

UNIVERSITÀ DEGLI STUDI DI SALERNO



LAUREA MAGISTRALE IN SICUREZZA INFORMATICA
CORSO DI SICUREZZA DEI DATI

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

Anno Accademico 2017/2018

Indice

Overview.....	6
1 Introduzione alla crittografia quantistica e QKD	8
1.1 Storia della crittografia: dalla classica alla moderna.....	9
1.1.1 La crittografia classica	9
1.1.2 La crittografia medievale.....	10
1.1.3 La crittografia dal 1800 alla II Guerra Mondiale	10
1.1.4 La crittografia moderna	11
1.2 I limiti della crittografia moderna	13
1.2.1 L'avvento del computer quantistico	13
1.2.2 Il problema dello scambio della chiave	13
1.2.3 Uno schema perfettamente sicuro: il One-Time Pad.....	14
1.2.4 Il problema dell' evesdropping	16
1.3 La crittografia quantistica e QKD come soluzione.....	16
1.4 Obiettivi dell'attività progettuale	17
1.5 Outline	18
2 QKD - Il Contesto e i Protocolli	19
2.1 I principi fisici	19
2.1.1 La teoria quantistica	19
2.1.2 La sovrapposizione quantistica	20
2.1.3 Il principio di indeterminazione di Heisenberg.....	21
2.1.4 Il Quantum Entanglement	21
2.1.5 Il teorema di Bell.....	21
2.1.6 Il teorema di no-cloning quantistico	22
2.1.7 Il canale quantistico	22
2.1.8 La polarizzazione del fotone.....	23
2.2 QKD - I protocolli	26
2.2.1 Lo scenario di base	26
2.2.2 Il meccanismo generale del QKD	27

2.2.3	Il Quantum Key Exchange	30
2.2.4	Il protocollo BB84.....	32
2.2.5	Il protocollo di Ekert	36
3	QKD - Gli Attacchi, la Sicurezza e le Limitazioni	39
3.1	La quantum security.....	39
3.1.1	Considerazioni sull'Eavesdropping.....	39
3.1.2	La sicurezza incondizionata.....	40
3.2	Gli attacchi e le strategie difensive	41
3.2.1	Attacco di intercettazione-rinvio	41
3.2.2	Photon Number Split Attack.....	42
3.2.3	Man in the Middle (MITM)	43
3.2.4	Denial of Services (Dos)	43
3.2.5	Trojan-Horse Attacks	44
3.3	Le limitazioni della QKD	44
3.3.1	I collegamenti Point-to-Point e DoS	44
3.3.2	Le sorgenti e i rilevatori di fotoni	44
3.3.3	Le perdite nel canale quantistico e distanza limitata	45
3.3.4	Problemi di Autenticazione classica	46
3.3.5	Limiti della fisica quantistica	46
3.3.6	Side Channel Attacks	46
3.3.7	La gestione delle chiavi e Key Distribution Rate	47
4	QKD - Un Applicazione: Quantum Netwok	48
4.1	La Quantum Network	49
4.1.1	I tipi di Quantum Network	49
4.2	Implementazioni pratiche di Quantum Network	52
5	Il Futuro del QKD.....	55
5.1	La necessità e l'utilizzo del QKD	55
5.1.1	Quando utilizzare la QKD.....	56
5.1.2	Le possibilità di sviluppo della QKD.....	56
5.2	La ricerca nei protocolli e QN	57

6	Uno strumento per la simulazione del protocollo BB84.....	59
6.1	Descrizione del tool: BB84 Simulator	59
6.1.1	Le modalità di utilizzo e le fasi di esecuzione	60
6.1.2	Le probabilità utilizzate per effettuare analisi.....	63
6.2	La struttura del progetto e classi principali	66
6.2.1	Le tecnologie utilizzate e struttura del progetto	66
6.2.1	Overview sulle classi principali.....	66
6.3	Esempi di scenari principali e analisi.....	74
6.3.1	Scenario 1 - Scambio senza eavesdropping.....	76
6.3.2	Scenario 2 - Scambio con eavesdropping livello 5	83
6.3.3	Scenario 3 - Scambio con eavesdropping livello 1	91
	Conclusioni	94
	Bibliografia.....	95

Overview

La crittografia si occupa dello studio delle tecniche matematiche, per proteggere l'informazione digitale, i sistemi di elaborazione e le computazioni distribuite, da attacchi avversari. La sua nascita ha motivi principalmente militari fino a diventare una necessità comune per l'intero mondo: inizia con metodi di cifratura che utilizzavano "carta e penna" per poi arrivare all'implementazione di algoritmi di cifratura su computer.

I calcolatori tradizionali hanno delle limitazioni dovute alle leggi della fisica classica e una possibile realizzazione di un computer quantistico comprometterebbe l'intera sicurezza della crittografia moderna rendendola vulnerabile. Al giorno d'oggi sono stati realizzati dei prototipi di computer quantistici e la possibilità di impiegarlo sta diventando un'ipotesi concreta. Un altro problema legato alla crittografia moderna è come condividere delle chiavi di grande taglia in modo completatamente segreto: nel corso del tempo sono stati pubblicati vari protocolli che però non possono garantire una sicurezza incondizionata, a causa dell'impossibilità di individuare un infiltrato che ascolta passivamente l'esecuzione del protocollo.

L'avvento della crittografia quantistica risolve definitivamente questi aspetti: essa utilizza le leggi della meccanica quantistica per creare nuove primitive crittografiche, di cui la maggior parte sono ancora teoriche, poiché si basano su tecniche di elaborazione che non sono possibili con la tecnologia odierna.

Tuttavia, una primitiva, Quantum Key Distribution (QKD) , è realizzabile oggi e può fornire comunicazioni incondizionatamente sicure. Nonostante questo, la QKD ha riscontrato pareri contrastanti all'interno della comunità crittografica e non è stata ancora ampiamente adottata.

L'attività progettuale del seguente elaborato ha il fine di mettere in mostra la realizzazione software di uno strumento che effettua la simulazione del protocollo della QKD: BB84 Simulator.

Il tool permette di effettuare delle simulazioni e analizzare vari scenari possibili, in maniera molto semplice e intuitiva grazie all'utilizzo di un'interfaccia grafica animata.

Gli obiettivi del seguente documento sono:

- Fornire delle conoscenze di base della meccanica e crittografia quantistica.
- Descrivere e analizzare la QKD, i relativi protocolli, gli attacchi possibili e la sicurezza fornita.
- Esibire una breve panoramica dell'applicazione della QKD: Quantum Network.
- Mostrate le limitazioni, il futuro, i vantaggi e l'effettiva utilità della QKD ad oggi.
- Simulare e analizzare scenari di esecuzione del protocollo BB84 tramite il tool realizzato Simulator BB84.

La struttura del documento è organizzata come segue:

- Il primo capitolo descrivere brevemente la storia della crittografia, analizza quali sono i limiti della crittografia moderna e introduce al mondo della crittografia quantistica e QKD come soluzione a tali problemi.
- Il secondo capitolo analizza la QKD mostrandone i principi fisici della meccanica quantistica su cui si basa, il funzionamento dei principali protocolli,
- Il terzo capitolo si occupa degli attacchi possibili, la sicurezza fornita e i limiti della QKD.
- Il quarto capitolo si focalizza sull'applicazione della QKD, ovvero le Quantum Networks descrivendone: cos'è, i tipi e le implementazione pratiche.
- Il quinto capitolo fornisce il quadro conclusivo sull'effettivo utilizzo e necessità della QKD, il suo futuro e campi di ricerca.
- Il sesto capitolo è dedicato alla realizzazione del simulatore del protocollo BB84: verrà descritto definendone le modalità di utilizzo, le probabilità, un'overview sulle classi principali implementate ed esempi di scenari possibili.

1 Introduzione alla crittografia quantistica e QKD

La necessità di nascondere messaggi strategici da occhi indiscreti ha richiesto, fin dall'antichità, lo sviluppo di tecniche crittografiche per garantire segretezza dell'informazione, autenticità delle parti e integrità dei dati.

Dare una definizione di cos'è e di cosa si occupa la crittografia è estremamente complesso. Possiamo descriverla come: lo studio delle tecniche matematiche, per proteggere l'informazione digitale, i sistemi di elaborazione e le computazioni distribuite, da attacchi avversari.

La sua nascita ha motivi principalmente militari con l'intento di nascondere informazioni strategiche al nemico. Oggi, la capacità di garantire la segretezza delle comunicazioni militari o diplomatiche è vitale come sempre, ma la crittografia sta diventando sempre più importante nella vita di tutti i giorni. Con la crescita delle reti informatiche per le transazioni commerciali e la comunicazione di informazioni confidenziali vi è una crescente necessità di crittografia per garantire che queste informazioni non possono essere acquisite da terzi.

I due obiettivi principali della crittografia sono per un mittente e un intento destinatario di poter comunicare in un formato incomprensibile a terzi, e l'autenticazione dei messaggi per dimostrare che non sono stati modificati in transito. Entrambi questi obiettivi possono essere raggiunti con sicurezza dimostrabile se il mittente e il destinatario sono in possesso di una chiave condivisa e segreta, una sequenza di numeri casuali.

Uno dei principali problemi di crittografia è quindi il cosiddetto "problema di distribuzione delle chiavi", cioè come stabilire una chiave segreta tra il mittente e il destinatario ed essere sicuri che terze parti (intercettazioni) non possano acquisire neanche parzialmente informazioni a riguardo. È impossibile stabilire una chiave segreta con comunicazioni convenzionali, per cui la distribuzione delle chiavi si è basata sulla creazione di un canale fisicamente sicuro, per esempio i così detti corrieri di fiducia, o la sicurezza condizionata da problemi matematici "difficili" nella crittografia a chiave pubblica.

In questo capitolo verranno definiti proprio questi limiti della crittografia moderna e come l'avvento della crittografia quantistica possa risolvere tali problemi, la quale ha portato alla definizione di protocolli che utilizzano i principi della meccanica quantistica, per permettere lo scambio in modo sicuro di una chiave (Quantum Key Distribution). Per completezza verrà riportata nel primo paragrafo, brevemente, la storia della crittografia.

1.1 Storia della crittografia: dalla classica alla moderna

Ad oggi la crittografia moderna utilizza tecniche matematiche fornendo delle prove di sicurezza. Tale risultato è frutto di molte evoluzioni nel corso dei secoli delle varie tecniche e scoperte, ma l'obiettivo di fondo non è mai cambiato: nascondere il messaggio agli occhi di un attaccante.

La controparte della crittografia è la crittoanalisi, vale a dire "lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione".

Da sempre, durante il corso della storia, crittografia e crittoanalisi si sono dati battaglia per prevalere l'una sull'altra.

1.1.1 La crittografia classica

La storia della crittografia inizia con la crittografia classica con metodi di cifratura che utilizzavano carta e penna o al massimo semplice supporti meccanici, definendo i così detta cifrari a sostituzione monoalfabetica: dal testo in chiaro si effettua una semplice permutazione delle lettere ottenendo il testo cifrato. Tra i principali metodi ricordiamo:

- Il cifrario di atbash definito dagli ebrei;
- la scitala: un particolare sistema di comunicazione dei messaggi segreti degli spartani;
- il cifrario di Cesare definito dai romani;

Il problema principale della crittografia classica era l'assenza delle nozioni di cosa significasse schema sicuro. Il passaggio dalla crittografia classica a quale moderna avviene in quanto gli schemi di crittografia classica erano progettati ad hoc (valutati basandosi sulla chiarezza e ingegnosità del disegno) ed erano ritenuti sicuri se il designer non trovava degli attacchi validi, mentre gli schemi di crittografia sono ideati fornendo la definizione formale e matematica e una prova di sicurezza in un modello ben definito.

