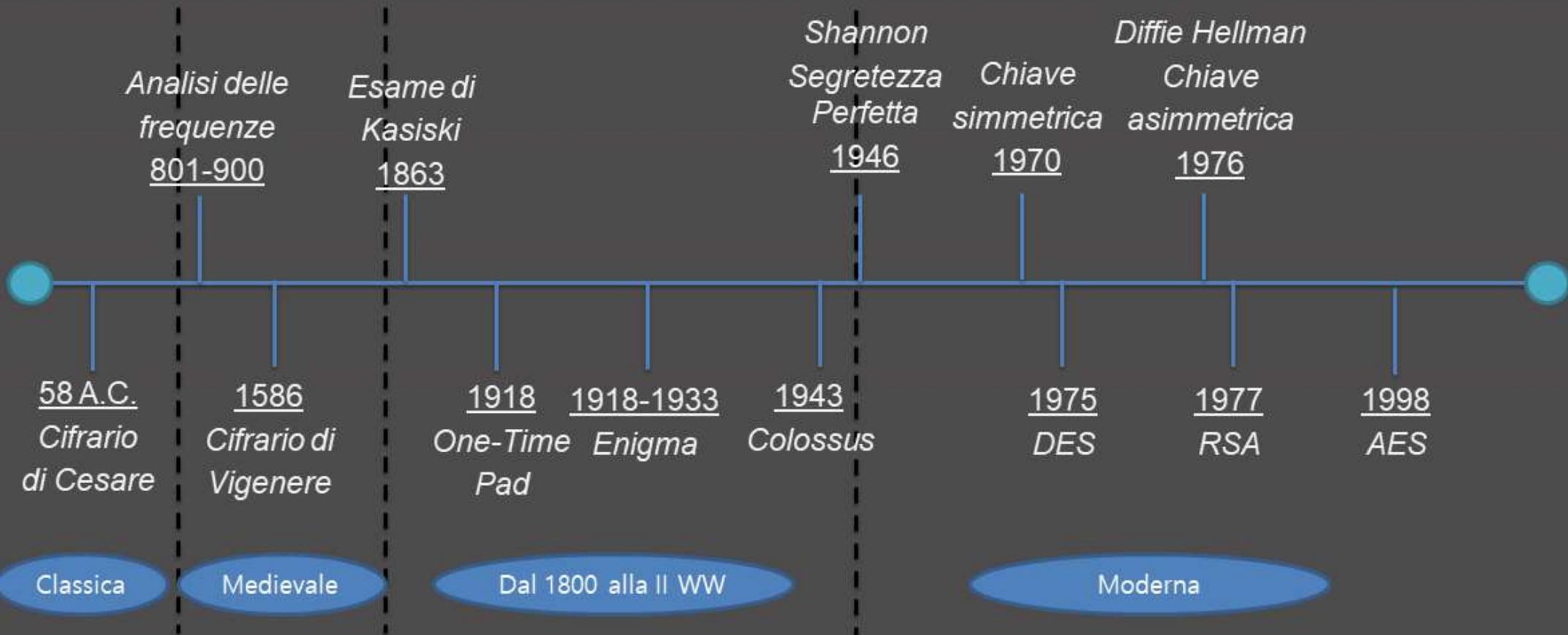
Obiettivi

- ▶ Un mittente e un destinatario devono poter comunicare in un formato sicuro ed incomprensibile a terzi
- ▶ L'autenticazione dei messaggi per dimostrare che non sono stati modificati in transito

Quando nasce

- ▶ Inizia con metodi di cifratura che utilizzavano carta e penna...
...fino ad arrivare all'utilizzo di algoritmi di cifratura

Introduzione alla crittofotografia quantistica – Storia della Crittografia





Introduzione alla Crittografia Quantistica

Limiti della Crittografia Moderna

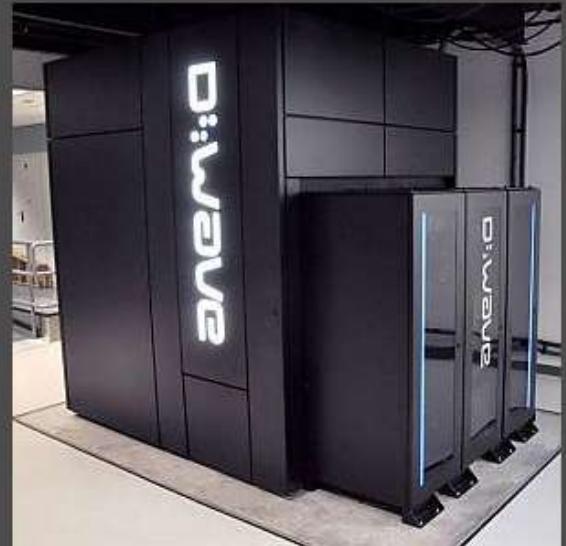


L'avvento del Computer Quantistico

Idealizzazione

- ▶ Nel 1982 Richard Feynman pensò di sfruttare dei fenomeni della fisica quantistica per ideare un computer quantistico:
 - una macchina con alta capacità elaborativa in grado di trasformare un problema di complessità esponenziale (NP-Completo) in un problema di complessità polinomiale (P)

- ▶ Dal 2001 si è partiti con la costruzione di prototipi fino ad arrivare a dei veri e propri “piccoli” computer quantistici



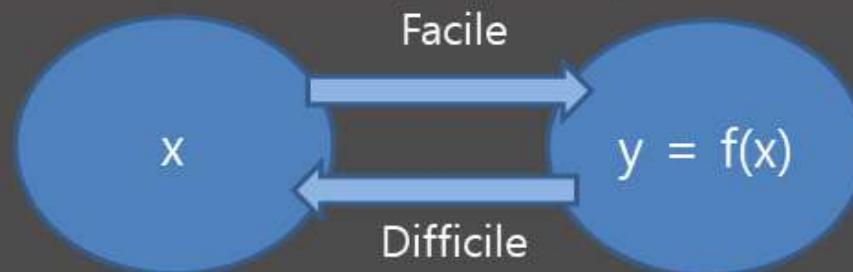


L'avvento del Computer Quantistico

Che problemi causa?

- ▶ Per molti schemi di cifratura basano la loro sicurezza su una classe di problemi matematici

Funzioni one-way



- Facile da calcolare
- Difficile da invertire

- ▶ L'ipotesi di una realizzazione computer quantistico a pieno regime mette a serio rischio l'intera crittografia moderna rendendola facilmente vulnerabile



Il problema dello scambio della chiave

- ▶ Due parti (Alice e Bob) vogliono poter condividere una chiave segreta in maniera sicura



- ▶ Se vogliamo mettere in comunicazioni più utenti N, ognuno di essi deve condividere una chiave simmetrica con un utente, richiedono la distribuzione di un numero di chiavi proporzionale a N^2

Soluzione

- utilizzare un Key Distribution Center (se il numero di utenti è ridotto)
- utilizzare protocolli basati sui principi della crittografia a chiave pubblica (Scambio Diffie-Hellman)



Il problema dello scambio della chiave

Che problemi causa?

- La sicurezza si basa sulla difficoltà computazionale di recuperare la chiave privata dalla chiave pubblica: con il progredire della tecnologia potrebbe essere un fattore limitante
- Vulnerabile ad attacchi di tipo man-in-the-middle: non si può essere certi infatti che la chiave appartenga davvero alla persona nominata nell'intestazione della chiave stessa

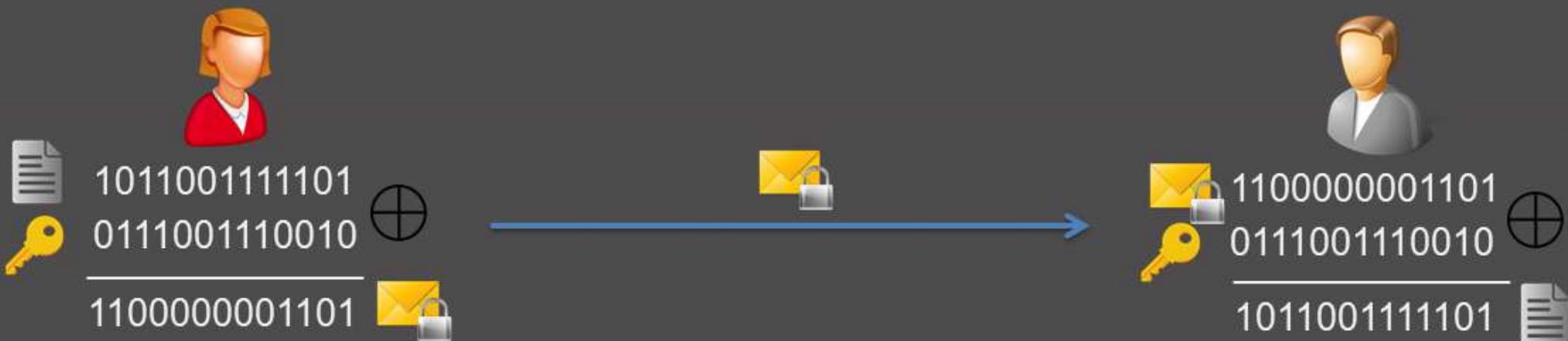




Schemi perfettamente sicuri: One-Time Pad

- ▶ È uno schema crittografico che è assolutamente inattaccabili dal punto di vista teorico
- ▶ Shannon ne ha dimostrato la sua validità e segretezza perfetta

Funzionamento





Schemi perfettamente sicuri: One-Time Pad

Pro

- Casualità dei caratteri che compongono la chiave
- Ogni cfrato corrisponde ad un messaggio equibrobabile

Contro

- La chiave non deve essere mai riutilizzata per cifrare un messaggio
- La chiave deve avere la stessa lunghezza del messaggio da trasmettere
- Problema della condivisione della chiave

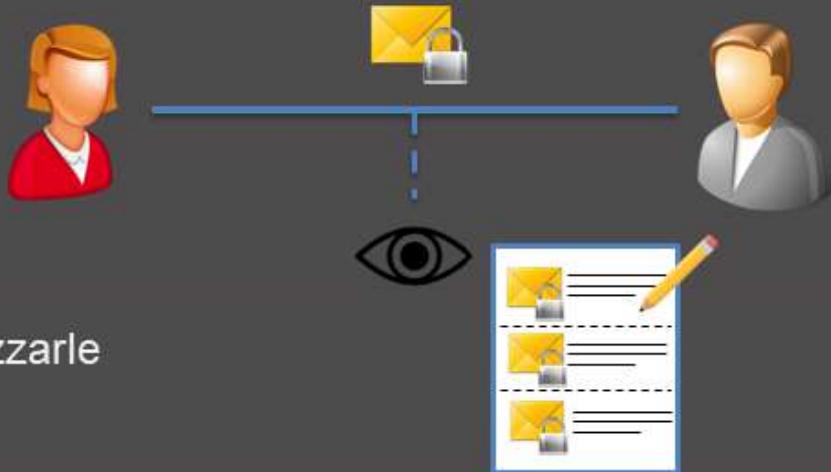
Che problema causa?

- Schemi di questo genere non sono utilizzabili attualmente
- Con la crittografia moderna non si può ottenere la nozione di segretezza perfetta



Il problema dell'eavesdropping

- ▶ Due parti stanno comunicando su un canale classico sicuro scambiando informazioni
- ▶ Un intercettatore (eavesdropper) che ha accesso al canale può osservare le informazioni in transito e memorizzarle



Che problemi causa?

- Con la crittografia moderna l'eavesdropping è sempre ammissibile e non rilevabile



Introduzione alla Crittografia Quantistica

La Crittografia Quantistica e QKD

Introduzione alla Crittografia Quantistica – La Crittografia Quantistica e QKD



Cos'è la Crittografia Quantistica

- ▶ Possiamo definirla come:
«la scienza che sfrutta le proprietà della meccanica quantistica per eseguire attività crittografiche»

Obiettivi

- ▶ Trasmettere le informazioni tra le parti in maniera totalmente sicura rilevando la presenza di eventuali eavesdropper con potenza computazionale illimitata la cui tecnologia è ristretta dalle leggi fondamentali della meccanica quantistica
- ▶ Cercare di affermarsi nel mondo reale (è un campo di ricerca)

Quando nasce

- ▶ Introdotta nel 1970 da Wiesner (Quantum Conjugate Coding), realizzata da Charles Bennet (BB84, QKD) ...
... fino ad aziende specializzate nel settore (IDQuantique, MagicQ Technologies)

Introduzione alla Crittografia Quantistica – La Crittografia Quantistica e QKD



Cos'è la Quantum Key Distribution

- ▶ E' una delle principali applicazioni della meccanica quantistica alle telecomunicazioni e all'informatica

Obiettivo

- ▶ Utilizzare un canale quantistico e classico per fare in modo che due interlocutori scambino una chiave casuale di lunghezza arbitraria in completa sicurezza, con la certezza che ogni tentativo di intercettazione verrebbe rilevato inequivocabilmente

Quando nasce

- ▶ Definita nel 1984 da Charles Bennet nel protocollo BB84, al quale ne seguirono altri...