1.1.2 La crittografia medievale

Tuttavia è semplice violare cifrari a sostituzione monoalfabetica, tant'è vero che Al-Kindi intorno al IX secolo ci riuscì sviluppando la tecnica dell'analisi delle frequenze.

Per rafforzare la sicurezza nascono i primi cifrari "moderni": vengono definiti come cifrari polialfabetici che si differenziano dai monoalfabetici in quanto un dato carattere del testo in chiaro non viene cifrato sempre con lo stesso carattere, ma con caratteri diversi in base ad una qualche regola, in genere legata ad una parola segreta da concordare.

Tra i più importanti:

- il disco cfrante di Leon Battista Alberti, che poi venne migliorato da Giovan Battista Bellaso;
- il cifrario di Vigenère che prende il nome dal francese Vigenère, che si basa sul disco di Bellaso.

Quest'ultimo è stato considerato indecifrabile per molto tempo, finché nel 1863 Friedrich Kasiski non pubblicò un metodo per "forzarlo", chiamato Esame Kasiski.

1.1.3 La crittografia dal 1800 alla II Guerra Mondiale

Durante il XIX secolo e agli inizi del XX la crittografia aveva assunto un ruolo primario in ambito militare e diplomatico: molti crittologi lavorano a nuovi schemi di cifratura e analisi crittografiche.

Degli elementi che resero più interessante il bisogno di crittografia furono:

- l'introduzione delle comunicazioni radio: siccome chiunque poteva ascoltare una frequenza radio, c'era la necessità di rendere incomprensibili i messaggi.
- l'invenzione di dispositivi elettromeccanici, come ad esempio la macchina Enigma a rotori, elevò a più sofisticati ed efficienti livelli la cifratura;
- la successiva introduzione dell'elettronica e dei computer ha permesso l'utilizzo di schemi di cifratura sempre più complessi, molti dei quali non ottenibili con carta e penna.

Un concetto importante per quanto riguarda la sicurezza fu formulata da Kerckhoffs: "La sicurezza di un crittosistema non deve dipendere dal tener celato il crittoalgoritmo. La sicurezza dipenderà solo dal tener celata la chiave."

I principali sistemi di cifratura furono :

- il cifrario di Vernam (One-Time Pad) ideato da Gilbert Vernam nel 1918, il quale perfezionò il metodo di Vigenère proponendo l'idea di usare chiavi segrete casuali lunghe almeno quanto il messaggio;
- la macchina Enigma a rotorì;
- la macchina di Lorenz, che codificava i messaggi usando un sistema binario basato sul cifrario Vernam.

Un importante svolta nella crittografia ma anche nell'informatica in generale lo diede il team Ultra che mise a punto i Colossus, 1943, macchine che oggi vengono ricordate come i primi computer programmabili della storia. Il progetto si deve a Max Newman e Tommy Flowers, che ebbero l'idea di usare i circuiti elettronici al posto degli elementi meccanici per rendere il calcolo più veloce.

1.1.4 **La crittografia moderna**

La nascita della crittografia moderna è da registrare nel 1946 quando Claude Shannon grazie ai suoi lavori e agli studi sulla teoria dell'informazione (di cui viene considerato il padre), che includevano i risultati dei suoi lavori eseguiti durante il conflitto mondiale, costituirono una base teorica molto solida per la crittografia ed anche per molta della crittanalisi. Un importante risultato fu la dimostrazione che il che il cifrario di Vernam è l'unico metodo crittografico possibile che sia perfettamente sicuro.

Solo a partire dagli anni 1970 la crittografia ha iniziato ad essere di pubblico dominio, in cui si diede vita alla crittografia a chiave simmetrica in cui la stessa chiave è usata sia dal mittente che dal destinatario del messaggio, la quale deve essere tenuta da entrambi segreta.

Visto l'impiego dei computer nell'ambito crittografico il termine cifrato viene soppiantato dal termine algoritmo di cifratura. Nascono di versi standard di cifratura come:

- il DES (Data Encryption System): un cifrario a blocchi che utilizza la rete di Feistel per cifrare un blocco del testo in chiaro;

- l'AES (Advanced Encryption Standard): anche esso un cifrario a blocchi che utilizza una rete a sostituzione e permutazione; sostituì il DES in quanto insicuro a causa della piccola taglia della chiave e della lunghezza di blocco, oltre che alle possibili backdoor progettuali.

Con gli algoritmi di cifratura a chiave privata, la chiave condivisa deve necessariamente essere scambiata fra le parti comunicanti in qualche maniera sicura come ad esempio un corriere fidato, un contatto faccia-a-faccia, o altro. Ciò è un problema non banale da risolvere: diventa ingestibile all'aumentare del numero dei partecipanti nello scambio, l'impossibilità di definire canali sicuri oppure quando le chiavi vengono cambiate frequentemente.

La risposta a questo problema arriva nel 1976 con il lavoro di Whitfield Diffie e Martin E. Hellman, definendo il concetto di chiave pubblica: ogni comunicante utilizza una coppia di chiavi correlate matematicamente: una chiave privata, per decifrare i cfrati ricevuti, che deve rimanere segreta, ed una chiave pubblica, utilizzata dai mittenti per cifrare i messaggi, la quale può essere liberamente distribuita senza alcuna necessità di utilizzare un canale sicuro. Fino a che la chiave privata resta segreta, la chiave pubblica può essere distribuita a tutti e per un tempo indefinito senza compromettere la sicurezza del sistema, potendo riutilizzare la stessa coppia praticamente all'infinito.

Furono i matematici Ron Rivest, Adi Shamir e Leonard Adleman a capire come mettere in pratica questa idea, e a loro si deve il nome RSA. Si affidarono alla fattorizzazione dei numeri primi: moltiplicare tra loro dei numeri primi molto grandi è semplice, ma risalire agli stessi numeri primi partendo dal risultato richiede un tempo esponenziale.

L'avvento della crittografia a chiave pubblica, tuttavia, non ha eliminato la crittografia a chiave simmetrica in quanto quest'ultima ha notevoli vantaggi in termini di prestazioni (molti protocolli crittografici odierni utilizzano schemi ibridi).

Gli algoritmi a chiave pubblica (o asimmetrici) basano la propria sicurezza su una classe di problemi matematici, funzioni one-way, che richiedono una piccola potenza elaborativa per essere eseguiti ma, per contro, una grande potenza di calcolo per poterli invertire, ovviamente quando l'inversione è possibile. Ad oggi questi problemi risultano essere irrisolvibile con la tecnologia a disposizione, tuttavia alcuni progressi futuri nell'analisi matematica potrebbero rendere i sistemi basati su di essi insicuri.

1.2 I limiti della crittografia moderna

Come intuito nel paragrafo precedente la sicurezza fornita dalla crittografia moderna sembra essere inviolabile con le risorse attuali. Se consideriamo, però, attaccanti con potenza di calcolo illimitata allora molti cripto-sistemi risulterebbero insicuri e facilmente vulnerabili: un tale scenario è auspicabile? Esistono schemi perfettamente sicuri? Si possono realizzare?

Nel seguente paragrafo verranno definite le principali limitazioni della crittografia moderna, introducendo la crittografia quantistica come soluzione a tali problemi.

1.2.1 L'avvento del computer quantistico

La crittografia tramite l'utilizzo di problemi matematici difficili da risolvere, cioè con alta complessità risolutiva, riesce a proteggere le informazioni da eventuali attacchi. Un esempio sono i problemi appartenenti alla classe NP Completo: per risolverli, cioè trovare una soluzione, richiede tempo e potenza di calcolo adeguate. Questi due fattori sono complementari tra loro: aumentato la potenza di calcolo, diminuisce il tempo e viceversa. Teoricamente, se disponessimo di potenza di calcolo illimitata romperemmo qualsiasi algoritmo di cifratura in un tempo irrisorio rispetto alle risorse attuali.

Nel 1982 Richard Feynman, fisico americano, 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). Successivamente il fisico inglese David Deutsch, ne dimostrò la validità.

I calcolatori tradizionali hanno delle limitazioni dovute alle leggi della fisica classica e una possibile realizzazione di un computer quantistico comprometterebbe l'intera sicurezza della crittografia moderna rendendola vulnerabile. Al giorno d'oggi sono stati realizzati dei prototipi di computer quantistici e la possibilità di impiegarlo sta diventando un'ipotesi concreta.

1.2.2 Il problema dello scambio della chiave

Un'altra limitazione della crittografia moderna è il problema dello scambio della chiave, ovvero al modo in cui due parti (Alice e Bob), vogliono condividere una chiave segreta sicura.

Per mettere in comunicazioni più utenti, 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 . Chiaramente questo diventa impraticabile quando il numero di utenti è elevato, per cui è necessaria una strategia alternativa.

Una soluzione a tale problema possono essere un Key Distribution Center, se il numero di utenti del sistema non è elevato, oppure, soluzione effettivamente utilizzata, l'utilizzo di protocolli che permettono di scambiare la chiave in maniera sicura tra due parti utilizzando i principi della crittografia a chiave pubblica (il più importante lo scambio Diffie-Hellman).

In realtà, il problema della sicurezza riguardante la segretezza della comunicazione non è del tutto risolto con questo tipo di crittografia, in quanto:

- la sicurezza si basa sulla difficoltà di recuperare la chiave privata dalla chiave pubblica, ovvero sull'utilizzo di problemi supposti essere difficili, per cui, come spiegato nel paragrafo precedente con il progredire della tecnologia potrebbe essere un fattore limitante;
- passibile 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; una soluzione resta sempre il contatto fisico tra i due interlocutori, i quali, scambiandosi le chiavi pubbliche hanno una reciproca autenticazione oppure l'utilizzo di una autorità certificata.

1.2.3 **Uno schema perfettamente sicuro: il One-Time Pad**

Molti protocolli e schemi di cifratura/autenticazione per essere provati sicuri si basano su assunzioni, per le quali non esistono prove matematiche, di problemi che sono supposti essere difficili cioè non possono essere risolti in tempo polinomiale, cioè la complessità computazionale e temporale sono limitate dalle risorse di calcolo disponibili attualmente, oppure sulla sicurezza di primitive crittografiche.

Tuttavia esiste uno schema crittografico che è stato provato sicuro utilizzando una dimostrazione matematica che lo rende assolutamente inattaccabili dal punto di vista teorico: il cifrario di Vernam (denominato anche one-time pad). C. Shannon ha dimostrato che i cifrari di Vernam sono inattaccabili alla crittoanalisi ed inoltre esiste un unico sistema crittografico perfettamente sicuro e questo è il cifrario di Vernam.

Ci sono vari motivi che lo rendono un cifrario perfetto:

- **casualità dei caratteri che compongono la chiave**

Infatti, chi non possiede la chiave e volesse decifrare il messaggio potrebbe, in linea di principio, tentare con ogni possibile chiave (attacco di forza bruta). Questa operazione ha una enorme complessità computazionale, in quanto il numero di chiavi cresce come un fattoriale al crescere della lunghezza del messaggio. Tuttavia non è solo questo il motivo per cui il cifrario è inattaccabile, infatti con un possibile futuro avvento dei computer quantistici problemi di calcolo di questo tipo potrebbero non essere più rilevanti.