...fino alle realizzazioni pratiche (limitate) di Quantum Network (dal 2001 - ad oggi)

Introduzione alla Crittografia Quantistica – La Crittografia Quantistica e QKD



Limitazioni

Crittografia Moderna

Computer
Quantistico

Problema
scambio della
chiave

One-Time Pad

Eavesdropping

Soluzione

Crittografia Quantistica

- un approccio fisico più che matematico fornendo una sicurezza incondizionata
- Meccanismo QKD risolve il problema dello scambio della chiave
 - Utilizzo di un canale di comunicazione quantistico sul quale non è possibile effettuare un'osservazione senza essere scoperti
 - Permette l'utilizzo di schemi One-Time Pad
 - Chiave di lunghezza arbitraria
 - Generazione casuale e sicura



Quantum Key Distribution

Principi Fisici



Cos'è la Meccanica Quantistica

- ▶ «E' la teoria fisica che descrive il comportamento della materia, della radiazione e le reciproche interazioni, nel mondo microscopico»

Concetti

- Si contrappone alla meccanica classica
- Si abbandona la visione deterministica del mondo fisico
- La realtà viene modellata attraverso l'introduzione di funzioni di probabilità
- il "caso" gioca un ruolo essenziale: è una proprietà intrinseca del sistema (Dio gioca a dadi?)

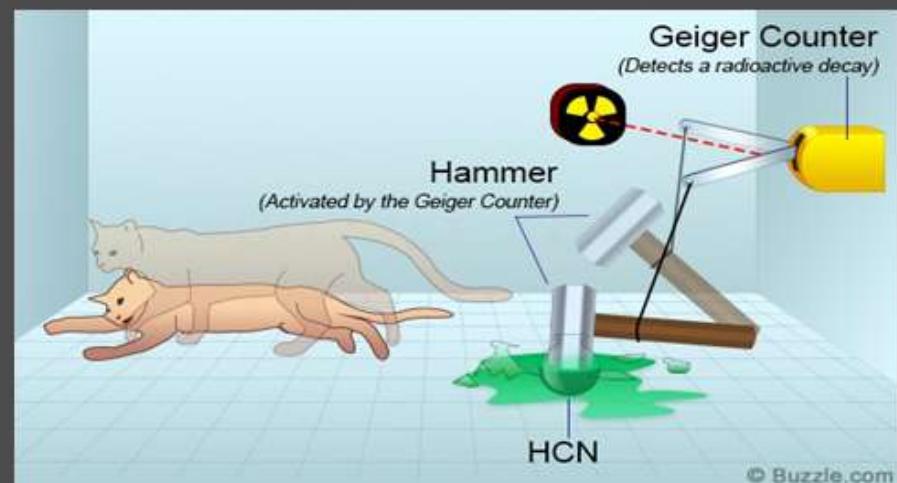
Quantum Key Distribution – Principi fisici

Teoria Quantistica

- ▶ L'energia non è solamente un onda che si propaga in modo continuo e in tutte le direzioni, ma l'energia viene emanata in quanti predefiniti dello stesso valore
- ▶ Un quanto è descritto da una funzione d'onda probabilistica (l'equazione di Schrodinger) che dà la probabilità di trovare il quanto in qualsiasi posizione particolare, ma non la sua posizione reale

Sovrapposizione Quantistica

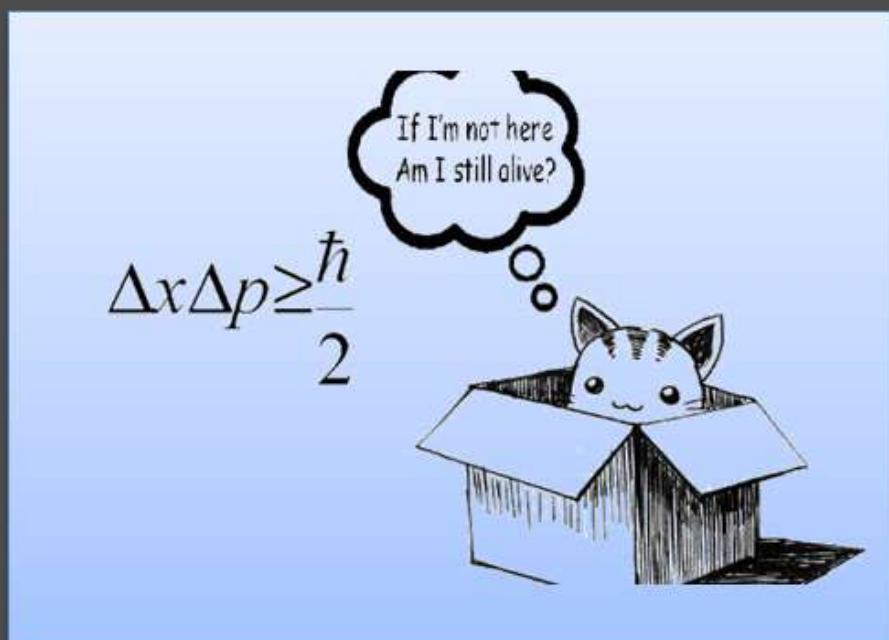
- ▶ Un quanto può avere molti stati possibili, ma esiste in tutti loro simultaneamente in assenza di un osservatore
- ▶ Una volta che un osservatore misura il quanto, la funzione d'onda collassa e uno degli stati precedentemente sovrapposti è scelto in base alla probabilità inherente alla funzione d'onda





Il Princípio di Indeterminazione di Heisenberg

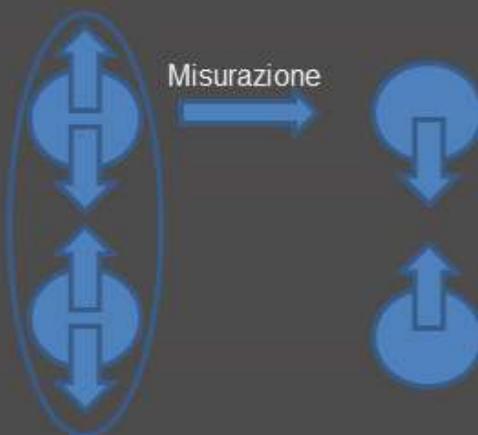
- ▶ In un sistema fisico microscopico ci sono coppie di proprietà osservabili (coniugate) che non si possono entrambe determinare o misurare in modo esatto allo stesso tempo:
 - la misurazione di una delle due proprietà coniugate altera irrimediabilmente l'altra
- ▶ Questa alterazione non dipende dalle scarse capacità dei sistemi di misurazione, ma è un'obiettiva impossibilità



Quantum Key Distribution – Principi fisici

Quantum Entanglement

- ▶ Si possono produrre coppie (EPR) di quanti che si comportano come se fossero una singola entità



Per esempio, i quanti possiedono una proprietà chiamata "spin": un quanto potrebbe avere spin up e spin down, in modo che lo spin totale sia zero ma fino a che una misura non viene effettuata non è chiaro quale sia quale delle due

- ▶ Se la coppia è separata, la misurazione di una fa collassare la funzione d'onda dell'altro nello stato opposto
- ▶ Sembra sapere istantaneamente che il suo partner è stato misurato, apparentemente in contraddizione con la scoperta di Einstein che nulla può viaggiare più veloce della luce

Quantum Key Distribution – Principi fisici

Fotone

- ▶ La prima conseguenza della teoria dei quanti fu la scoperta che la luce oltre a comportarsi come un'onda si comporta anche come una particella
- ▶ Il quanto (fotone) che la luce trasporta ha un'energia limitata
- ▶ I fotoni hanno un proprio angolo di polarizzazione compreso fra 0° e 180°



- ▶ Il canale quantistico è composto da:
 - Un dispositivo ottico di emissione capace di produrre fotoni polarizzati
 - Un canale quantistico che permette alla luce di propagarsi (fibra ottica o spazio della vista libera)
 - Un dispositivo che permetta all'utente destinatario di misurare la polarizzazione dei fotoni

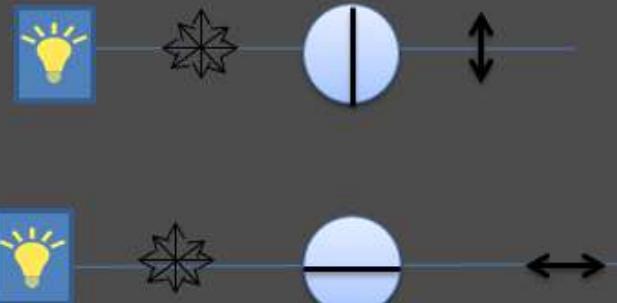
Fotone: Polarizzazione

- ▶ Una base di polarizzazione è formata da due stati di polarizzazione ortogonali

Base Rettilinea  = (↔, ↑) = (0°, 90°)

- ▶ La sorgente di luce genera i fotoni con una polarizzazione arbitraria e per poter far assumere una determinata polarizzazione bisogna utilizzare dei filtri polarizzatori:

- Il fotone viene polarizzato secondo un determinato angolo
- Se i fotoni polarizzati con un angolo differente rispetto al filtro provano ad “attraversarlo” vengono fermati oppure lo oltrepassano assumendo la polarizzazione secondo l’angolo

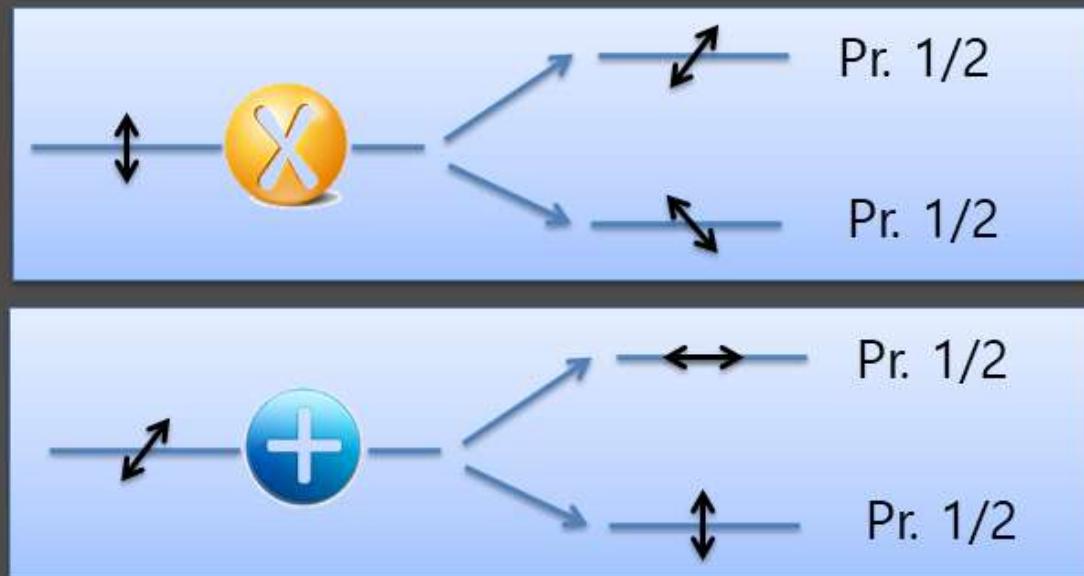


Quantum Key Distribution – Principi fisici

Basi Coniugate

- ▶ Due basi sono coniugate se la misurazione della polarizzazione di una randomizza l'altra

Basi	Stati Polarizzazione	Filtri Polarizzatori	Gradi
Rettilinea 	 	 	0°, 90°
Diagonale 	 	 	45°, 135°



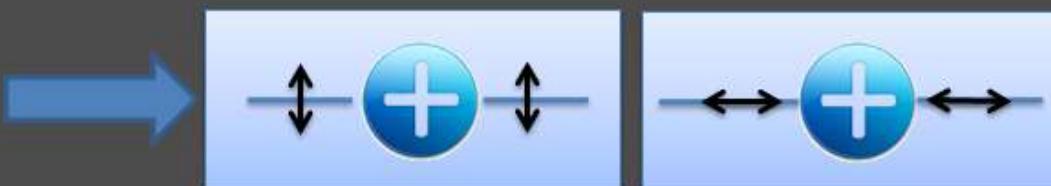
Quantum Key Distribution – Principi fisici