- **ogni cfrato può corrispondere ad un messaggio equiprobabilmente**

A causa dell'arbitrarietà della chiave, si otterrebbero, nel fare la suddetta analisi, tutti i possibili testi in chiaro. Inoltre, per la casualità della chiave, tutti questi testi in chiaro sarebbero ugualmente probabili e dunque sarebbe impossibile optare per l'uno o l'altro di questi.

La realizzazione di un sistema crittografico perfetto sicuro mettere fine alla battaglia teorica tra crittografia e crittoanalisi, in quanto risulta essere inattaccabile.

Tuttavia restano però aperti molti problemi pratici per realizzarlo, infatti i punti deboli sono:

- **La chiave non può essere riutilizzata**

Se si riutilizza la chiave per effettuare un'altra cifratura, allora un attaccante potrebbe osservare la correlazione tra i cfrati osservati per ottenere correlazione con i relativi messaggi in chiaro.

- **Il problema della generazione della chiave**

Per farsi che la comunicazione sia sicure bisogna che la chiave: deve essere opportunamente lunghe per consentire lo scambio di messaggi sufficientemente articolati; devono essere casuali e, visto che non possono essere riutilizzate, occorre produrne tante per aver modo di comunicare frequentemente. La generazione di numeri causali non è un problema banale dal punto di vista dell'informatica.

- **Il problema dello scambio della chiave**

Per utilizzare tale schema di cifratura, occorre aver preventivamente inviato la chiave attraverso un canale che deve essere assolutamente sicuro. Tuttavia, la chiave ha la stessa lunghezza del messaggio che dobbiamo inviare per cui è un metodo molto dispendioso.

In definitiva il cifrario di Vernam resta teoricamente perfettamente sicuro ma molto difficilmente utilizzabili in pratica. Tuttavia resta il fatto che, se si riuscisse a risolvere queste limitazioni si potrebbero tranquillamente e in tutta sicurezza utilizzarlo.

1.2.4 Il problema dell' evesdropping

Un altro punto debole è il seguente: in un canale di comunicazione classico un intercettatore, eveasdropper, che ha accesso ad esso, può osservare le informazioni in transito e memorizzarle. Ciò significa che limitandosi ad osservare il canale, in maniera passiva, l'eavesdropping è sempre ammissibile e non rilevabile.

1.3 La crittografia quantistica e QKD come soluzione

La soluzione a tutti i problemi esposti nel paragrafo precedente possono essere risolti con l'utilizzo di un nuovo approccio al mondo della crittografia: la crittografia quantistica, definita come “la scienza che sfrutta le proprietà della meccanica quantistica per eseguire attività crittografiche”.

La sua nascita è dovuta proprio al problema venutosi a creare con l'avvento del computer quantistico, dove si cercò di trovare una soluzione che sfruttasse la natura stessa della comunicazione e si ipotizzò un approccio fisico più che matematico, basandosi proprio sui principi della meccanica quantistica.

Come osservato nel sottoparagrafo 1.2.4. un ascoltatore passivo può sempre inserirsi su un canale classico di comunicazione senza che ne venga rilevata la presenza. Tuttavia la crittografia quantistica si pone come obiettivo di impedire qualsiasi tipo di intercettazione, per cui viene realizzato allo scopo un canale di comunicazione quantistico sul quale non è possibile effettuare un'osservazione senza essere scoperti fornendo la così detta sicurezza incondizionata.

La crittografia quantistica ha realizzato nuove primitive crittografiche, di cui la maggior parte sono ancora teoriche, poiché si basano su tecniche di elaborazione che non sono possibili con la tecnologia odierna. Ciò nonostante,

una primitiva, Quantum Key Distribution (QKD) , è realizzabile oggi e può fornire comunicazioni incondizionatamente sicure.

La distribuzione a chiave quantistica (Quantum key Distribution) è “un meccanismo che utilizza tale canale quantistico per risolvere il problema dello scambio della chiave in maniera sicura tra le parti per evitare che questa possa essere intercettata da un attaccante senza che le due parti in gioco se ne accorgano”.

Con tale meccanismo si riesce a produrre chiavi casuali sufficientemente lunghe che possono essere spedite in maniera sicuro, rendendo possibile utilizzare i cifrari di Vernam per cifrare messaggi in maniera tale che nessuna spia possa decifrarli.

L'enorme rivoluzione introdotta da questa tecnica sembra mettere la parola fine alla battaglia tra crittografia e crittoanalisi, nonostante questo, la QKD ha riscontrato pareri contrastanti all'interno della comunità crittografica e non è stata ancora ampiamente adottata in quanto ci sono grosse limitazioni pratiche dovute proprio alla teoria della meccanica quantistica essendo ancora un campo tutto da scoprire.

1.4 Obiettivi dell'attività progettuale

L'attività progettuale del seguente elaborato ha il fine di mettere in mostra la realizzazione software di uno strumento che effettua la simulazione del protocollo della QKD: BB84 Simulator.

Il tool permette di effettuare delle simulazioni e analizzare vari scenari possibili, in maniera molto semplice e intuitiva grazie all'utilizzo di un'interfaccia grafica animata.

Gli obiettivi del seguente documento sono:

- Fornire delle conoscenze di base della meccanica e crittografia quantistica.
- Descrivere e analizzare la QKD, i relativi protocolli, gli attacchi possibili e la sicurezza fornita.
- Esibire una breve panoramica dell'applicazione della QKD: Quantum Network.
- Mostrate le limitazioni, il futuro, i vantaggi e l'effettiva utilità della QKD ad oggi.

- Simulare e analizzare scenari di esecuzione del protocollo BB84 tramite il tool realizzato Simulator BB84.

1.5 Outline

La struttura del documento è organizzata come segue:

- Il secondo capitolo analizza la QKD mostrandone i principi fisici della meccanica quantistica su cui si basa, il funzionamento dei principali protocolli,
- Il terzo capitolo si occupa degli attacchi possibili, la sicurezza fornita e i limiti della QKD.
- Il quarto capitolo si focalizza sull'applicazione della QKD, ovvero le Quantum Networks descrivendone: cos'è, i tipi e le implementazione pratiche.
- Il quinto capitolo fornisce il quadro conclusivo sull'effettivo utilizzo e necessità della QKD, il suo futuro e campi di ricerca.
- Il sesto capitolo è dedicato alla realizzazione del simulatore del protocollo BB84: verrà descritto definendone le modalità di utilizzo, le probabilità, un'overview sulle classi principali implementate ed esempi di scenari possibili.

2 QKD - Il Contesto e i Protocolli

La Quantum Key Distribution (QKD) “è una delle principali applicazioni della meccanica quantistica alle telecomunicazioni e all’informatica”.

Lo scopo della QKD è che permette, mediante l’utilizzo di un canale quantistico, di scambiare una chiave casuale di lunghezza arbitraria in completa sicurezza tra due parti che vogliono poter comunicare, con la certezza che ogni tentativo di intercettazione verrebbe rilevato.

In questo capitolo verranno definiti i principali principi fisici delle meccanica quantistica su cui la QKD si basa, il funzionamento di base e i principali protocolli.

2.1 I principi fisici

La meccanica quantistica “è la teoria fisica che descrive il comportamento della materia, della radiazione e le reciproche interazioni, nel mondo microscopico.”

E’ conosciuta per essere spesso contraria al modo di pensare comune, in quanto alcuni dei postulati su cui si basa possono risultare non intuitivi. Viste da un punto di vista quantistico, molte delle nostre certezze diventano invece incertezze e azioni che consideriamo possibili, impossibili.

Alcuni di questi postulati, che ad una prima analisi possono apparire delle limitazioni, sono risultati invece utili nel tempo a sviluppare dei sistemi di sicurezza che si basino proprio su queste incertezze e/o impossibilità.

2.1.1 La teoria quantistica

Nel 1900 uno studente di fisica Max Planck scoprì che le radiazioni emesse da un corpo caldo non sono emesse in modo continuo ma in pacchetti, ovvero in quanti. Precedentemente a tale scoperta si pensava che le radiazioni fossero un fenomeno costante e frazionabile a piacere.

In sostanza “l’energia non è solamente un’onda che si propaga in modo continuo e in tutte le direzioni (emanazione continua), l’energia viene emanata a proiettili, ovvero in quanti predefiniti dello stesso valore (emanazione discreta). La costante di Planck esprime il valore fisso e non frazionabile in cui

l'energia di una radiazione è divisa. L'onda della radiazione si esprime in frequenza, maggiore è la frequenza maggiore è l'energia racchiusa in un quanto. L'energia, in sostanza, cambia in quantità, ma per essere emessa viene racchiusa sempre nel medesimo quanto, della stessa dimensione."

2.1.2 La sovrapposizione quantistica

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, ma non la sua posizione reale. In sostanza la sovrapposizione quantistica afferma che un quanto può avere molti possibili stati, 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. Questa proprietà è solitamente illustrata dall'esperimento il "Gatto di Schrodinger", come mostrato in figura 2.1..

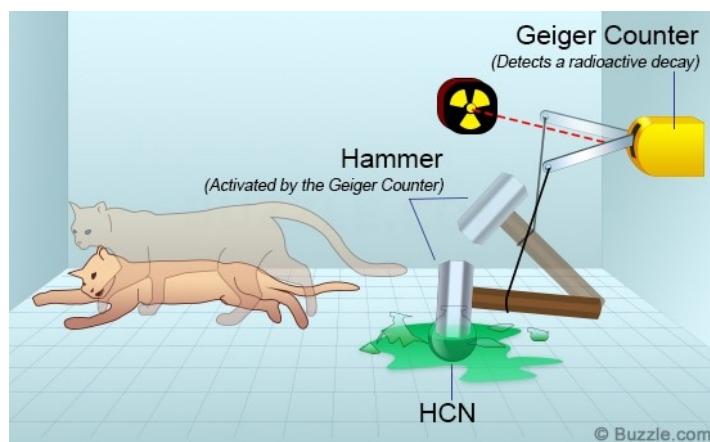


Figura 2.1 - Illustrazione dell'esperimento "il Gatto di Schrodinger"

Un gatto (quanto) è chiuso in una scatola con una fiala di cianuro che può essere rotta da un meccanismo casuale (per esempio può essere innescato da una particella emessa da una fonte radioattiva), che avrà conseguenze prevedibilmente spaventose per lo sfortunato felino se viene attivato. Inoltre non è possibile stabilire se il cianuro sia stato rilasciato fino all'apertura della scatola.

Una interpretazione classica di questo esperimento è che il gatto è vivo o morto nella scatola indipendentemente da quando è aperto. Tuttavia, l'interpretazione quantistica afferma che il gatto è sia vivo che morto allo stesso tempo, ed è solo l'atto di aprire la scatola, cioè la misurazione, che collassa la funzione d'onda

del gatto. Quindi, è proprio l'atto di osservazione che distrugge la funzione d'onda e determina lo stato finale del sistema in uno dei suoi stati possibili.

2.1.3 Il principio di indeterminazione di Heisenberg

Lo stato di una particella di un sistema atomico viene caratterizzato utilizzando due parametri: velocità e posizione. Werner Heisenberg nel 1927 postulò invece, che a un certo valore queste quantità rimangono sempre indefinite (Principio di Indeterminazione di Heisenberg).

Formalmente afferma "che vi sono coppie di proprietà osservabili di un sistema fisico microscopico, dette coniugate, come la posizione e la velocità, o l'energia e il tempo, che non si possono entrambe determinare o misurare allo stesso tempo."

Questa limitazione non è dovuta dalle scarse capacità dei sistemi di misurazione, ma è un evidente impossibilità dovuta alla misurazione di una delle proprietà coniugate che altera l'altra.

2.1.4 Il Quantum Entanglement

Una strana proprietà quantica di rilevanza per il QKD è quella del fenomeno dell'entanglement quantistico: si possono produrre coppie di quanti che si comportano come se fossero una singola entità, le cosiddette coppie EPR.

Per esempio, i quanti possiedono una proprietà chiamata "spin": un quantum potrebbe avere spin up o 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 causa 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. Questo è noto come il paradosso EPR, che non è stato risolto fino al 1965 da John Bell.

Si è ipotizzato che questo strano comportamento quantistico potesse essere usato nel teletrasporto.

2.1.5 Il teorema di Bell

Bell ha studiato le proprietà di un sistema entangled nel caso di "localizzazione ristretta", cioè ciò che accade a una particella dipende solo dagli eventi nella sua posizione e una particella diversa dovrebbe essere influenzata solo da eventi nella sua, diversa, posizione. Ha dimostrato che in questo caso ci sono effetti

misurabili che la fisica quantistica viola quando sono soddisfatte determinate condizioni: disuguaglianze di Bell.

I risultati sperimentali hanno dimostrato che la "localizzazione ristretta" non era corretta e che gli entanglement quantistici si mantengono anche quando le due particelle componenti sono separate fisicamente.

2.1.6 Il teorema di no-cloning quantistico

Il teorema di no-cloning quantistico afferma che "non è possibile duplicare (cloning) esattamente uno stato quantistico sconosciuto a priori".

È un altro meccanismo di "protezione" per la teoria quantistica, in quanto la copia di stati quantici sconosciuti consentirebbe a un osservatore di misurare esattamente le copie ed evitare le restrizioni del Principio di incertezza di Heisenberg. Quindi, copie degli stati quantici non possono essere effettuate da un intercettatore ed inviarle lungo il canale quantistico. Ne deriva che un segnale quantico non può essere amplificato lungo un canale quantico.

2.1.7 Il canale quantistico

Gli stati quantici possono essere utilizzati per trasmettere informazioni tra due parti autorizzate, convenzionalmente chiamati Alice e Bob. Teoricamente, non farà alcuna differenza se atomi, ioni, molecole, elettroni o qualsiasi altra particella quantizzata sono coinvolti nel scambio.

Da una prospettiva pratica, tuttavia, è il quanto di luce, il fotone, che è l'opzione preferita, perché gli stati quantici del fotone possono essere trasmessi su lunghe distanze senza decoerenza rispetto agli altri candidati quantistici.

Ci sono perdite dovute alla dispersione che non incidono sulla sicurezza complessiva di un protocollo QKD, ma a condizione che siano contabilizzate e gestite in modo efficace.

Il canale quantistico è composto da:

- Un dispositivo ottico di emissione capace di produrre fotoni polarizzati;
- Un canale quantistico: mezzo che permetta alla luce di propagarsi (fibra ottica o spazio libero), cioè trasportare i fotoni;
- un dispositivo che permetta all'utente destinatario di misurare la polarizzazione dei fotoni.

2.1.8 La polarizzazione del 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.

Ora come abbiamo visto l'energia di un quanto (fotone) dipende dalla frequenza dell'onda dalla quale viene generato e visto che la luce è una parte dello spettro di tutte le onde elettromagnetiche il quanto che essa trasporta avrà un'energia limitata.

I fotoni hanno un proprio angolo di polarizzazione, formato dal piano in cui essi oscillano con l'asse di propagazione. Tale angolo ha un valore compreso tra 0° e 180° .

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.

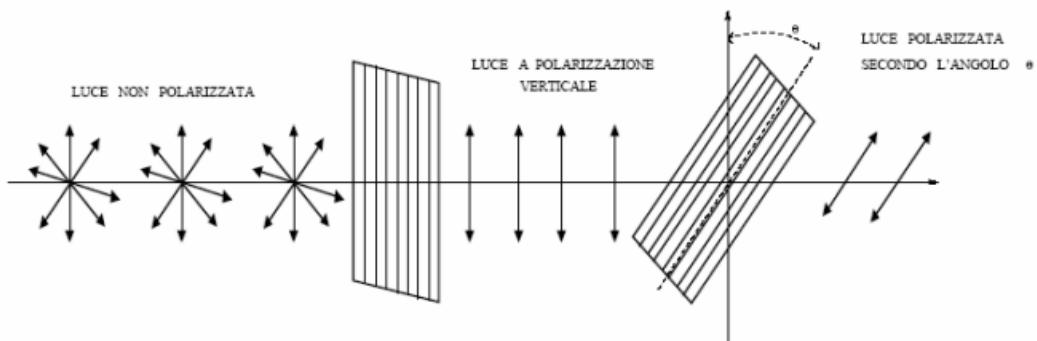


Figura 2.2 - Illustrazione di come avviene la polarizzazione

Gli stati di polarizzazione ortogonali sono indicati come una base di polarizzazione. Due basi sono coniugate se la misurazione della polarizzazione di una randomizza l'altra, e quindi sono soggette al principio di incertezza di Heisenberg: la misura influenza il valore dell'altro, quindi non è possibile conoscere entrambi i valori contemporaneamente. Ad esempio, i filtri impostati su 0° o 90° formano una base, e la sua base coniugata ha filtri impostati a 45° e 135° .

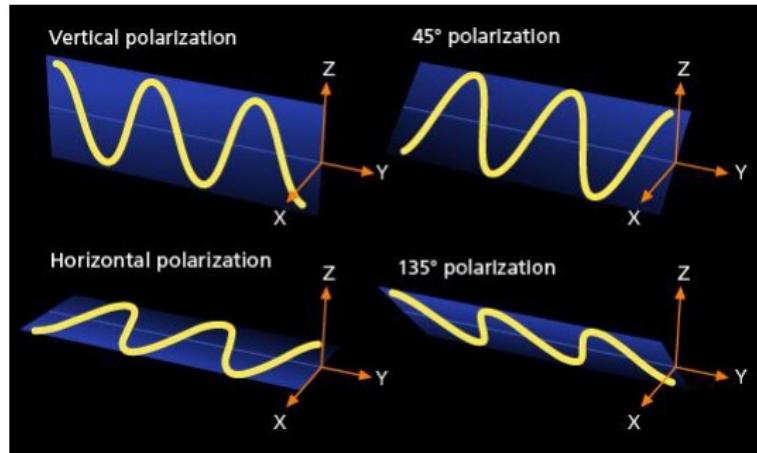


Figura 2.3 - illustrazione dei fotoni polarizzati secondo vari angoli

Si utilizza la notazione di Dirac per descrivere uno stato quantico, per esempio:
 $| \uparrow \rangle$ che sta ad indicare una polarizzazione a 90° .

Definiremo la base rettilinea con tale notazione $\oplus = (| \uparrow \rangle, | \leftrightarrow \rangle)$; mentre la base diagonale $\otimes = (| \nearrow \rangle, | \searrow \rangle)$.

Per misurare la polarizzazione del fotone l'utente destinatario si dota di un dispositivo, per esempio un cristallo di calcite.

Supponiamo che tale dispositivo misura i fotoni con angolo di polarizzazione 0° e 90° . A questo punto il cristallo di calcite permette di inoltrare i fotoni in arrivo in due modi:

- Se il fotone è già polarizzato secondo le direzioni possibili del cristallo, cioè può essere traslato lungo l'asse stesso oppure attraversarlo verticalmente ed emergere perpendicolarmente rispetto all'asse ottico, lo attraversa senza alterarne la polarizzazione.

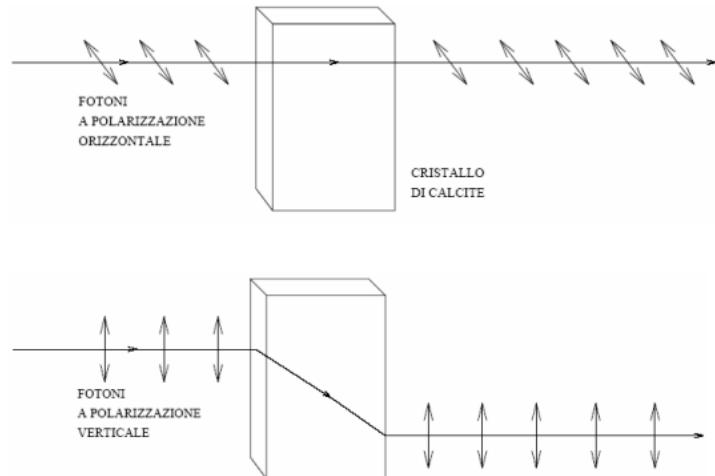


Figura 2.4 - illustrazione della misurazione con base rettilinea di fotoni rettilinei

- Se il fotone ha una polarizzazione intermedia, cioè 45° e 135° si ha un comportamento casuale: il fotone segue con la stessa probabilità l'uno o l'altro cammino, alterandone la polarizzazione del fotone originaria.

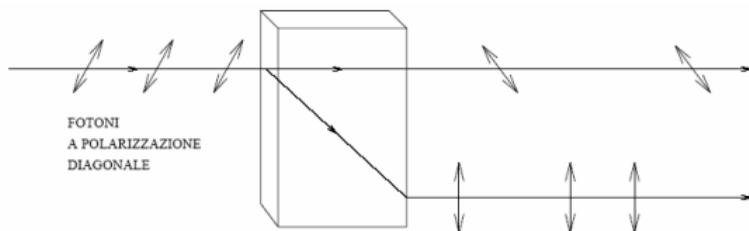


Figura 2.5 - illustrazione della misurazione con base rettilinea di un fotone diagonale

Nella seguente tabella sono riportate le varie probabilità con cui un fotone, con angolo di polarizzazione 0° , 90° , 45° e 135° , attraversi i vari filtri di polarizzazione.

	0° -filter	90° -filter	45° -filter	135° -filter
$0^\circ \leftrightarrow$	1	0	$\frac{1}{2}$	$\frac{1}{2}$
$90^\circ \uparrow$	0	1	$\frac{1}{2}$	$\frac{1}{2}$
$45^\circ \nearrow$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
$135^\circ \nwarrow$	$\frac{1}{2}$	$\frac{1}{2}$	0	1

Figura 2.6 - Tabella contenente le probabilità con cui un fotone attraversi i vari filtri di polarizzazione

La polarizzazione del fotone trasmesso sarà determinata dal valore del bit da rappresentare (0,1) e dalla base di conversione utilizzata. La codifica di un bit mediante un fotone polarizzato rappresenta un “qubit” (quantum bit).

2.2 QKD - I protocolli

Dopo aver visto i principi della meccanica quantistica il focus in questo paragrafo si sposta a come sfruttarli in ambito crittografico.

Utilizzando una primitiva della crittografia quantistica, ovvero la Quantum Key Distribution (QKD), possiamo costruire comunicazioni sicure tra due parti. Per farlo bisogna stabilire delle procedure che ci permettono di rilevare la presenza di eventuali intercettatori, costruire il canale quantistico e codificare le informazioni su di esso, ovvero si definiscono dei protocolli.