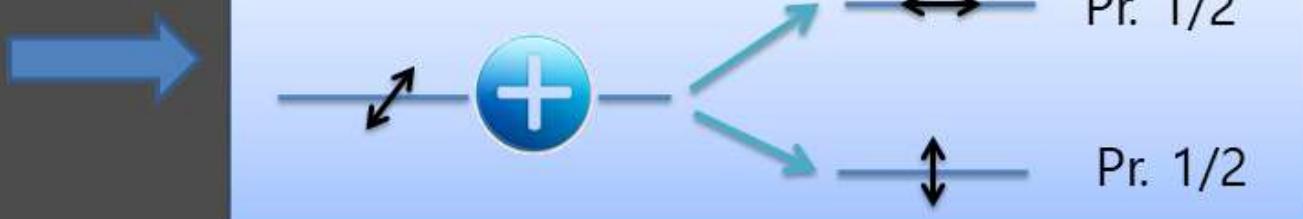
Fotone: Misurazione

- ▶ Supponiamo di effettuare una misura dei fotoni con angolo di polarizzazione 0° e 90°
Abbiamo due casi possibili:

1) Se il fotone è già polarizzato secondo la base utilizzata lo attraversa senza alterarne la polarizzazione



2) Se il fotone ha una polarizzazione intermedia (cioè 45° o 135°) si ha un comportamento casuale





Quantum Key Distribution

Meccanismo e Protocolli

Quantum Key Distribution – Meccanismo e Protocolli



ScENARIO DI BASE

Parti in gioco

- **Alice**: crea e codifica la chiave
- **Bob**: decodifica il segnale ricevuto
- **Eve**: intercetta le informazioni per compromettere la chiave

Canali di comunicazione

- **Quantistico**: vengono inviati i fotoni (Qubits)
- **Classico**: scambiano informazioni relative al protocollo

Obiettivo

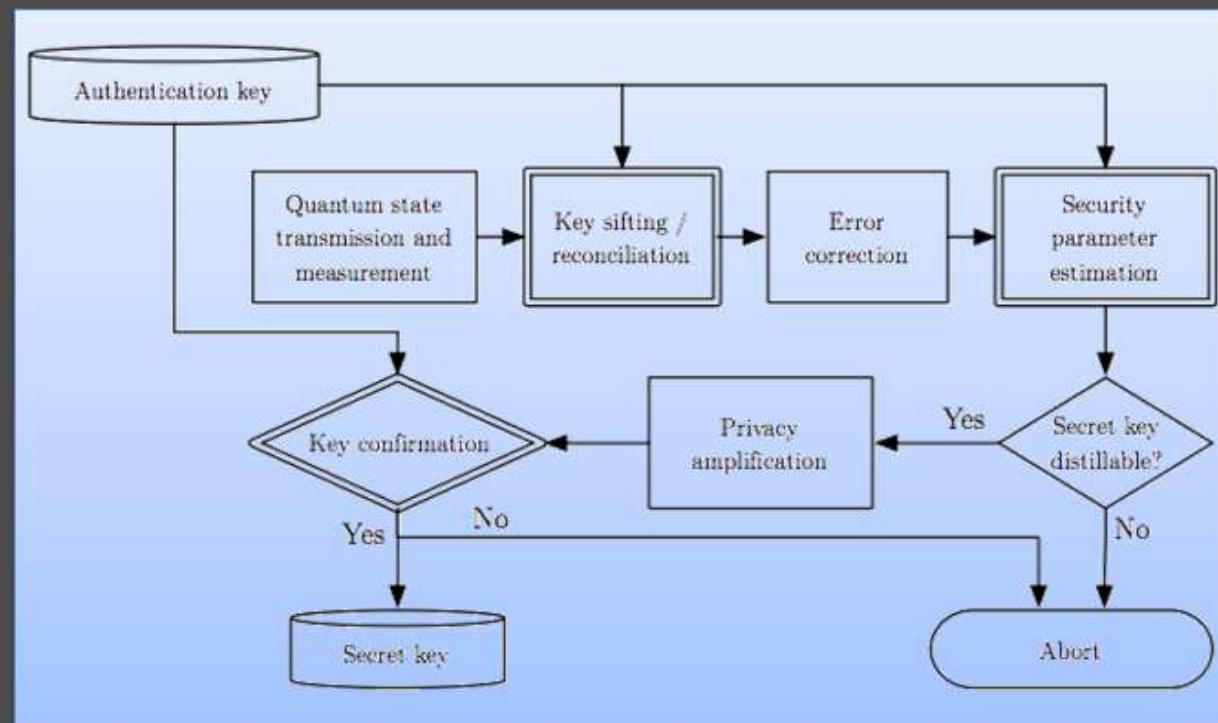
Permettere a due parti (Alice e Bob) di condividere una sequenza casuale di caratteri, chiave, senza che un possibile infiltrato nella comunicazione (Eve) riesca ad ottenere informazione a riguardo e rilevare l'intrusione



Quantum Key Distribution – Meccanismo e Protocolli

Meccanismo Generale della QKD

- ▶ Bisogna definire delle regole e passi da seguire, un protocollo di distribuzione delle chiave, combinando l'elaborazione quantistica e procedure classiche ben consolidate:
 - *Raw Key Exchange*
 - *Key Sifting*
 - *Key Distillation*
- ▶ Inoltre bisogno garantire la possibilità di scartare la chiave segreta in una qualsiasi delle fasi se si ritiene che non si sia ottenuta abbastanza sicurezza da essa





Meccanismo Generale della QKD – Raw Key Exchange

- ▶ Questa fase è l'unica parte quantistica della QKD in cui Alice e Bob si scambiano "alcuni stati quantici" i quali transitano lungo un canale quantico inviati da Alice per essere poi misurati da Bob, con o senza la presenza di Eve



- ▶ In tutti i successivi passi di un protocollo, si utilizzerà come forma di comunicazione solo un canale classico sicuro (classical post-processing)



Meccanismo Generale della QKD – Sifting Key

- ▶ Alice e Bob decidono tra di loro quale delle misure verrà utilizzata per determinare la chiave segreta
- ▶ Le regole decisionali dipendono dal protocollo utilizzato e alcune misure verranno scartate:
 - ad esempio se le misure utilizzate da Alice e Bob non corrispondevano





Meccanismo Generale della QKD – Distillation Key

- I canali sono soggetti alla perdita di informazioni e il protocollo deve essere praticabile anche in presenza di errori di trasmissione. Quindi sono necessari tre ulteriori step:

1) Error Correction

- Si calcola il Quantum Bit Error Rate:
 - Se è inferiore a un valore massimo predeterminato, la chiave segreta passa alla fase successiva della distillazione della chiave
 - Altrimenti le quantità di informazioni perse è troppo grande per garantire la segretezza, quindi la chiave segreta viene scartata e viene avviato un nuovo ciclo QKD
- Si presume che tutti gli errori siano dovuti a intercettazioni

2) Privacy Amplification

- Ha come scopo quello di rimuovere almeno lo stesso numero di bit dalla chiave di cui Eve potrebbe esserne a conoscenza
- Comprime la chiave setacciata di un fattore appropriato, determinato dall'indice QBER precedentemente calcolato

3) Autenticazione

- Bisogna eseguire un'autenticazione classica per garantire che Alice e Bob non siano i soggetti di un attacco man-in-the-middle (MITM)
- una chiave segreta deve essere pre-condivisa tra Alice e Bob, per l'utilizzo dell'autenticazione del primo scambio quantico
- L'autenticazione iniziale può essere estesa per coprire tutte le sessioni future

Quantum Key Distribution – Meccanismo e Protocolli



Protocollo BB84

- ▶ Alice e Bob vogliono generare una chiave crittografica segreta e condivisa
- ▶ Fra di esse sono presenti due canali: uno pubblico classico e uno quantistico in cui sia possibile inviare fotoni
- ▶ Le fasi del protocollo sono:
 - 1) *Creazione raw key e codifica*
 - 2) *Lettura – raw key exchange*
 - 3) *Sifting Key*
 - 4) *Distillation Key*



Quando nasce

- ▶ È stato proposto nel 1984 da Charles H. Bennet e Gilles Brassard



Protocollo BB84 – Creazione della raw key e codifica

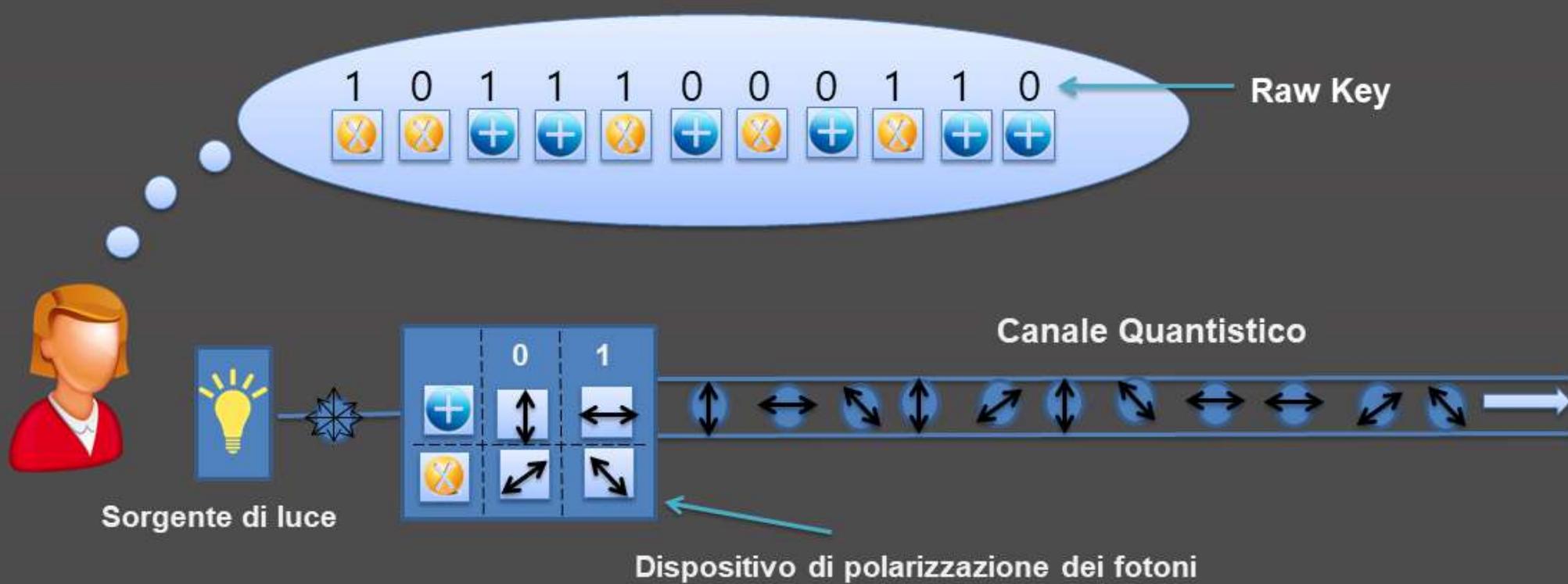
- Alice sceglie una stringa di bit (raw key) e una sequenza di basi casuali con cui codificarla (rettilinea o diagonale)
- ▶ Le informazioni che Alice scambia con Bob sul canale quantistico sono singoli fotoni ad una determinata polarizzazione: ogni bit 0 o 1 può essere trasmesso sul canale quantistico in forma di fotoni opportunamente polarizzati;
La codifica di un bit mediante un fotone polarizzato rappresenta un “qubit” (quantum bit)
- Alice invia sul canale quantistico a Bob la corrispondente sequenza di fotoni polarizzati, ognuno rappresentante un bit della stringa nella base scelta in accordo allo schema definito

Basi	Bit 0	Bit 1
Rettilinea		90°
Diagonale		45° 135°

Quantum Key Distribution – Meccanismo e Protocolli



Protocollo BB84 – Creazione della raw key e codifica





Protocollo BB84 – Lettura: Row Key Exchange

- Per ogni fotone ricevuto Bob sceglie casualmente (indipendentemente dalle scelte di Alice) una delle due basi di polarizzazione rettilinea o diagonale
 - Misura la polarizzazione del fotone e intrepreta ogni risultato come 0 o 1 a seconda dell'esito della corrispondente misura ottenendo la propria raw key
- Con tale strategia si ottiene una risposta del tutto causale in modo che Bob riesce ad ottenere dati significativi da circa il 50% dei fotoni che ha misurato