2.2.1 Lo scenario di base

L'obiettivo dei protocolli di Key Distribution è permettere a due parti, indicate per tradizione come 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. Questa condivisione avviene tramite un sistema fisico e l'informazione viene codificata negli stati che possono descriverlo.

- **Parti in gioco**

Alice e Bob, hanno due ruoli ben distinti e caratterizzati: il ruolo di Alice è di creazione e codifica della chiave, generando una sequenza casuale di simboli e, rispettando delle regole prestabilite, preparare degli stati da inviare a Bob; Il compito di Bob è decodificare il segnale di Alice. Alla fine del protocollo in seguito ad operazioni di post-processing Alice e Bob condividono una chiave segreta.

Il compito di Eve è quello di intercettare le informazioni che Alice e Bob si scambiano, in modo tale da comprometterne la sicurezza dello scambio della chiave.

- **Canali di comunicazione**

Ogni schema di QKD si basa sull'utilizzo di due canali:

- Un canale quantistico in cui viene condivisa la chiave, tramite qubit;
- Uno classico autenticato, in cui Alice e Bob si scambiano informazioni relative al protocollo.

Le informazioni condivise sul primo canale possono essere intercettate e modificate nel rispetto dei postulati della meccanica quantistica, mentre

nel secondo canale avviene una comunicazione pubblica, in cui si ha garanzia dell'integrità dei messaggi e certezza del mittente.

Entrambi i canali sono necessari: tramite il canale quantistico si possono condividere informazioni in maniera sicura però serve il canale classico per estrarle.

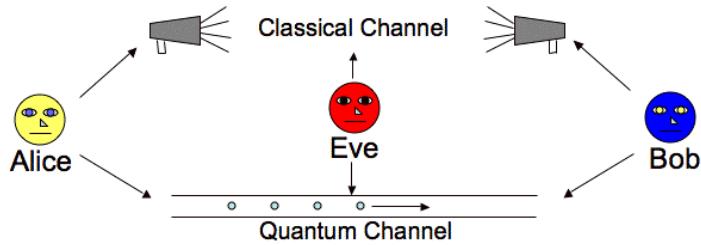


Figura 2.7 - illustrazione dello scenario della QKD

2.2.2 Il meccanismo generale del QKD

Come ben chiarito precedentemente gli effetti della meccanica quantistica possono essere usati per trasferire informazioni da Alice a Bob, e qualsiasi tentativo di intercettazione di Eva sarà sempre rilevabile. Per permettere ciò bisogna definire delle regole e passi da seguire, un protocollo di distribuzione delle chiavi, combinando l'elaborazione quantistica e procedure classiche ben consolidate.

Possiamo definire tre passi necessari:

1. Scambio della chiave non elaborata (raw key exchange);
2. Setacciatura della chiave (key sifting);
3. Distillazione della chiave (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.

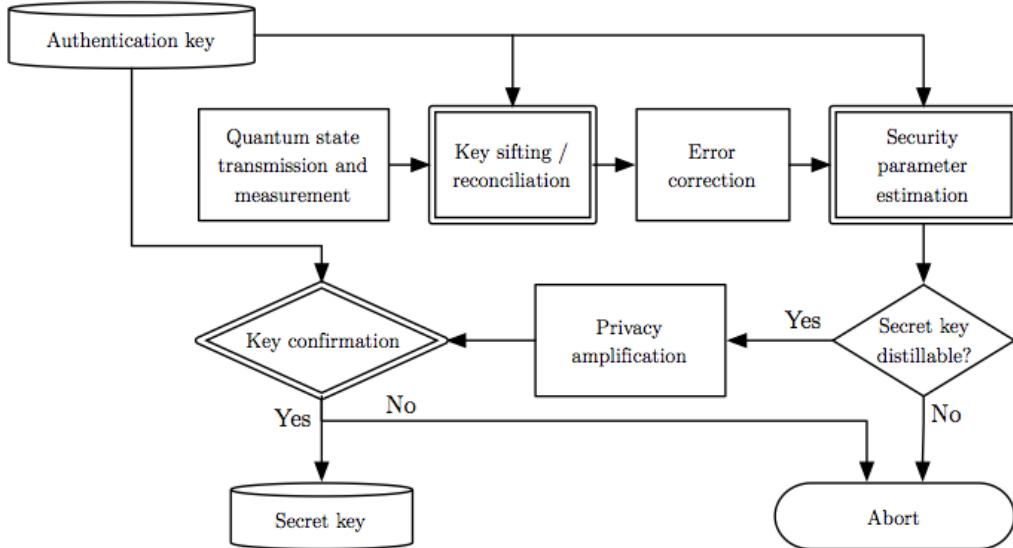


Figura 2.8 - schema generale delle fasi di un protocollo QKD

Raw Key Exchange

Questa fase è l'unica parte quantistica della Quantum Key Distribution in cui Alice e Bob si scambiano “alcuni stati quantici”, rappresentati l'informazione quantistica, i quali transitano lungo un canale quantico inviati da Alice per essere poi misurati da Bob, con o senza la presenza di Eve (l'intercettatore).

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

Key Sifting

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.

Key Distillation

La necessità di un'ulteriore elaborazione dopo la fase di setacciamento della chiave è stata definita durante la revisione dei risultati sperimentali in quanto 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:

- **Error Correction**

Un classico protocollo di correzione degli errori stima il tasso di errore effettivo della trasmissione, noto come Quantum Bit Error Rate (QBER). Gli errori si verificano sia attraverso il rumore sul canale quantico, sia con la presenza di un intercettatore, ma per ragioni di sicurezza, si presume che tutti gli errori siano dovuti a intercettazioni. Se il QBER è inferiore a un valore massimo predeterminato, la chiave segreta passa alla fase successiva della distillazione della chiave. Se il QBER è maggiore di questo valore, si giunge alla conclusione che la quantità di informazioni perse è troppo grande per garantire la segretezza, quindi la chiave segreta viene scartata e viene avviato un nuovo ciclo di QKD.

- **Privacy Amplification**

Questa fase è progettata per neutralizzare qualsiasi conoscenza che Eve possa aver acquisito sulla chiave setacciata. L'amplificazione della privacy comprime la chiave setacciata di un fattore appropriato, determinato dall'indice QBER precedentemente calcolato: un QBER elevato richiede più compressione, che ha come scopo quello di rimuovere almeno lo stesso numero di bit dalla chiave di cui Eve potrebbe esserne a conoscenza. Sono stati definiti processi di amplificazione della privacy dimostrabili su l'utilizzo di due funzioni hash universali.

- **Autenticazione**

Come affermato in precedenza, probabilmente la fase più importante dell'intero protocollo QKD è questa finale: bisogna eseguire un'autenticazione classica per garantire che Alice e Bob non siano i soggetti di un attacco man-in-the-middle (MITM). Un avversario si potrebbe porre come Bob ad Alice e Alice a Bob: tutto il traffico tra loro viene quindi reindirizzato attraverso una terza parte, senza che loro lo sappiano. Sfortunatamente, la stessa elaborazione quantistica è impotente contro un simile attacco. Tuttavia, la QKD ha una proprietà che può essere utilizzata per rafforzare le procedure di autenticazione classiche: 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, con livelli di sicurezza maggiori.

Lunghezza della chiave utilizzabile

Con il progredire delle varie fasi del protocollo QKD, la lunghezza della chiave utilizzabile viene ridotta, ciò rende la QKD intrinsecamente inefficiente nell'utilizzo della chiave generata, dato che molti bit vengono scartati alla fine di ogni passo del protocollo.

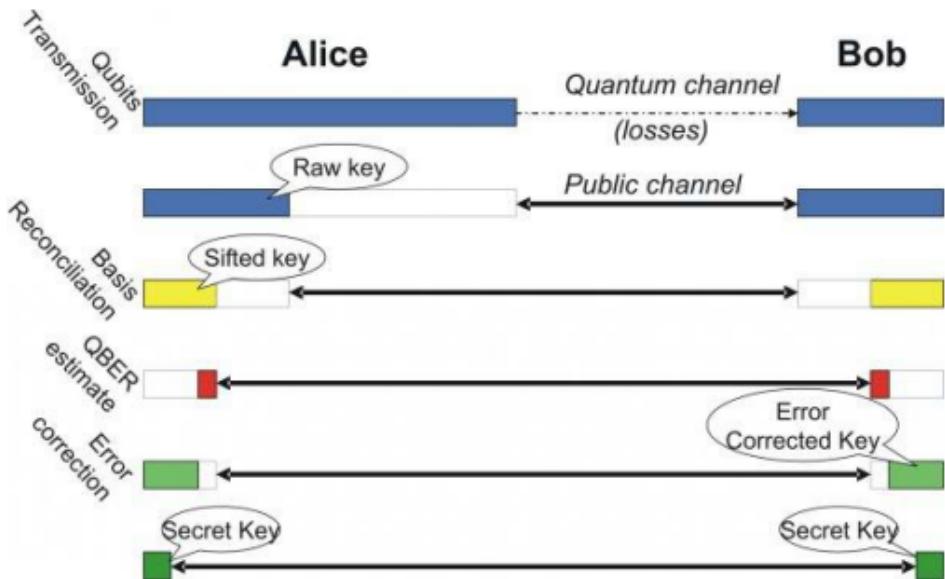


Figura 2. 9 - illustrazione della lunghezza della chiave dopo le varie fasi del protocollo QKD

2.2.3 Il Quantum Key Exchange

La comunicazione quantica implica la codifica dell'informazione in stati quantici, o qubit, al contrario dell'uso di bit della comunicazione classica. La QKD sfrutta certe proprietà di questi stati quantistici per garantirne la sicurezza. Esistono diversi approcci, ma possono essere suddivisi in due categorie principali a seconda della proprietà:

- **Prepare and measure protocols**

In contrasto con la fisica classica, l'atto di misurazione è parte integrante della meccanica quantistica. In generale, misurare uno stato quantico sconosciuto cambia in qualche modo quello stato. Questa è una conseguenza dell'indeterminazione quantistica e può essere sfruttata al fine di rilevare qualsiasi intercettazione sulla comunicazione (che richiede necessariamente misurazioni) e, soprattutto, per calcolare la quantità di informazioni che è stata intercettata.

- **Entanglement based protocols**

Gli stati quantici di due (o più) oggetti separati possono essere collegati insieme in modo tale che essi debbano essere descritti da un solo stato quantico combinato. Questo è noto come entanglement: la misurazione su un oggetto influisce sull'altro. Se una coppia di oggetti “aggrovigliati” è condivisa tra due parti, chiunque intercetta l'oggetto altera il sistema complessivo, rivelandone la presenza (e la quantità di informazioni che hanno ottenuto).

I protocolli descritti successivamente utilizzano entrambi la codifica a variabili discrete: il BB84 (Prepare and measure) e il protocollo di Ekert (Entanglement based).

2.2.4 Il protocollo BB84

Il primo protocollo di QKD è stato proposto nel 1984 da Charles H. Bennett e Gilles Brassard con il nome BB84.

Chiamiamo Alice e Bob le due entità che vogliono creare una chiave crittografica segreta e condivisa. Fra di esse sono presenti due canali: uno pubblico ordinario, classico, e uno “quantistico” in cui sia possibile inviare fotoni.

Potendo considerare i fotoni come oggetti “quantistici”, essi sono soggetti alle leggi fisiche sopra descritte. 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.

Consideriamo ora 4 stati quantistici definiti da fotoni polarizzati a 0° , 90° , 45° e 135° e rappresentiamoli rispettivamente con i simboli \uparrow , \rightarrow , \nearrow e \searrow .