Quantum Key Distribution – Meccanismo e Protocolli

Protocollo BB84 – Lettura: Row Key Exchange





Protocollo BB84 – Sifting Key

- Una volta spediti e letti tutti i qubit, Bob comunica ad Alice pubblicamente utilizzando un canale classico le basi da lui utilizzate per misurare i fotoni che ha ricevuto, ma senza comunicare cosa ha misurato
 - Alice, analogamente, fa la stessa cosa comunicando le proprie basi a Bob
- ▶ Nessuna informazione chiave può essere acquisita da un intercettatore a questo punto
- Con queste informazioni tutti e due possono determinare i bit che sono stati inviati correttamente confrontando le basi e ogni fotone che è stato elaborato utilizzando basi non corrispondenti viene eliminato dalla raw key, ottenendo la sifting key
- ▶ Il processo di setacciamento dovrebbe, in media, lasciare la metà dei qubit, 50%

Quantum Key Distribution – Meccanismo e Protocolli



Protocollo BB84 – Sifting Key



Alice raw key

1	0	1	1	1	0	0	0	1	1	0
X	X	+/-	+/-	X	+/-	X	+/-	X	+/-	+/-
+/-	X	+/-	X	+/-	+/-	X	+/-	X	+/-	+/-

Alice sifting key

Bob raw key

0	0	1	1	0	0	0	1	1	1	0
+/-	X	+/-	X	+/-	X	+/-	X	+/-	X	+/-
X	X	+/-	+/-	X	+/-	X	+/-	X	+/-	+/-

Bob sifting key



Protocollo BB84 – Key Distillation

- In questa fase sia Bob che Alice estraggono un sottoinsieme di bit dalla propria sifting key e vengono inviati pubblicamente alla parte interessata
- Successivamente Alice e Bob verificano se questi bit di controllo inviati e ricevuti coincidono:
 - Se tutti i bit coincidono allora la comunicazione è avvenuta senza nessun ascolto e dunque viene generata la chiave segreta identica da entrambe le parti eliminando dalla sifting key i bit di controllo inviati
 - Altrimenti, se l'intervento di Eve è stato notevole, la trasmissione viene interrotta e bisognerà rieseguire nuovamente il protocollo da capo

Quantum Key Distribution – Meccanismo e Protocolli



Protocollo BB84 – Distillation Key



Alice siftng key

0	1	0	0	1	1	0
Bit di controllo Alice	1	0	1			
Bit di controllo Bob	1	0	1			
0	0	1	0			

Alice secret key

Bob siftng key

0	1	0	0	1	1	0
Bit di controllo Bob	1	0	1			
Bit di controllo Alice	1	0	1			
0	0	1	0			

Bob secret key



Protocollo BB84 – Post-Processing

Problema

- ▶ L'ultimo passo del protocollo descritto è dispendioso come controllo:
 - molti bit deve essere controllati per fornire un ragionevole margine di sicurezza anche se gli episodi di spionaggio sono stati poco frequenti e hanno causato pochi errori
- ▶ Possono capitare degli errori sperimentali:
 - ripolarizzazioni dei fotoni durante il transito, anche in assenza di origliamento
 - fotoni persi nel canale quantistico
 - fotoni che non sono stati rilevati correttamente
- ▶ Sembra che ci sono sempre errori e non si riesce a distinguere con sicurezza tra errori sperimentali e errori dovuti ad Eve



Protocollo BB84 – Post-Processing

Soluzione

- ▶ Si considera che gli errori siano sempre dovuti ad Eve e bisogna aggiungere due ulteriori fasi da applicare alla sifted key:

- 1) ***Error Correction***

Permette stimare la percentuale di errori trovati nella sifted key, Quantum Bit Error Rate (QBER);
Se questa percentuale è inferiore all'11%, allora si può passare alla fase Privacy Amplification

- 2) ***Privacy Amplification***

La chiave segreta viene modificata secondo una procedura tale che l'informazione che nel caso Eve ha sulla chiave segreta viene ridotta praticamente a zero

- ▶ Queste due fasi possono essere realizzate anche pubblicamente poiché le informazioni scambiate tra Alice e Bob non aiutano Eve a fare lo stesso



Protocollo di Eckert

- ▶ Metodo per eseguire la distribuzione delle chiavi tra due parti attraverso fotoni polarizzati entangled in un canale quantistico
 - Una sorgente produce una coppia di fotoni entangled che si propagano in versi opposti
 - Un intercettatore effettuando una misurazione sul sistema quantistico mirata a conoscere la stringa degli esiti o truccarne la sorgente, si ha inevitabilmente una certa probabilità di distruggere le correlazioni perfette degli esiti ottenuti da Alice e Bob



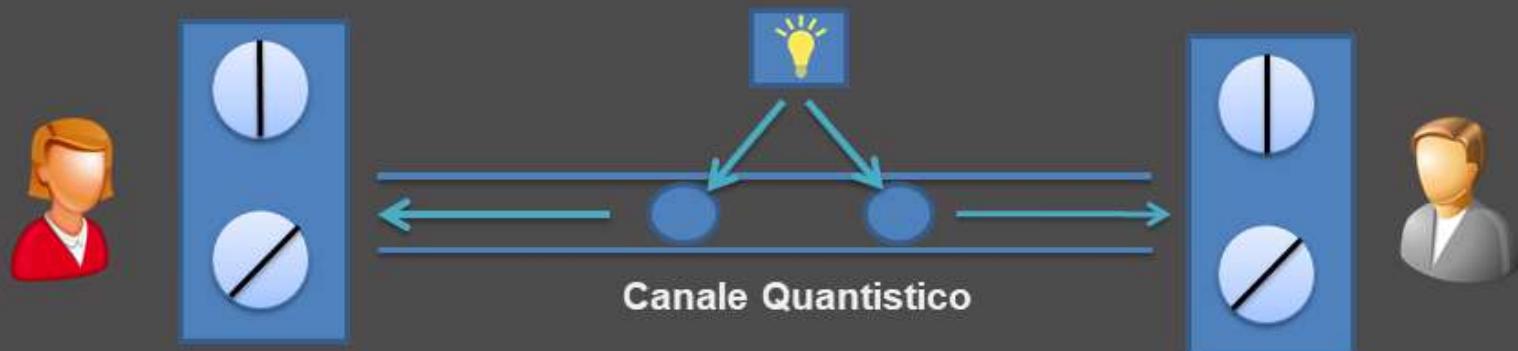
Quando nasce

- ▶ E' stato proposto nel 1991 da Ekert



Protocollo di Eckert

- ▶ Lo stato di polarizzazione del sistema dei due fotoni entangled sarà una combinazione lineare di stati di polarizzazione ortogonali tra loro
- ▶ Stato quantistico $|\alpha\rangle = 1/\sqrt{2} [|0^\circ, 0^\circ\rangle + |90^\circ, 90^\circ\rangle] = 1/\sqrt{2} [|45^\circ, 45^\circ\rangle + |135^\circ, 135^\circ\rangle]$
- ▶ Per effettuare le misurazioni dei fotoni le parti utilizzando due filtri di polarizzazione verticale 0° oppure a 45°





Quantum Key Distribution

Sicurezza

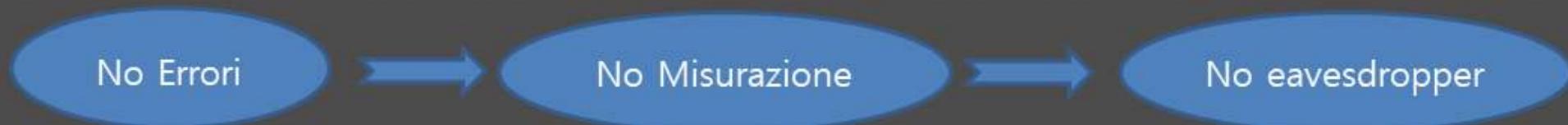


Eavesdropping

- ▶ Uno dei punti di forza di tutti i protocolli QKD è l'impossibilità per Eve di "ascoltare" la comunicazione ovvero:
 - di misurare lo stato del fotone e rinviarlo a Bob senza alterare il sistema ed evitare ad Alice e Bob di accorgersene

Come?

- ▶ Alice e Bob possono rilevare alcuni dei bit delle loro chiavi in modo da determinare la presenza di un intercettatore



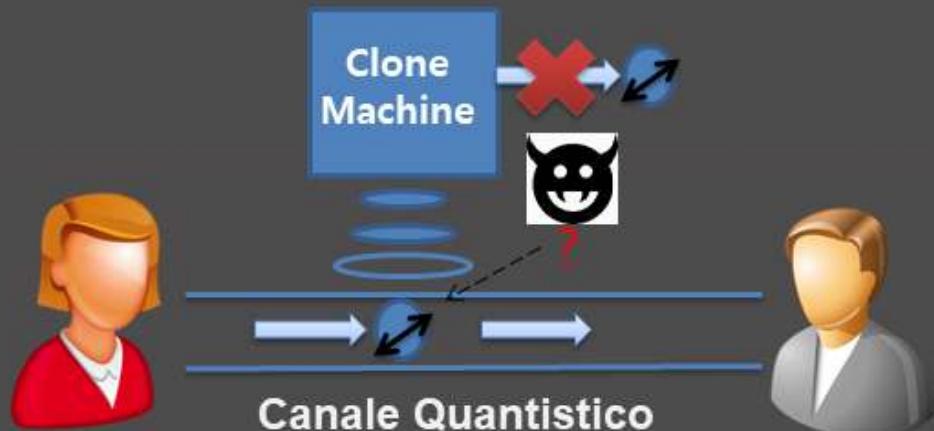
- ▶ Tuttavia se Eve prova ad intercettare una piccola frazione dei bit trasmessi l'errore prodotto risulterebbe molto limitato e diventerebbe quindi difficile per Alice e Bob rilevare la presenza di un eavesdropper

Quantum Key Distribution – Sicurezza



Eavesdropping

- ▶ Per il teorema di no-cloning quantistico Eve non è in grado di copiare perfettamente il fotone inviato da Alice, non conoscendolo a priori, e misurarlo separatamente una volta che Bob ha annunciato le basi usate





Sicurezza Incondizionata

- ▶ Eve non può ottenere alcuna informazione su una trasmissione quantistica senza essere rilevato



- ▶ Questo è vero anche se Eve avesse risorse e tempo di calcolo infiniti, o un computer quantistico, in quanto le leggi della fisica lo impediscono
- ▶ Punto di forza della crittografia quantistica: sicurezza incondizionata immune da intercettazioni non rilevate



Sicurezza Incondizionata

Sicurezza
Incondizionata

Condizioni

- Eve non può ispezionare i dispositivi di Alice e Bob per vedere o influenzare la loro creazione o il rilevamento dei fotoni
- I generatori di numeri casuali che Alice e Bob usano per impostare le loro apparecchiature deve essere veramente casuale e attendibile in modo implicito
- Il canale di comunicazione classico deve essere autenticato utilizzando uno schema di autenticazione incondizionatamente sicuro (protocollo di Carter Wegman)
- Eve deve obbedire alle leggi della fisica
- Il messaggio deve essere crittografato utilizzando uno schema simile ad OTP



Quantum Key Distribution

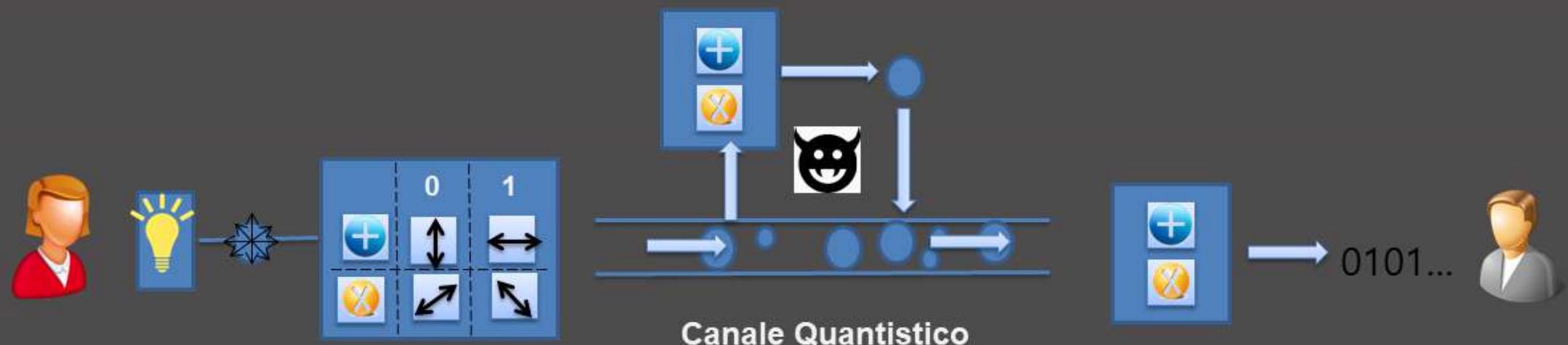
Attacchi

Quantum Key Distribution – Attacchi



Attacco di intercettazione-rinvio

- Eve misura gli stati quantici, fotoni, inviati da Alice e invia stati di sostituzione a Bob, preparati nello stato che misura;
Nel protocollo BB84, ciò produce errori nella sifting key condivisa tra Alice e Bob