Gli stati \uparrow e \rightarrow identificano una base che indicheremo con \oplus (base rettilinea); a loro volta \nearrow e \searrow ne identificano un’altra che indicheremo con \otimes (base diagonale).

Le due basi sono tra loro non ortogonali, ciò significa che, per il principio di indeterminazione, non è possibile misurare contemporaneamente se la polarizzazione è diagonale o rettilinea, perché nel momento in cui si misura il fotone in una base, lo si modifica in modo permanente.

Le basi e polarizzazioni utilizzate sono:

Base	Rappresentazione	Bit 0	Bit 1
Rettilegna	\oplus	\uparrow	\leftrightarrow
Diagonale	\otimes	\nearrow	\searrow

Il protocollo è il seguente:

1. Creazione della chiave e Codifica

Alice sceglie una stringa di bit e una sequenza di basi casuali con cui codificarla (rettilegna o diagonale) e 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 (Prepare and measure).

2. Lettura – Raw Key Exchange

Per ogni fotone ricevuto, Bob sceglie casualmente (indipendentemente dalle scelte di Alice) una delle due basi di polarizzazione \oplus o \otimes , misura la polarizzazione del fotone e intreppa ogni risultato come 0 o 1 a seconda dell'esito della corrispondente misura.

Con tale strategia si ottiene una risposta del tutto causale, in modo tale che Bob riesce ad ottenere dati significativi da circa il 50% dei fotoni che ha misurato.

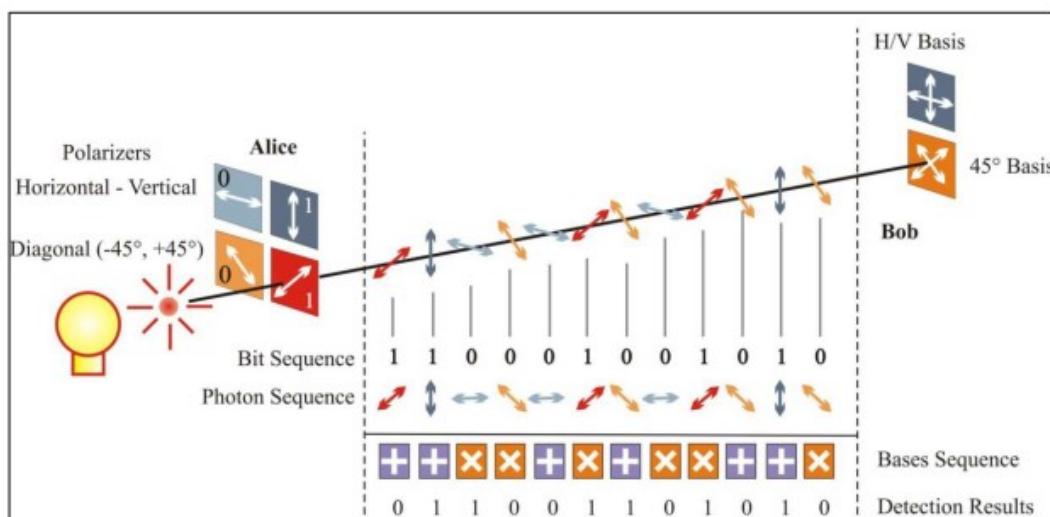


Figura 2.10 - illustrazione della fase di raw key exchange

3. Key Sifting

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.

Poiché è solo la base che viene discussa pubblicamente, 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.

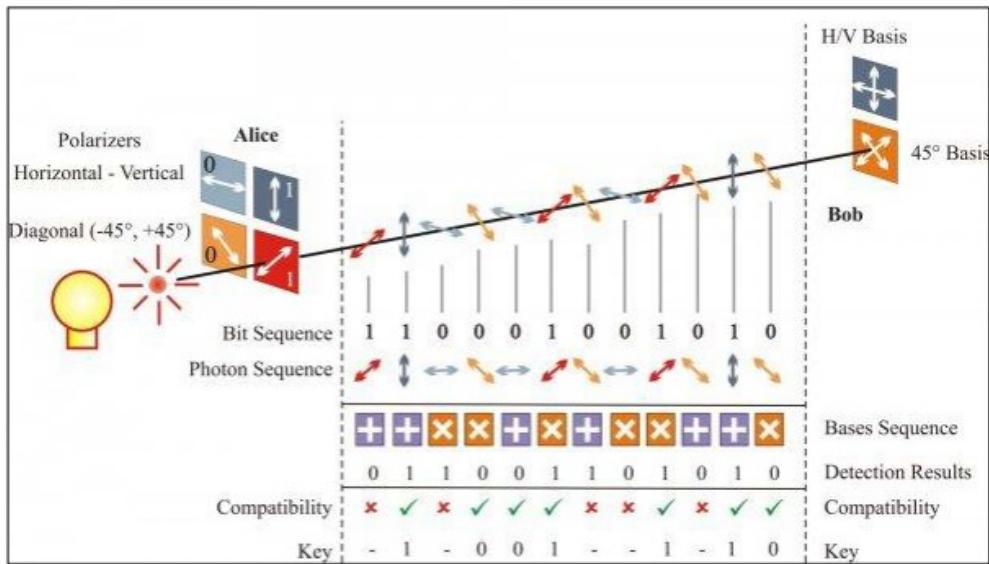


Figura 2. 11 - illustrazione della fase sifting key

4. Key Distillation

Il processo di setacciamento dovrebbe, in media, lasciare la metà dei qubit, 50%. 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.

Post-Processing - Key Distillation

L'ultimo passo del protocollo descritto, è dispendioso come controllo in quanto una 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, infatti, capitare degli errori sperimentali, dovuti, ad esempio, a ripolarizzazioni dei fotoni durante il transito, anche in assenza di origliamento, oppure fotoni persi o che non sono stati rilevati correttamente. Sembrerebbe quindi che non ci sia una via di uscita: ci sono sempre errori e non si riesce a distinguere con sicurezza tra errori sperimentali ed errori dovuti ad Eve.

La soluzione a questo apparente insolubile problema, è in realtà relativamente semplice. Come già detto, si considera che gli errori siano sempre dovuti ad Eve e bisogna aggiungere due ulteriori fasi da applicare alla sifted key :

- **Error Correction**

La prima fase si chiama “Reconciliation” o “Error Correction” e permette ad Alice e Bob di eliminare tutti gli errori nella sifted key di Bob ed al contempo stimare la percentuale di errori trovati, Quantum Bit Error Rate (QBER). Se questa percentuale è inferiore all’11%, allora si può passare alla fase successiva.

- **Privacy Amplification**

In questa fase 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.

Questo è possibile perché se Eve ha introdotto errori solo per al più l’11%, vuol dire che la sua conoscenza della sifted key è sufficientemente ridotta, conosce pochi bit della chiave, e quindi modificando appropriatamente la chiave segreta Alice e Bob possono eliminare i bit a conoscenza di Eve.

Queste ultime due fasi possono essere realizzate anche pubblicamente poiché le informazioni scambiate tra Alice e Bob non aiutano Eve a fare lo stesso. Bisogna inoltre notare che in queste due fasi la lunghezza della chiave viene ridotta. A seconda delle procedure utilizzate la chiave segreta finale può anche essere lunga solo 1/8 del numero di fotoni inizialmente inviato da Alice, come mostrato precedentemente. Da notare che la presenza di Eve viene rilevato soltanto dopo aver concluso l’invio dei fotoni, ovvero nella fase della Error Correction.

2.2.5 Il protocollo di Ekert

Nel 1991, Ekert propose un metodo per eseguire la distribuzione delle chiavi tra due parti attraverso fotoni polarizzati entangled in un canale quantico (entangled based protocol).

Questi fotoni entangled, che hanno particolari caratteristiche di correlazione, possono essere creati da Alice, Bob o da una terza parte fidata (Trusted Third Party), e ogni coppia è separata in modo che Alice e Bob ricevano una di ciascuna coppia.

Consideriamo il caso in cui si ha a disposizione una sorgente che produce una coppia di fotoni entangled che si propagano in versi opposti, uno verso il mittente Alice, e l'altro verso il destinatario, Bob.

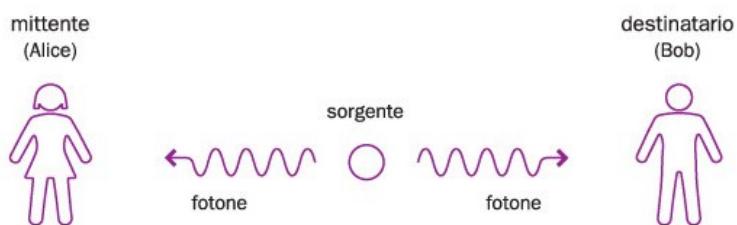


Figura 2. 12 - illustrazione dello scenario del protocollo di Ekert

In generale, lo stato di polarizzazione del sistema dei due fotoni entangled sarà una combinazione lineare, sovrapposizione di stati quantistici, di stati di polarizzazione ortogonali tra loro (nel nostro caso esempio verticale e orizzontale, oppure a 45° e a 135°).

Per effettuare le misurazioni dei fotoni le parti utilizzando due filtri di polarizzazione verticale 0° oppure a 45°.

I passi del protocollo sono:

1) Raw Key Exchange

Ciascuno dei due sceglierà, individualmente, in maniera perfettamente casuale la direzione lungo cui eseguire ciascuna misura. Registreranno il numero 0 ogni volta in cui il fotone non supera il test, e il numero 1 ogni volta in cui esso lo supera e annotano il tipo di test eseguito

I risultati delle misure sono genuinamente casuali, con probabilità 0,5 per ciascuna possibilità; nel caso in cui una misura venga eseguita nella stessa direzione da Alice e Bob i due esiti coincideranno inevitabilmente.

Ognuno di essi possiede una raw key.

Alice		1		1	0				1	0	1		0	1		1	1	0
			0			0	1	0				0		0		0		

Bob			1	1				1		0				1		1	1	
		0			1	0	1		0		1	0	0	0		0		0

2) SiftingKey

A questo punto del processo sia Alice che Bob potranno annunciare pubblicamente la direzione che hanno scelto per eseguire ciascuna misura.

Alice		1		1	0				1	0	1		0	1		1	1	0
			0			0	1	0				0		0		0		

Bob			1	1				1		0				1		1	1	
		0			1	0	1		0		1	0	0	0		0		0

Alice e Bob elimineranno dalla propria raw key tutti i casi in cui risultano aver effettuato misure lungo direzioni diverse l'uno dall'altro, mantenendo invece tutti i rimanenti risultati cioè quelli che coincidono, nel loro ordine, determinando la sifting key.

Alice		1			0		1		1	1								
			0	1		0		0		0								

Bob		1			0		1		1	1								
			0	1		0		0		0								

Mediamente la lunghezza della chiave dopo la fase di setacciamento è circa il 50% della raw key iniziale.

3) DistillationKey

Per rilevare la presenza di un eventuale intercettatore (Eve), Alice e Bob annunciano pubblicamente alcuni dei bit della sifting key, ad esempio i bit in posizione dispari;

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.

Alice			0	1	1
		0			

Bob			0	1	1
		0			

Il punto di forza è che 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.