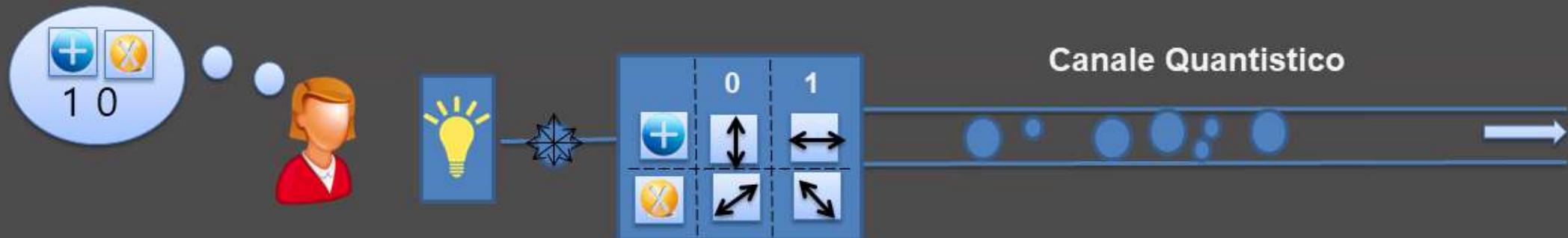


Quantum Key Distribution – Attacchi



Attacco di intercettazione-rinvio – Fase 1

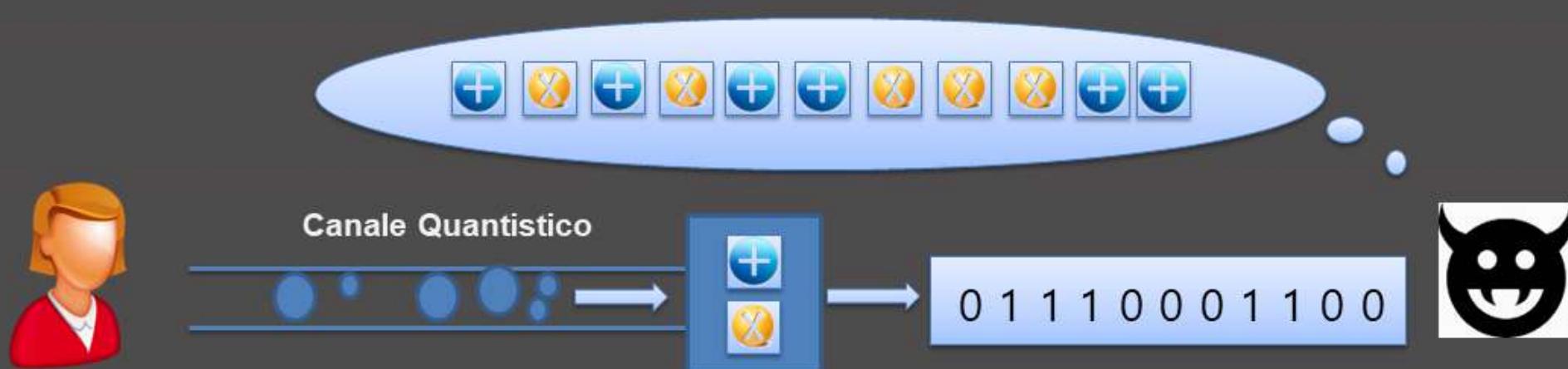
- Alice sceglie una stringa di bit e una sequenza di basi casuali con cui codificarla (rettilinea o diagonale)
- invia sul canale quantistico la corrispondente sequenza di fotoni polarizzati, ognuno rappresentante un bit della stringa nella base scelta in accordo allo schema definito





Attacco di intercettazione-rinvio – Fase 2

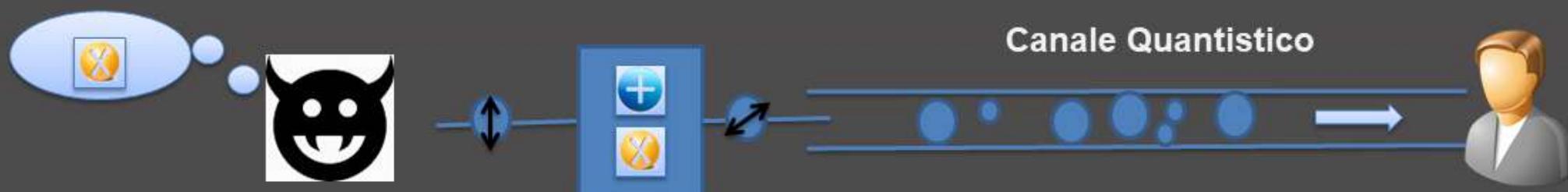
- Eve intercetta i fotoni, ma non sa quali basi ha usato Alice per generare le polarizzazioni
- Imposta casualmente le sue basi di intercettazione e misurare i fotoni





Attacco di intercettazione-rinvio – Fase 2

- Le basi di Eve verranno impostate correttamente solo metà delle volte
- Le impostazioni errate provocheranno letture di polarizzazione casuali e la distruzione della polarizzazione originale
- Di conseguenza, quando Eve invia nuovamente i fotoni che ha intercettato, il 50% di essi sarà sbagliato





Attacco di intercettazione-rinvio – Fase 3

- Bob imposta le sue basi casualmente
- Quando imposta una base uguale a Alice, ottiene solo un risultato corretto il 50% delle volte, poiché Eve ha cambiato le polarizzazioni dei fotoni che riceve nel 50% dei casi;
Questo sarà evidenziato nella fase successiva poiché il QBER sarà troppo alto

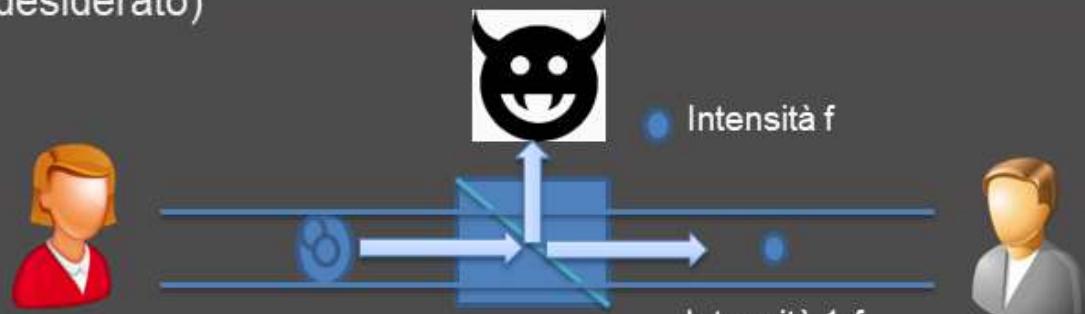


Quantum Key Distribution – Attacchi



Photon Number Split Attack

- ▶ In pratica molte implementazioni usano impulsi laser che contengono un numero molto piccolo di fotoni per impulso che sono distribuiti secondo una distribuzione di Poisson:
 - la maggior parte degli impulsi in realtà non contiene fotoni (non viene inviato alcun impulso)
 - alcuni impulsi contengono 1 fotone (che è desiderato)
 - alcuni impulsi contengono 2 o più fotoni.
- ▶ Se l'impulso contiene più di un fotone, allora Eve può scindere i fotoni extra, deviando a se una frazione f dell'intensità del raggio, e trasmettere il singolo fotone rimanente a Bob, d'intensità $1-f$
- ▶ Non introduce alcune errore, in quanto si attribuisce la riduzione dell'intensità dell'impulso a perdite del canale





Photon Number Split Attack

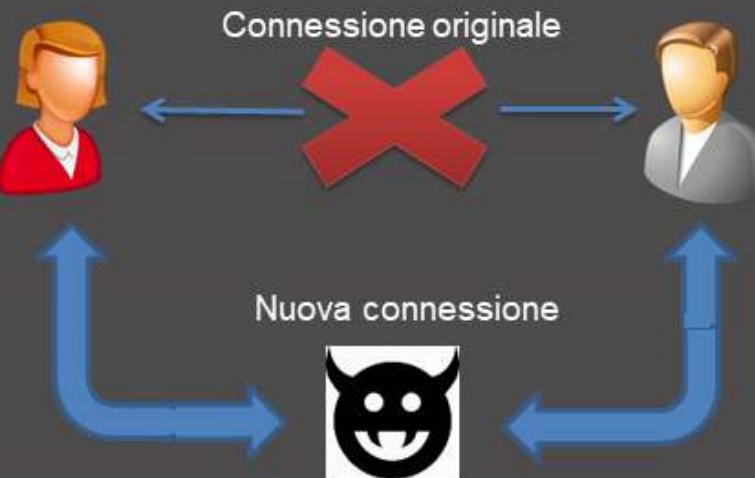
- Eve memorizza i fotoni extra in una memoria quantistica finché le corrette basi della codifica non sono state annunciate nella discussione pubblica tra Bob e Alice per misurarli correttamente
- ▶ Tale tecnica funziona soltanto in teoria in quanto non è possibile conservare fotoni per un più di una piccola frazione di secondo
- ▶ Tuttavia esistono varie soluzioni a tale attacco:
 - Alice invia a caso alcuni stati di esca per rilevare un attacco PNS
 - attendere un tempo sufficiente per far sì che gli impulsi si rovinino nel tempo e successivamente annunciare la basi
 - utilizzare impulsi molto deboli in modo da tale da non poter dividere il raggio in modo significativo

Quantum Key Distribution – Attacchi



Man-in-the-Middle

- ▶ La QKD è vulnerabile a un attacco man-in-the-middle quando usato senza autenticazione:
 - nessun principio noto della meccanica quantistica può distinguere una parte onesta da un attaccante
- ▶ Come nel caso classico, Alice e Bob non possono autenticarsi l'un l'altro e stabilire una connessione sicura senza informazioni condivise inizialmente per verificare l'identità:
 - se Alice e Bob hanno una chiave condivisa iniziale, possono utilizzare uno schema di autenticazione incondizionatamente sicuro (come il protocollo Carter-Wegman) insieme alla QKD per espandere esponenzialmente questa chiave, utilizzando una piccola quantità della nuova chiave per autenticare la prossima sessione

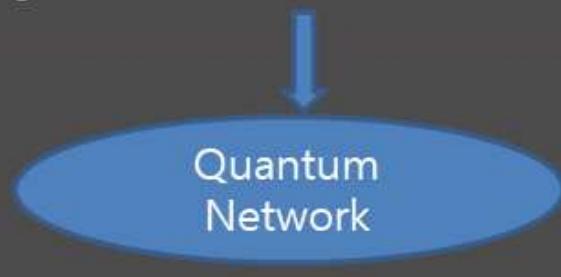


Quantum Key Distribution – Attacchi



Denial of Services

- ▶ Poiché attualmente una QKD richiede un mezzo (fibra ottica) tra i due punti, un attacco Dos (negazione del servizio) può essere montato semplicemente tagliando o bloccando a linea
- ▶ Occorre instradare la comunicazione tramite collegamenti alternativi in caso di interruzione



Quantum Key Distribution – Attacchi



Trojan –Horse Attack

- ▶ Una QKD può essere sondata da Eve inscenando un Trojan-horse attack:
 - Invia una luce brillante nel canale quantistico e analizza i riflessi posteriori



- ▶ E' stato dimostrato che Eve individua la scelta segreta della base di Bob con una probabilità superiore al 90%



Quantum Key Distribution

Limiti

Quantum Key Distribution – Limiti



Collegamenti Point-To-Point e DoS

- ▶ Il canale quantistico è una connessione point-to-point



- Limita la potenziale crescita, cioè connessione tra più parti
- Dà luogo alla possibilità di un attacco denial-of-service:
 - se Eve non può ottenere la chiave, potrebbe tagliare/alterare il collegamento fisico e dunque significherebbe che anche Alice e Bob non possono comunicare



Le sorgenti e rilevatori di fotoni

- ▶ La qualità delle sorgenti e dei rivelatori di fotoni può avere un impatto significativo sulla sicurezza
- ▶ I rivelatori hanno anche problemi pratici, per esempio:
 - l'attività in background non è correlata ai segnali QKD, noti come dark counts, in cui i fotoni vengono falsamente rilevati e devono essere eliminati dalla chiavi segrete
 - la presenza di un "tempo morto" tra la rilevazione di un fotone e la disponibilità dell'apparecchiatura a rilevare il prossimo, che può essere sfruttato da un aggressore
- ▶ Anche di fronte a un protocollo incondizionatamente sicuro, Eva può sempre attaccare l'attrezzatura:
 - Eve illumina l'apparato di Bob analizzando il suo backscattering (Trojan-Horse Attack)



Le perdite nel canale quantistico e distanza limitata

- ▶ Le proprietà quantistiche (come la polarizzazione) sono influenzate negativamente dalla distanza percorsa lungo un canale:
 - Canali quantistici in fibra ottica possono portare a una perdita irreversibile dello stato quantico per i fotoni inviati lungo il canale
 - Canali quantistici su spazio libero dipendono dall'atmosfera e dall'attrezzatura
- ▶ Poiché i segnali quantici non possono essere amplificati, alla fine le perdite sul canale saranno così alte che le letture ottenute dai rivelatori saranno indistinguibili dai dark count rates
- ▶ Sfortunatamente, è impossibile evitare canali lossy:
 - introducono carenze di sicurezza (esempio attacchi PNS)
 - limitano la trasmissione a lunga distanza di informazioni

Quantum Key Distribution – Limiti



Problemi di autenticazione classica

- ▶ Un canale classico fortemente autenticato deve essere usato tra Alice e Bob, per effettuare le classiche fasi di post-elaborazione e per prevenire un attacco man-in-the-middle
- ▶ La sicurezza del sistema QKD complessivo è ridotta a quella del classico algoritmo usato per autenticazione, che potrebbe essere solo computazionalmente sicuro piuttosto che incondizionatamente sicuro
 - L'uso degli algoritmi di Carter Wegman di autenticazione offrono comunque sicurezza incondizionata





Limiti della fisica quantistica

- ▶ Poiché la sicurezza della fase quantistica della QKD si basa interamente sulla teoria quantistica, come possiamo essere sicuri che la teoria quantistica sia corretta?
 - Una teoria non può mai essere dimostrata di per sé, ma non confutata
- ▶ La teoria quantistica è stata formulata per oltre un secolo e molti risultati sperimentali corrispondono alle sue previsioni
 - Tuttavia, potrebbe non essere abbastanza convincente

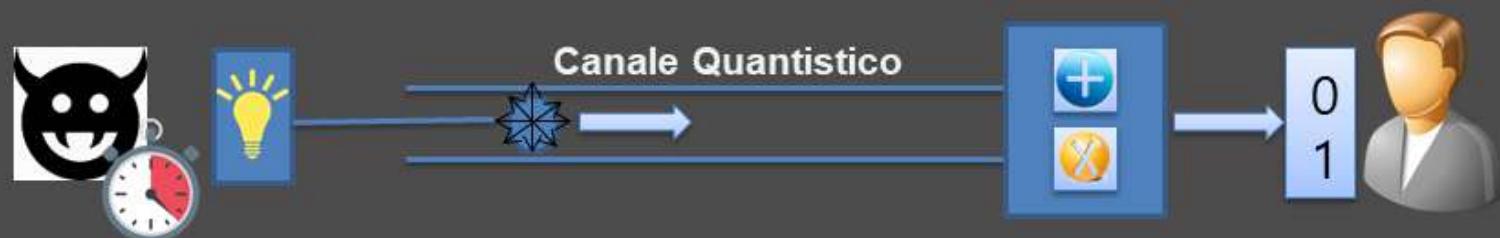


Quantum Key Distribution – Limiti



Side Channel Attacks

- ▶ Si verificano quando è possibile estrarre informazioni significative dal sistema indirettamente:
 - Inducendo dei guasti
 - Analisi delle caratteristiche fisiche di un sistema (tempo impiegato, potenza di calcolo, ecc...)

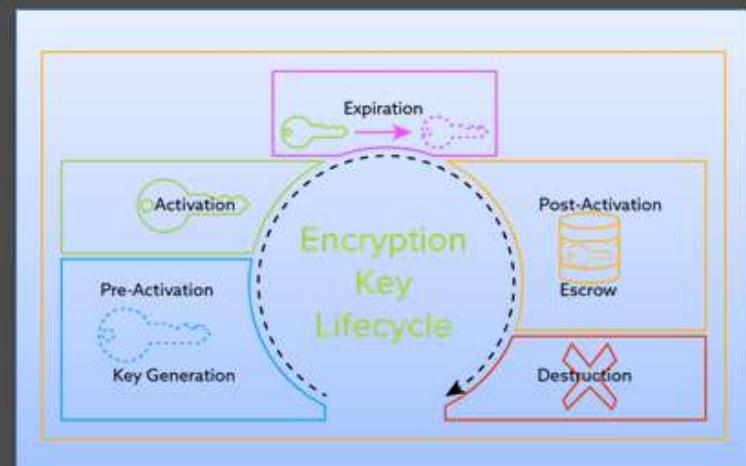


- ▶ La tecnologia QKD non ha avuto il beneficio di sostenere ricerca su questa tipologia di attacchi:
 - nella prima pratica dimostrazione del protocollo BB84 il modulo di Bob per rilevare i fotoni emetteva diverso il suono quando registra diverse polarizzazioni, a causa di un alimentatore rumoroso

Quantum Key Distribution – Limiti

Key Distribution Rate e la Gestione delle Chiavi

- ▶ Un fattore limitante nell'usabilità dei sistemi QKD è che:
 - La velocità con cui la raw key può essere inviata diminuisce in modo esponenziale rispetto alla lunghezza del canale quantistico
- ▶ Per essere efficace un sistema QKD deve essere in grado di:
 - fornire uno schema di gestione generale delle chiavi che tratti: la generazione, l'archiviazione, la manutenzione e la distruzione della chiave
 - fornire chiavi per l'autenticazione e chiavi per essere utilizzate in schemi OTP
 - garantire che durante il ciclo di vita a chiave rimanga sicura





Quantum Key Distribution

Applicazioni: Quantum Network



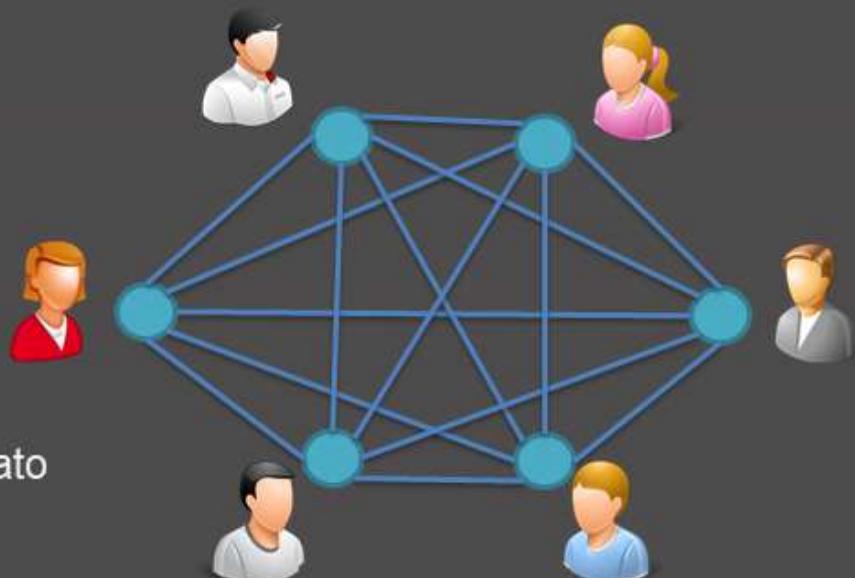
Problemi pratici

- ▶ La trasmissione quantica ha due problemi evidenti non affrontati dai protocolli, che ne limitano la praticità in un contesto più ampio:

1) La natura point-to-point

Per mettere in comunicazione più utenti N, ognuno di essi deve pre-condividere le chiavi simmetriche, quindi gli utenti N connessi tramite collegamenti point-to-point, richiedono la distribuzione di un numero di chiavi proporzionale a N^2

- Diventa impraticabile quando il numero di utenti è elevato



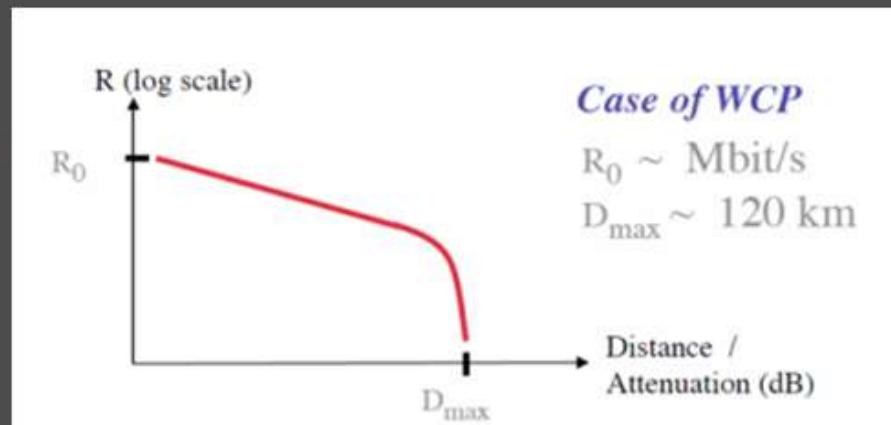


Problemi pratici

- ▶ La trasmissione quantica ha due problemi evidenti non affrontati dai protocolli, che ne limitano la praticità in un contesto più ampio:

2) Limitazione della distanza di un canale quantistico

- Ci sono dei limiti alla distanza che un segnale quantico può percorrere lungo un canale
- Una forte attenuazione del segnale viene osservata a una distanza critica, prima che il segnale scompaia a circa 120 km
- Molte ricerche sono state fatte nel tentativo di estendere questa distanza, ma è un fattore fortemente limitante intrinseco dei canali quantistici





Quantum Network

► La natura point-to-point dei collegamenti quantici potrebbe essere rimossa utilizzando una rete quantistica

- Deve includere una ridondanza sufficiente per far fronte al guasto in uno o più collegamenti e prolungare la distanza dei segnali quantici per poterli trasportare
- l'architettura di rete deve essere scelta in modo che ogni potenziale coppia di utenti della rete QKD possa scambiare la chiave con sicurezza incondizionata, senza che la rete diventi inutilizzabile
- il metodo per unire i singoli nodi deve essere compatibile con le proprietà dei segnali ottici quantici e non deve distruggere o alterare la chiave in modo che comprometta la sicurezza incondizionata della trasmissione

Quantum Network

Progettazione
Obiettivi



Tipi di Quantum Network

Reti di nodi quantici

- Richiede l'uso di fonti di entanglement quantistico, memorie quantistiche e tecniche di purificazione di entanglement
- I nodi sono ripetitori quantici: concatenano gli stati memorizzati ottenendo un perfetto entanglement end-to-end
- Estendono la distanza potenziale del segnale
- I ripetitori quantici esistono solo in teoria, non realizzabili con la tecnologia odierna

Reti di nodi ottici

- Utilizzano processi classici sul segnale quantico (scissione del fascio, multiplexing, de-multiplexing e commutazione)
- Rientra nelle capacità della tecnologia esistente
- Permette il funzionamento multiutente
- Non può essere utilizzata per estendere la distanza percorsa dal segnale quantico, a causa di perdite ottiche sul nodo

Reti di relay affidabili

- Un nodo relay è considerato attendibile per inoltrare il segnale quantico senza intercettarlo o alterarlo
- Le chiavi locali vengono generate tramite collegamenti QKD e archiviate in modo sicuro in nodi relay
- Quando due parti vogliono eseguire un protocollo QKD, viene creata una catena di relay affidabili con collegamenti quantici tra loro, formando un percorso QKD
- Fornisce una sicurezza incondizionata end-to-end a patto che tutti i nodi nel percorso QKD siano attendibili



Implementazioni pratiche di Quantum Network

- ▶ Tabella delle implementazioni QN realizzate e protocolli supportati

Quantum network	Start	BB84	BBM92	E91	DPS	COW
DARPA QKD network	2001	Yes	No	No	No	No
SECOCQ QKD network in Vienna	2003	Yes	Yes	No	No	Yes
Tokyo QKD network	2009	Yes	Yes	No	Yes	No
Hierarchical network in Wuho, China	2009	Yes	No	No	No	No
Geneva area network (SwissQuantum)	2010	Yes	No	No	No	Yes



Quantum Key Distribution

Owerview sul futuro

Quantum Key Distribution – Overview sul futuro



Necessità di utilizzo

- ▶ La questione se la QKD sia effettivamente necessaria ha diviso gli accademici della comunità crittografica in due:
 - chi sostiene che la QKD è una soluzione che non può avere un uso pratico in futuro
 - chi sostiene che la QKD è una soluzione più che valida, in quanto la crittografia odierna è condannata