3 QKD - Gli Attacchi, la Sicurezza e le Limitazioni

Il computing quantistico minaccia l'obiettivo di base della comunicazione sicura e autentica perché, essendo in grado di eseguire certi tipi di calcoli che i computer convenzionali non sono in grado, le chiavi di crittografia possono essere compromesse rapidamente da un computer quantistico, permettendo a un intercettatore di ascoltare le comunicazioni private e sostituirsi a qualcuno. Tuttavia primitive come la QKD che basano le sue radici nella meccanica quantistica non rendono possibile ciò.

In questo capitolo verrà descritto il tipo di sicurezza offerto dalla QKD, i tipi di attacchi possibili e, infine, le limitazioni della QKD.

3.1 La quantum security

L'introduzione della meccanica quantistica nella crittografia è volta principalmente ad identificare un metodo infallibile per trasferire informazioni in modo sicuro, ovvero per fornire al crittologo uno strumento tramite il quale, con opportuni protocolli di comunicazione, si renda fisicamente impossibile intercettare e decifrare la comunicazione

Com'è noto, la sicurezza degli algoritmi di crittografia classica è legata all'elevata complessità computazionale richiesta dagli attacchi crittoanalitici, anche dai più efficienti. Ciò significa che la sicurezza di tali algoritmi è legata al fatto che, nel caso peggiore, il tempo richiesto al crittoanalista per decifrare il messaggio, con l'attuale potenza di calcolo, risulta proibitivo.

3.1.1 Considerazioni sull'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.

Alice e Bob possono infatti come descritto nei protocolli precedenti rilevando alcuni dei bit delle loro chiavi possono determinare la presenza di un intercettatore. Infatti seguendo quanto esposto in precedenza, considerando i risultati dalla meccanica quantistica, possiamo affermare che se non sono

presenti errori, non c'è stata nessuna misurazione e dunque significa che non vi è alcuna presenza di un eavesdropper. 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.

Un altro vantaggio è dato dal fatto che 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.

Il BB84 è stato dimostrato sicuro contro ogni attacco permesso dalla meccanica quantistica, sia per inviare informazioni usando una sorgente di fotoni ideale che emette un solo fotone alla volta, e anche usando sorgenti di fotoni pratici che a volte emettono impulsi multifotonici.

3.1.2 La sicurezza incondizionata

Come spiegato nella sezioni precedenti, la misurazione degli stati quantici modifica il sistema quantico: Eve non può, quindi, ottenere alcuna informazione su una trasmissione quantica senza essere rilevato. Questo è vero anche se Eve avesse risorse e tempo di calcolo infiniti, o anche un computer quantistico, in quanto le leggi della fisica lo impediscono.

Questo è la forza della crittografia quantistica: sicurezza incondizionata, immune da intercettazioni non rilevate. Sfortunatamente, "incondizionato" è un termine improprio, poiché ci sono alcune condizioni che devono essere soddisfatte per esserlo:

- Eve non può ispezionare i dispositivi di Alice e Bob per vedere o influenzare la loro creazione o il rilevamento dei fotoni.
- Il generatore 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 (Carter Wegman protocols).
- Eve deve obbedire alle leggi della fisica.
- Il messaggio deve essere crittografato utilizzando uno schema simile ad OTP.

3.2 Gli attacchi e le strategie difensive

In questo paragrafo verranno esposti i principali attacchi possibili alla QKD e quali strategie difensive adottare, la cui sicurezza è garantita intrinsecamente dell'applicazione della meccanica quantistica.

3.2.1 Attacco di intercettazione-rinvio

Il tipo più semplice di attacco possibile è l'attacco di intercettazione-rinvio, in cui Eve misura gli stati quantici, fotoni, inviati da Alice e quindi 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.

Riconsideriamo le fasi della raw key exchange:

1. Alice sceglie una stringa di bit e una sequenza di basi casuali con cui codificarla (rettilinea o diagonale) e invia sul canale quantistico la corrispondente sequenza di fotoni polarizzati, ognuno rappresentante un bit della stringa nella base scelta in accordo allo schema definito.
2. Eve intercetta i fotoni, ma è esattamente nella stessa posizione di Bob in precedenza: non sa quali basi ha usato Alice per generare le polarizzazioni, quindi la sua unica tattica possibile è di impostare casualmente anche le sue basi di intercettazione. Quindi, come Bob, le sue basi verranno impostate correttamente solo metà delle volte e le impostazioni errate provocheranno letture di polarizzazione casuali e la distruzione della polarizzazione originale. Di conseguenza, quando lei invia nuovamente i fotoni che ha intercettato, il 50% di essi sarà sbagliato.
3. Bob impone le sue basi casualmente come al solito, ma in questo caso, quando impone 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.

La tabella seguente mostra un esempio di questo tipo di attacco.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarisation Alice sends	↑	→	↖	↑	↖	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarisation Eve measures and sends	↑	↗	→	↑	↖	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×		+
Photon polarisation Bob measures	↑	↗	↗	↖	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS	+							
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

Figura 3.1 - Tabella che mostra i vari passi eseguiti dal protocollo in un attacco intercetta-rinvio

3.2.2 Photon Number Split Attack

Nel protocollo BB84, Alice invia stati quantici a Bob usando singoli fotoni. In pratica, molte implementazioni usano impulsi laser attenuati ad un livello molto basso per inviare gli stati quantici. Questi impulsi laser contengono un numero molto piccolo di fotoni, ad esempio 0, 1 o 2 fotoni per impulso, che sono distribuiti secondo una distribuzione di Poisson.

Ciò significa che la maggior parte degli impulsi in realtà non contiene fotoni (non viene inviato alcun impulso), alcuni impulsi contengono 1 fotone (che è desiderato) e 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 $1-f$.

Questa è la base dell'attacco di divisione del numero di fotoni (PNS), denominata anche divisione del raggio, dove Eve memorizza questi fotoni extra in una memoria quantistica finché le corrette basi della codifica non sono state annunciate nella discussione pubblica tra Bob e Alice. Eve può quindi misurare i suoi fotoni nella base corretta e ottenere informazioni sulla chiave senza introdurre errori rilevabili. Non introduce alcune errori, in quanto riduce l'intensità dell'impulso che riceverà Bob di un fattore $1-f$, e attribuire tale perdita, se f è piccola a perdite del canale.

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, per esempio:

- Alice invia a caso alcuni dei suoi impulsi laser con un numero di fotoni medio inferiore; questi stati di esca possono essere usati per rilevare un attacco PNS, dato che Eve non ha modo di dire quali impulsi sono il segnale e quale esca;
- 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.

3.2.3 Man in the Middle (MITM)

La QKD è vulnerabile a un attacco man-in-the-middle quando usato senza autenticazione così come qualsiasi protocollo classico, poiché 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. Ciò nonostante 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.

Sono stati proposti diversi metodi per creare questo segreto condiviso iniziale, ad esempio utilizzando una terza parte o la teoria del caos. Tuttavia, solo una famiglia di funzioni hash "quasi fortemente universali" può essere utilizzata per l'autenticazione incondizionatamente protetta.

3.2.4 Denial of Services (DoS)

Poiché attualmente una QKD richiede un mezzo, per esempio fibra ottica, tra i due punti, un attacco di DoS (negazione del servizio) può essere montato semplicemente tagliando o bloccando la linea. Questa è una delle motivazioni per lo sviluppo di reti di distribuzione di chiavi quantistiche(Quantum Network), che instraderebbe la comunicazione tramite collegamenti alternativi in caso di interruzione.

3.2.5 Trojan-Horse Attacks

Una QKD può essere sondata da Eve inscenando un Trojan-horse attack: inviando una luce brillante nel canale quantistico e analizzando i riflessi posteriori. In un recente studio di ricerca è stato dimostrato che Eve individua la scelta segreta della base di Bob con una probabilità superiore al 90%, violando la sicurezza del sistema.

3.3 Le limitazioni della QKD

Dalle descrizioni fatte fino ad ora, la QKD sembra avere molte potenzialità e benefici, con sicurezza incondizionata dimostrata e rilevamento dell'intercettazione garantito, eppure non c'è stato alcuna implementazione del QKD su larga scala.

Questo paragrafo esaminerà alcuni dei problemi che limitano il suo appeal alla comunità crittografica.

3.3.1 I collegamenti Point-to-Point e DoS

Il canale quantico è, per sua natura, una connessione point-to-point: Alice e Bob devono trovarsi a ciascuna estremità, con le loro sorgenti e rilevatori di fotoni.

È in diretto contrasto con l'agglomerato di connessioni che compongono Internet, dove chiunque può connettersi con chiunque altro, utilizzando una rete di computer fisicamente collegati da linee di trasmissione convenzionali.

La natura point-to-point della QKD limita la potenziale crescita e 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.

3.3.2 Le sorgenti e i rilevatori di fotoni

La qualità delle sorgenti e dei rivelatori di fotoni può avere un impatto significativo sulla sicurezza di un protocollo. I rivelatori hanno anche problemi pratici, per esempio:

- l'attività in background non è correlata ai segnali QKD, noti come dark counts (conteggi scuri - il tasso medio di conteggi registrati senza luce incidente) 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;

Un rilevatore di fotoni ideale dovrebbe avere le seguenti proprietà:

- Alta efficienza su un ampio intervallo spettrale;
- Bassa probabilità di generare rumore (ad esempio low dark count);
- Il tempo tra il rilevamento di un fotone e il corrispondente segnale elettrico dovrebbe essere il più costante possibile;
- Il tempo morto dopo un evento di rilevamento dovrebbe essere il più piccolo possibile da consentire maggiori velocità di trasferimento dati.

Il processo di rilevamento non è preciso al 100%, a causa di imperfezioni nel materiale di rilevamento, quindi ci sarà una discrepanza tra i tempi morti delle misure in base rettilinee e diagonali. Eva può osservare ciò, in modo tale da elaborare l'esatta discrepanza tra le basi. Se lei può anche controllare il tempo di arrivo dei fotoni per i rilevatori di Bob, può scegliere due ritardi tra i segnali per dare la più alta probabilità di una lettura su un rilevatore o altro, e quindi fare ragionevolmente delle ipotesi plausibili sul valore del qubit, 0 o 1, e quindi ottenere informazioni chiave.

Anche di fronte a un protocollo incondizionatamente sicuro, Eva può sempre attaccare l'attrezzatura - ad es. nel cosiddetto attacco "Cavallo di Troia", Eve illumina Alice e l'apparato di Bob, quindi analizza il suo backscattering (un processo noto come reflectometry).

3.3.3 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. Così come i 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 sarà 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) e limitano la trasmissione a lunga distanza di informazioni.

3.3.4 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.

3.3.5 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? Dopotutto, 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.

3.3.6 Side Channel Attacks

Un aspetto della sicurezza che raramente viene affrontato nelle prove di sicurezza è la possibilità di attacchi side channel: si verificano quando è possibile estrarre informazioni significative dal sistema indirettamente, inducendo dei guasti, o attraverso l'analisi delle caratteristiche fisiche di un sistema (tempo impiegato, potenza di calcolo, ecc...). La tecnologia QKD è ancora agli inizi e non ha avuto il beneficio di sostenere ricerca su questa tipologia di attacchi.

Un esempio notevole di un problema si è verificato nella prima pratica dimostrazione del protocollo BB84. Nell'esperimento, il modulo di Bob per rilevare i fotoni emetteva diverso il suono quando registra diverse polarizzazioni, a causa di un alimentatore rumoroso.

3.3.7 La gestione delle chiavi e Key Distribution Rate

La lunghezza del canale quantistico ha anche un effetto sul tasso di distribuzione della chiave. La velocità con cui la raw key può essere inviata diminuisce in modo esponenziale rispetto alla distanza, ed è considerato come un altro fattore limitante nell'usabilità dei sistemi QKD.