Crittografia Moderna



Sicurezza Computazionale

VS

Crittografia Quantistica



Sicurezza Incondizionata

Quantum Key Distribution – Overview sul futuro

Necessità di utilizzo

Sicurezza Computazionale

- se un sistema di sicurezza fallisce si tratta di una cattiva gestione delle chiavi o sbagliata implementazione, piuttosto che la rottura di un algoritmo crittografico
- seppur ci sia una possibile minaccia di un computer quantistico pienamente operativo esistono soluzioni:
 - raddoppiando la lunghezza della chiave per annullare gli effetti dell'algoritmo di Grover
 - algoritmi basati su reticolo per annullare gli effetti dell'algoritmo di Shor

VS

Sicurezza incondizionata

- l'adozione della QKD sarebbe certamente auspicabile se:
 - gli attuali schemi di scambio di chiavi crittografiche non sono considerati sufficientemente sicuri
 - i progressi nelle tecniche matematiche, come la fattorizzazione di grandi numeri, minacciano la sicurezza degli algoritmi esistenti
 - un computer quantistico perfettamente funzionante è realizzabile
- potrebbe fornire un modo più economico e più veloce per raggiungere alti livelli di sicurezza, in un ambiente controllato e sicuro, con l'ulteriore vantaggio che la sicurezza può essere a prova di futuro



Quantum Key Distribution – Overview sul futuro

Necessità di utilizzo

- ▶ Delle domande da porsi sull'effettivo utilizzo della QKD sono:
 - La sicurezza incondizionata è un obiettivo aziendale sufficientemente grande da giustificare le spese di attrezzature e infrastrutture specializzate?
 - Quali vantaggi può portare in termini di sicurezza rispetto agli attuali protocolli di distribuzione delle chiavi crittografiche?
- ▶ L'aggiornamento dalla sicurezza computazionale a quella incondizionata, non aumenta necessariamente la protezione complessiva di un cripto-sistema «*La sicurezza è una catena: è forte quanto il suo anello più debole*»
- ▶ All'interno della comunità crittografica è che si è dato un taglio pessimistico sulla sicurezza odierna, come un tentativo di raccogliere fondi per la ricerca quantistica



Quantum Key Distribution – Overview sul futuro



Possibilità di Sviluppo

- ▶ Ci sono tre scelte aperte alla tecnologia embrionale della QKD:
 - La ricerca può continuare a sviluppare protocolli più sicuri e fornire più prove per raggiungere i più alti livelli di sicurezza, indipendentemente dalla loro praticità
 - Utilizzare il meglio tra le tecnologie e protocolli disponibili, cercare e trovare una nicchia competitiva e sfruttala
 - Abbandonare la tecnologia quantistica e concentrarsi sul miglioramento dei metodi crittografici classici pronti per il mondo dei computer post-quantico
- ▶ Ad oggi rinunciare alla QKD non è un'opzione finché il suo potenziale non è stato esplorato completamente. Entrambi i campi devono lavorare insieme per fornire soluzioni di sicurezza per il mondo dell'informatica pre e post quantistica



BB84 Simulator

[Descrizione del tool](#)

BB84 Simulator – Descrizione del tool



Cos'è BB84 Simulator

- ▶ E' un tool che permette di simulare i passi del protocollo BB84 e analizzare i risultati ottenuti a seguito della simulazione

Alice – Mittente

- ha il compito di generare casualmente la chiave iniziale, codificarla e inviare i fotoni a Bob
- successivamente effettuare delle operazioni sul canale classico per rilevare che non ci siano stati errori
- generare la chiave segreta

Bob – Ricevente

- ha il compito di misurare i fotoni ricevuti, ottenendo la propria chiave iniziale
- successivamente effettuare delle operazioni sul canale classico per rilevare che non ci siano stati errori
- generare la chiave segreta

Eve – Eveasdropper

- ha il compito di intercettare i fotoni inviati da Alice, con il fine di ottenere informazioni sulla chiave segreta, effettuandone la misurazione e inoltrarli a Bob (attacco intercettazione-rinvio)



Limitazioni

- ▶ Il tool non tiene in considerazione alcuni fattori:
 - Qualsiasi rilevamento di errore viene attribuito alla presenza di un intercettatore
 - Non sono simulate perdite di informazioni dovute al transito all'interno del canale quantistico
 - Non è fissato alcuna lunghezza del canale quantistico
 - Non sono state simulate tecniche di correzione degli errori e amplificazione della privacy

Modalità di utilizzo

1) Senza Eavesdropping

Alice e Bob riusciranno sempre a condividere una chiave segreta, in quanto non vi sarà alcun intervento da parte di Eve sul canale

2) Con Eavesdropping

Eve interviene nella comunicazione effettuano la misurazione dei fotoni in transito in base ad una probabilità, compromettendo la sicurezza della chiave segreta



Fasi di esecuzione

- ▶ Il tool prevede 8 fasi di esecuzione:
 - *Fase 0 – Inizializzazione*
 - *Fase 1 – Alice genera la chiave raw e le basi*
 - *Fase 2 – Alice invia i fotoni e Bob esegue la lettura*
 - *Fase 3 – Bob invia le sue basi ad Alice*
 - *Fase 4 – Alice invia le sue basi ad Bob*
 - *Fase 5 – Generazione della sifting key*
 - *Fase 6 – Alice invia i suoi bit di controllo a Bob*
 - *Fase 7 – Bob invia i suoi bit di controllo ad Alice*
 - *Fase 8 – Generazione della distillation key*
- ▶ A fine protocollo è possibile visualizzare le statistiche relative all'esecuzione del protocollo



Probabilità utilizzate

1) Probabilità Stimate

Vengono calcolate a priori, prima che il protocollo viene eseguito

Si considerano i seguenti fattori:

- la lunghezza della sifting key sia la metà della raw key
- il numero dei bit da controllare è calcolato sulla lunghezza della sifting key
- la percentuale impostata nella fase di inizializzazione
- si utilizza la probabilità di intervento di Eve in base al livello scelto nella fase di inizializzazione

2) Probabilità Effettive

Vengono calcolate a posteriori, dopo che il protocollo viene eseguito

Si considerano le reali misurazioni:

- la lunghezza della sifting key può essere variabile
- il numero dei bit da controllare è calcolato sulla lunghezza della sifting key
- la percentuale impostata nella fase di inizializzazione
- la probabilità di intervento di Eve è definita dal numero di intercettazioni che sono effettivamente avvenute



BB84 Simulator

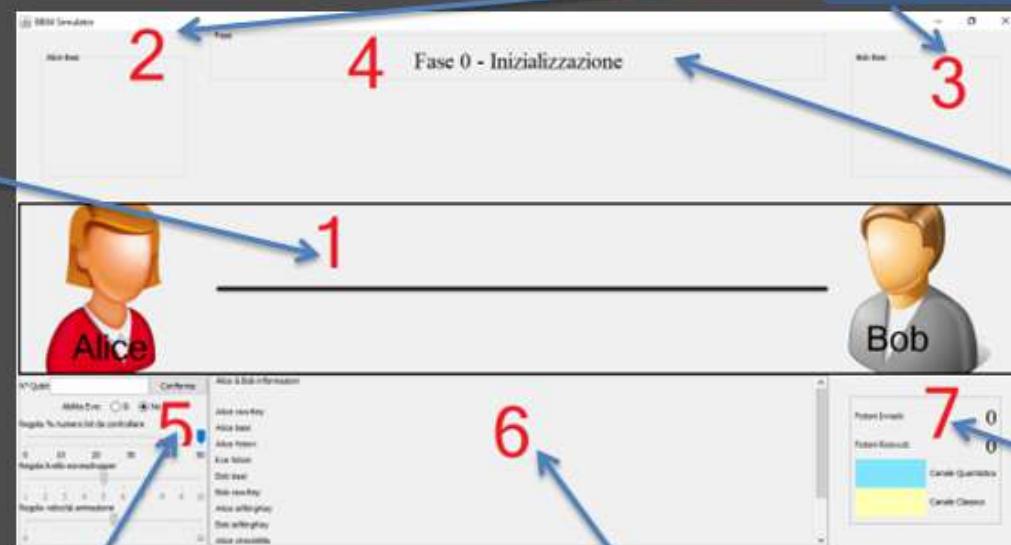
Esempio di esecuzione

BB84 Simulator – Esempio di esecuzione



Interfaccia Iniziale

canale di comunicazione quantistico/classico; agli estremi troviamo Alice e Bob



impostazioni dei parametri necessari per l'esecuzione

display che mostra le informazioni raccolte su Alice e Bob

scelte delle basi di Alice e Bob nelle varie fasi

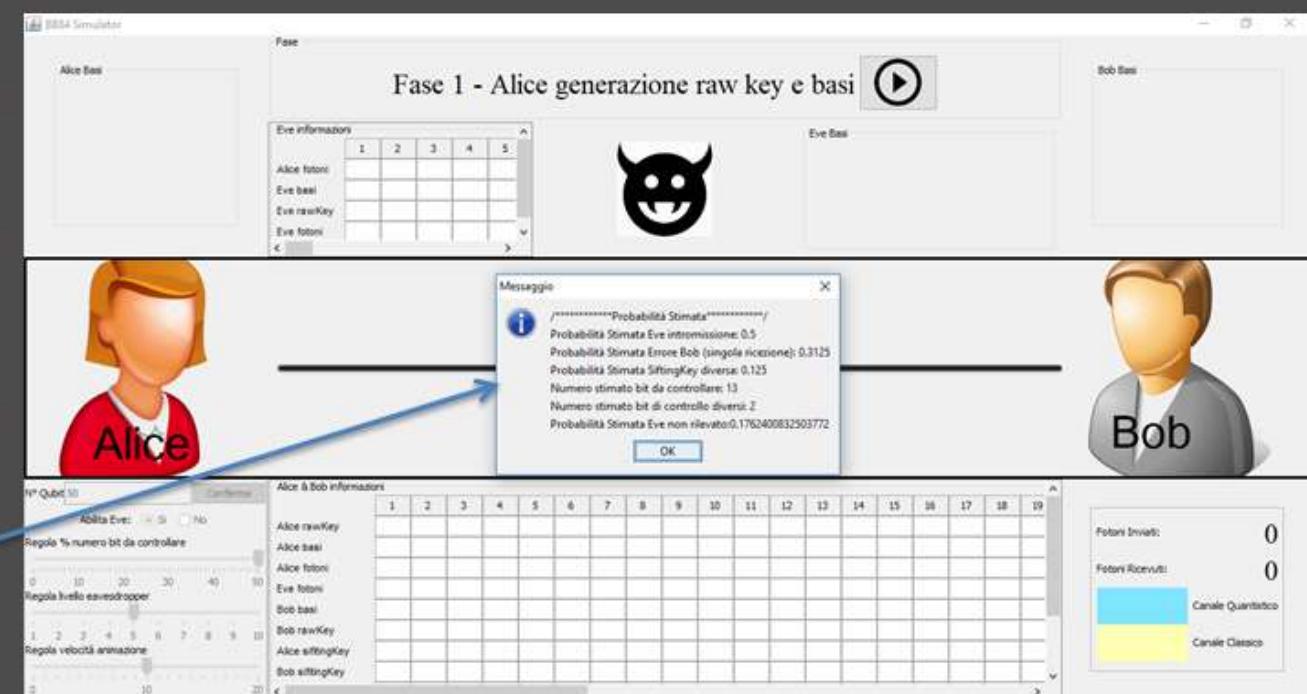
display della fase in esecuzione

contatori e legenda per indicare quando la comunicazione sta avvenendo sul canale quantistico o quello classico

BB84 Simulator – Esempio di esecuzione

Fase 0 – Inizializzazione

- ▶ Impostiamo i valori iniziale scegliendo:
 - il numero di qubit da inviare (50)
 - la percentuale dei bit da controllare (50% - default)
 - di abilitare Eve
 - il livello di Eve (5 - default)
- ▶ Una volta premuto il tasto conferma ci troviamo difronte un messaggio che riporta le varie probabilità stimate calcolate in base ai parametri inseriti



BB84 Simulator – Esempio di esecuzione



Fase 1 – Alice generazione row key e basi

- ▶ Vengono generate in maniera casuale:
 - la raw key di alice di lunghezza 50
 - le relative basi di polarizzazione da utilizzare per ciascun bit

BB84 Simulator – Esempio di esecuzione



Fase 2 – Alice invia i fotoni e Bob esegue la lettura

- ▶ L'animazione simula i fotoni inviati da Alice lungo il canale quantistico e quando giungono a Bob ne effettua la misurazione, andando ad aggiornare la tabella man mano che li riceve
- ▶ Eve può intercettare i fotoni, per cui la simulazione mostra due casi:

1) Eve non interviene

Il fotone transita regolarmente da Alice a Bob senza essere intercettato





Fase 2 – Alice invia i fotoni e Bob esegue la lettura

2) Eve interviene

- Il fotone viene intercettato da Eve e quando effettua la misurazione (occhio) il fotone viene ripolarizzato secondo la base scelta:

Eve e Alice stessa base

Siccome la base scelta da Eve risulta essere la stessa di Alice, il fotone viene intercattato da Eve e misurato correttamente ottenendo lo stesso bit di Alice; inoltre viene inoltrato sul canale a Bob mantenendo la polarizzazione originaria del fotone



Eve e Alice diversa base

Siccome la base scelta da Eve risulta essere diversa da quella di Alice, il fotone viene intercettato da Eve e misurato, ottenendo lo stesso bit di Alice con probabilità 1/2; inoltre viene inoltrato sul canale a Bob cambiando la polarizzazione originaria del fotone



BB84 Simulator – Esempio di esecuzione



Fase 3 – Bob invia le sue basi ad Alice

- L'animazione simula l'invio delle basi utilizzate da Bob lungo il canale classico e quando giungono ad Alice ne effettua il controllo con le proprie, andando ad aggiornare la tabella mano che le riceve:
 - background rosso: non coincidono
 - background verde: coincidono

Fase 3 - Bob invia le sue basi ad Alice

Alice Base

Bob Base

Eve informazioni

1	2	3	4	5
Alice fotoni	/			
Eve basi	D			
Eve rawKey	0			
Eve fotoni	/			

Eve Base

Fase 3 - Bob invia le sue basi ad Alice

Alice

Bob

Nº Qubit (0)

Abilita Eve: No

Regola % numero bit da controllare:

Regola livello eavesdropper:

Regola velocità animazione:

Alice & Bob informazioni

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Alice rawKey	R	I	I	O	I	O	O	I	I	O	O	I	O	O	O	I	O	O
Alice basi	G	G	G	G	G	G	G	G	G	G	G	G	G	R	R	R	R	R
Alice fotoni	-	\	\	/	-	I	I	\	/	I	-	/	I	/	I	\	/	/
Eve fotoni	-				-			-			-			-				
Bob basi	R	O	R	R	D	D	D	R	O	D	D	R	D	R	R	R	O	R
Bob rawKey	I	I	I	I	I	I	I	I	I	O	O	O	I	O	O	I	O	O
Alice siftinKey																		
Bob siftinKey																		

Base Inviate: 15
Base Ricevute: 14

Canale Quantistico
Canale Classico

BB84 Simulator – Esempi di esecuzione



Fase 4 – Alice invia le sue basi a Bob

- ▶ La simulazione è del tutto analoga alla fase precedente soltanto che questa volta è Alice ad inviare le basi a Bob che ne effettuerà il controllo

Fase 4 - Alice Invia le sue basi a Bob

Alice Basi

Eve informazioni

	1	2	3	4	5
Alice fotoni			/		
Eve basi			0		
Eve rawKey			0		
Eve fotoni			/		

Eve Basi

Bob Basi

Alice

Bob

N° Qubit: 50

Abilità Eve: Sì No

Regola % numero bit da controllare

Regola livello eavesdropper

Regola velocità animazione

Alice & Bob informazioni

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Alice rawKey	1	1	1	0	1	0	0	1	1	1	0	0	1	0	0	0	0	1	0
Alice basi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Alice fotoni	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Eve fotoni																			
Bob basi	0	0	0	0	R	D	D	D	R	D	R	D	R	R	R	D	R	R	R
Bob rawKey	1	1	1	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
Alice sittingKey																			
Bob sittingKey																			

Basi Inviate: 4

Basi Ricevute: 3

Canale Quantistico

Canale Classico



Fase 5 – Generazione della sifting key

- Vengono scartati (background grigio) i bit rispettivamente dalla raw key di Alice e Bob per i quali le basi utilizzate da entrambe le parti nel processo di polarizzazione/misurazione non coincidono andando a riempire una nuova riga nella tabella che rappresenta la sifting key generata rispettivamente da Alice e Bob

Alice & Bob informazioni																			
Alice rawKey	1	1	1	0	1	0	0	1	1	1	0	0	1	0	0	0	0	1	0
Alice basi	R	D	D	D	R	R	R	D	R	D	R	R	D	R	D	R	D	D	D
Alice fotoni	-	\	\	/	-	I	I	\	/	I	-	/	I	/	I	\	\	/	/
Eve fotoni											/	I		I	/	I	/		
Bob basi	R	D	R	R	D	D	R	D	R	D	R	R	D	R	R	D	D	D	D
Bob rawKey	1	1	1	1	1	1	1	1	1	0	0	0	1	0	0	1	0	0	0
Alice siftingKey	1	1								0		1	0	0		0	1		
Bob siftingKey	1	1								0		1	0	0		0	0		

Le sifting key generate non è detto che coincidono in quanto c'è la presenza di Eve in gioco

BB84 Simulator – Esempio di esecuzione



- ▶ L'animazione simula l'invio dei bit di controllo estratti dalla sifting key di Alice (Bob) lungo il canale classico a Bob (Alice)
 - ▶ La tabella viene aggiornata man mano che Alice (Bob) invia il bit, prendendo i bit che si trovano in posizione dispari della sifting key
 - ▶ Il numero di bit da controllare dipende dalla percentuale impostata nella fase di inizializzazione, nel nostro caso 50% cioè metà dei bit della sifting key

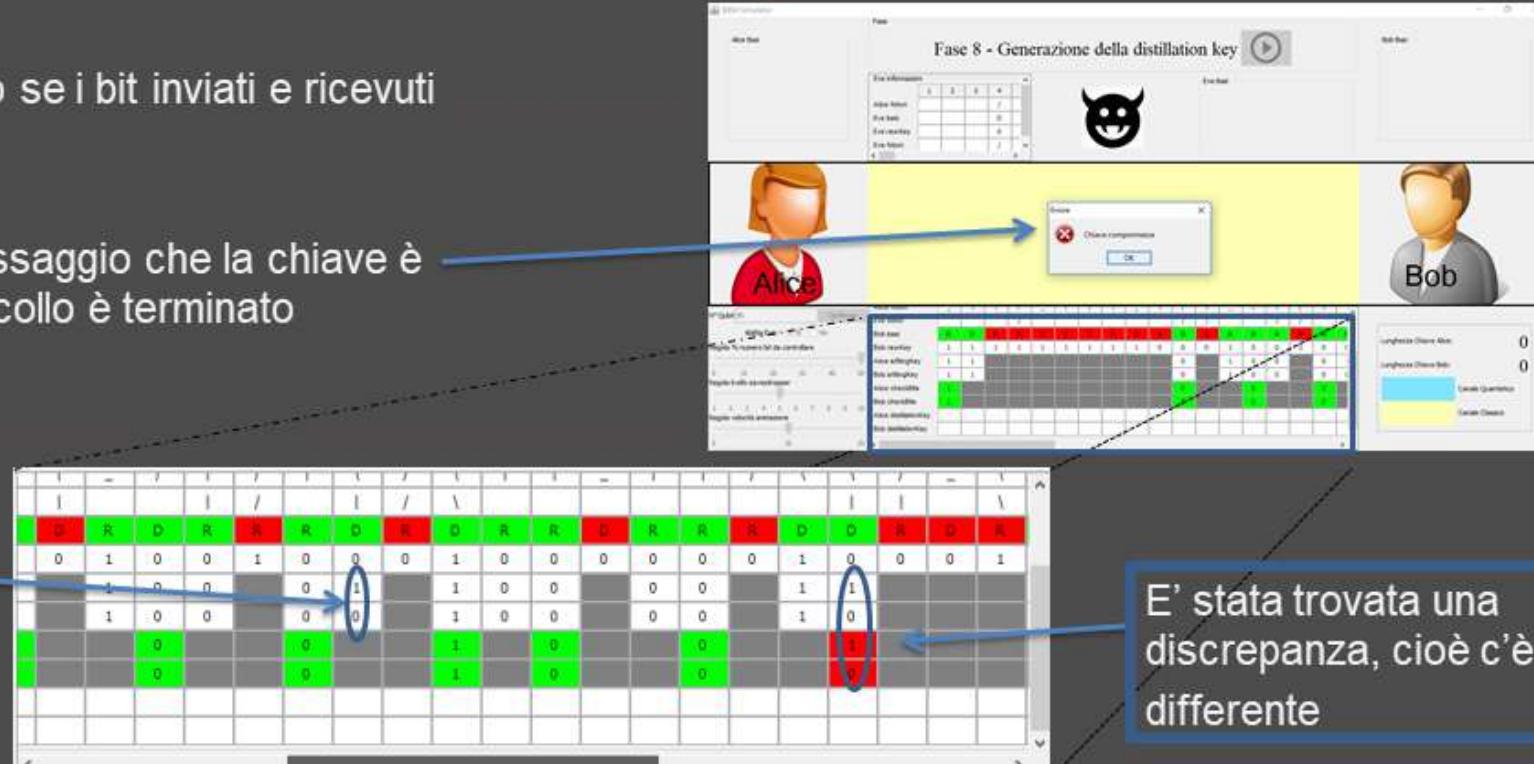
BB84 Simulator – Esempio di esecuzione



Fase 8 – Generazione della distillation key

- ▶ Alice e Bob controllano se i bit inviati e ricevuti coincidono
 - ▶ Viene mostrato un messaggio che la chiave è compromessa, il protocollo è terminato

Altri bit erano differenti della sifting key, soltanto che non sono stati estratti come bit di controllo essendo di posizione pari



E' stata trovata una discrepanza, cioè c'è un bit differente

BB84 Simulator – Esempio di esecuzione

Analisi

- ▶ A fine esecuzione del protocollo, cliccando sul bottone "mostra info" ci viene mostrato un messaggio contenente:

- **Informazioni generali:**

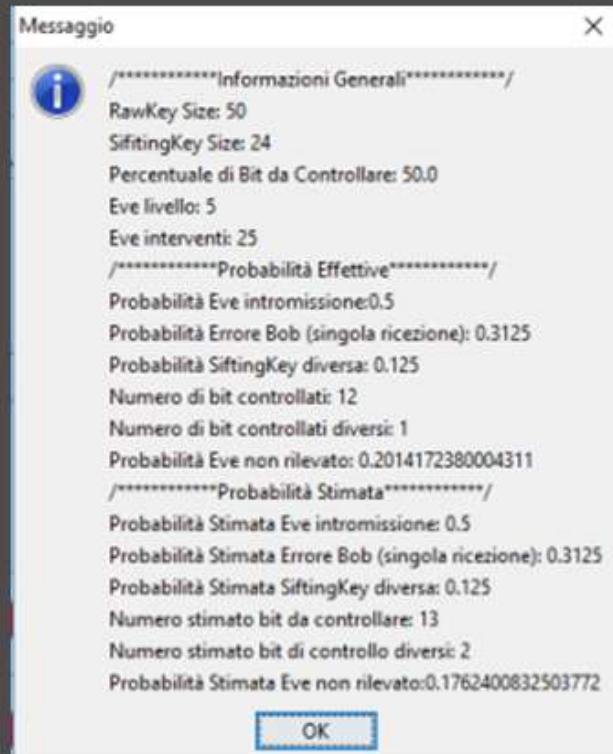
- **Informazioni generali:**
le varie lunghezze delle chiavi e i settaggi utilizzati

- **Le probabilità effettive:**

- **Le probabilità effettive:**
ovvero le probabilità calcolate a posteriori, dopo l'esecuzione del protocollo

- **Le probabilità stimate:**

- **Le probabilità stimate:**
ovvero le probabilità calcolate a priori, prima dell'esecuzione del protocollo





Conclusioni Finali

- ▶ Al momento la QKD è un campo di ricerca aperto:
 - ci sono molti limiti pratici e costi elevati da sostenere per poterla mettere in pratica su vasta scala
- ▶ Se le prestazioni della QKD vengono ulteriormente migliorate e i costi vengono ridotti, allora potenziali reti QKD potrebbe diventare un'infrastruttura essenziale per assicurare la generazione di chiavi per una vasta gamma di obiettivi di crittografia
 - potrebbe essere lo stimolo principale per perseguire il miglioramento della tecnologia QKD e la ricerca di Quantum Network
- ▶ Il tool BB84 Simulator permette di avere una visione pratica dell'esecuzione del protocollo BB84;
Dei possibili sviluppi futuri del tool possono essere:
 - simulare perdite di informazioni all'interno del canale quantistico
 - simulare tecniche di correzione degli errori e amplificazione della privacy