Inoltre la QKD, per essere efficace, 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. Questo non è un compito facile, e sarà soprattutto impegnativo per schemi di QKD in cui la risultante chiave segreta viene utilizzata in schemi One-Time Pad (OTP) .

Infatti schemi OTP non sono stati ampiamente utilizzati in passato proprio per questo motivo: la gestione della chiave è spesso difficile, poiché la chiave deve essere della stessa lunghezza del messaggio, completamente casuale e usato solo una volta, altrimenti la sicurezza è compromessa. Inoltre, vi è un canale classico autenticato che avrà bisogno di chiave simmetrica per essere scambiata come parte del set-up iniziale e appropriate chiavi di sessione simmetriche quando il canale viene utilizzato per la fase di setacciatura e distillazione dei protocolli QKD. Il punto cruciale non è solo una buona gestione delle chiavi, ma deve anche garantire che durante il ciclo di vita che la chiave rimanga sicura.

4 QKD – Un'Applicazione: Quantum Network

A questo punto si potrebbe pensare di aver tutti gli strumenti per poter realizzare un sistema crittografico perfetto. Questo è vero ma solo in parte, in quanto oltre ai limiti teorici bisogna ora risolvere i limiti pratici relativi all'implementazione di un sistema crittografico di questo tipo.

I protocolli descritti finora sono ben pensati e teoricamente validi. Tuttavia, la trasmissione quantica ha due problemi evidenti non affrontati dai protocolli, che ne limitano la praticità in un contesto più ampio:

- la natura point-to-point;
- limitazioni della distanza di un canale quantistico.

Alice e Bob hanno, necessariamente, bisogno di un collegamento fisso tra loro, il canale quantistico. Per mettere in comunicazioni più utenti, 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 . Chiaramente questo diventa impraticabile quando il numero di utenti è elevato, per cui è necessaria una strategia alternativa.

Ci sono dei limiti alla distanza che un segnale quantico può percorrere lungo un canale. La figura sottostante mostra la velocità di trasferimento di bit da un impulso coerente debole (Weak Coherent Pulse) rispetto alla distanza percorsa lungo un canale quantistico: una forte attenuazione del segnale viene osservata a una distanza critica, prima che il segnale scompaia a circa 120 km.

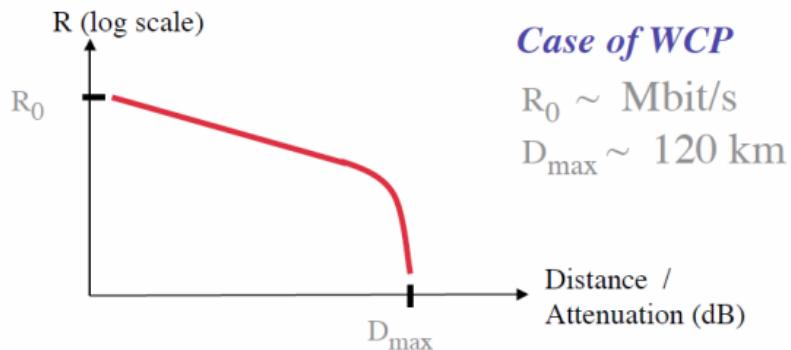


Figura 4. 1 - Grafico che mostra la velocità di trasferimento rispetto alla distanza percorsa

Molte ricerche sono state fatte nel tentativo di estendere questa distanza, ma è un fattore fortemente limitante intrinseco dei canali quantistici.

Verranno ora esaminate le varie strategie di progettazione per affrontare questi problemi e un overview sulle implementazione pratiche.

4.1 La Quantum Network

Tuttavia, la natura point-to-point dei collegamenti quantici potrebbe essere rimossa collegando i singoli collegamenti ali insieme in una rete. Gli obiettivi della progettazione per una rete quantistica sono:

- 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 collegamenti quantici (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.

4.1.1 I tipi di Quantum Network

Le reti quantistiche possono essere suddivise in tre tipi distinti, a seconda della tecnologia utilizzata in ciascun nodo che collega i singoli collegamenti quantici. Ognuno di essi ha punti di forza e di debolezza, e vari gradi di praticità.

- **Reti di nodi quantistici**

Un nodo quantistico può essere usato per combattere la decoerenza quantica del segnale lungo il canale quantistico eseguendo attivamente operazioni quantistiche sui fotoni in movimento.

Un modo per fare ciò richiede l'uso di fonti di entanglement quantistico, memorie quantistiche e tecniche di purificazione di entanglement successivamente memorizzati in una porzione del canale quantico.

Questi nodi sono ripetitori quantici: concatenano gli stati memorizzati e quindi ottengono un perfetto entanglement end-to-end utilizzabile su distanze arbitrariamente lunghe.

Tuttavia, i ripetitori quantici esistono solo in teoria, quindi per metterli in pratica si attende lo sviluppo di capacità di calcolo quantico a pieno titolo.

Un nodo quantistico meno elaborato è il Quantum Relay che non richiede una memoria quantistica, ed è quindi fattibile ma tecnologicamente difficile. Ciò nonostante, i Quantum Relay non estendono la distanza oltre la quale un segnale quantistico può essere inviato, quindi non sono adatti per una pratica rete QKD.

- **Reti di nodi ottici**

I nodi ottici utilizzano processi classici sul segnale quantico, ad esempio: scissione del fascio, multiplexing, de-multiplexing e commutazione.

Trattandosi di un approccio classico, rientra nelle capacità della tecnologia esistente e può essere utilizzato per creare relazioni QKD uno a molti.

Con l'aggiunta della commutazione attiva, due nodi QKD possono essere selezionati appositamente per la connessione. Questa funzionalità multiutente QKD è stata utilizzata nella prima rete di lavoro QKD, la rete BBN DARPA, che è stata istituita tra l'Università di Boston, Harvard e BBN.

I nodi ottici non hanno bisogno di essere considerati attendibili, poiché commutano semplicemente il segnale da un canale quantico a un altro; non viene eseguita alcuna elaborazione sul contenuto del segnale.

Lo svantaggio principale di questo tipo di rete è che non può essere utilizzata per estendere la distanza percorsa dal segnale quantico, a causa di perdite ottiche sul nodo.

- **Reti di relay affidabili**

Le opzioni descritte sopra hanno entrambi degli svantaggi: i nodi quantici estendono la distanza potenziale del segnale ma non sono realizzabili con la tecnologia odierna, i nodi ottici consentono il funzionamento multiutente ma riducono la distanza massima del segnale, rendendo entrambi meno che perfetti per un'implementazione pratica . Quindi una terza opzione, la rete di relay affidabili, è un compromesso.

Un nodo relay è considerato attendibile per inoltrare il segnale quantico senza intercettarlo o alterarlo. Per fare ciò in una rete QKD, le chiavi locali vengono generate tramite collegamenti QKD e archiviate in modo sicuro in nodi relay a ciascuna estremità dei collegamenti (i nodi sono effettivamente mini-Alice e mini-Bob che eseguono il protocollo QKD, indipendentemente da altri messaggi che vengono passati attraverso la rete.) Quando Alice e Bob, reali, vogliono eseguire un protocollo QKD, viene creata una catena di relay affidabili e i loro collegamenti quantici intermedi vengono creati per collegarli tra loro, formando un percorso QKD.

La chiave quantistica di Alice e Bob viene trattata come un messaggio e crittografata tramite un One-Time Pad utilizzando una chiave locale archiviata in un nodo relay: essa viaggia "hop-hop" tra ogni nodo sul percorso QKD, viene decrittografata e crittografata nuovamente in ciascuno nodo utilizzando una nuova chiave dall'archivio delle chiavi del nodo (naturalmente tutte le procedure di autenticazione classiche sicure e incondizionatamente sicure vengono eseguite anche su ciascun nodo utilizzando chiavi QKD memorizzate localmente).

Ciò fornisce una sicurezza incondizionata end-to-end a patto che tutti i nodi nel percorso QKD siano attendibili.

4.2 Implementazioni pratiche di Quantum Network

Per implementare una Quantum Network utilizzando la tecnologia odierna, la scelta ricade tra nodi ottici o relay affidabili.

Sono state implementate diverse reti di test che sono adattate al compito di QKD sia a breve distanza (ma collegando molti utenti), sia su distanze maggiori facendo affidamento su relay affidabili. Queste reti non consentono ancora la trasmissione end-to-end di qubit o la creazione end-to-end di entanglement tra nodi lontani.

Di seguito vengono riportate le principali implementazioni di Quantum Network:

- **DARPA Quantum Network**

A partire dai primi anni 2000, DARPA ha iniziato la sponsorizzazione di un progetto di sviluppo di QN con l'obiettivo di implementare comunicazioni sicure. La rete è diventata operativa all'interno del laboratorio di BBN Technologies alla fine del 2003 ed è stata ulteriormente ampliata nel 2004 per includere i nodi presso le università di Harvard e Boston. La rete è composta da più strati fisici, tra cui fibre ottiche che supportano laser modulati in fase e fotoni entangled, nonché collegamenti free-space.

- **SECOQC Quantum Network**

Dal 2003 al 2008 la Secure Communication based on Quantum Cryptography (SECOQC) ha sviluppato una rete collaborativa tra diverse istituzioni europee. L'architettura scelta per il progetto SECOQC è un'architettura di relay affidabili, che consiste in collegamenti quantici point-to-point tra dispositivi in cui la comunicazione a lunga distanza viene realizzata attraverso l'uso di relay (ripetitori). La rete utilizzava 200 km di cavo in fibra ottica standard per collegare sei ubicazioni attraverso Vienna e la città di St Poelten situata a 69 km ad ovest.

- **Rete gerarchica cinese**

Nel maggio 2009, a Wuhu, in Cina, è stata dimostrata una QN gerarchica. La rete gerarchica consiste in una rete backbone (dorsale) di quattro nodi

che collega un certo numero di sotto-reti. I nodi backbone sono connessi attraverso un router quantico a commutazione ottica. I nodi all'interno di ciascuna sottorete sono anche collegati tramite un interruttore ottico e sono collegati alla rete backbone tramite un relay affidabile.

- **Rete di Ginevra (SwissQuantum)**

IdQuantique ha completato con successo il progetto più lungo (testato tra il 2009 e il 2011) per testare la QKD in un ambiente di reale. L'obiettivo principale del progetto di rete SwissQuantum installato nell'area metropolitana di Ginevra nel marzo 2009 consisteva nel convalidare l'affidabilità e la robustezza del QKD in funzionamento continuo per un lungo periodo di tempo in un ambiente di campo. Lo strato quantico ha funzionato per quasi 2 anni fino alla chiusura del progetto nel gennaio 2011 poco dopo la durata inizialmente prevista del test.

- **Rete QKD di Tokyo**

Nel 2010, un certo numero di organizzazioni dal Giappone e dall'UE hanno installato e testato la rete QKD di Tokyo. Essa si basa sulle tecnologie QKD esistenti e ha adottato un'architettura di rete simile a SECOQC. Per la prima volta, la crittografia one-time-pad è stata implementata con una velocità di trasmissione dei dati sufficientemente elevata per supportare applicazioni comuni per utenti finali, quali videoconferenze. Le precedenti reti QKD su larga scala tipicamente utilizzavano algoritmi di crittografia classici come AES per il trasferimento di dati ad alta velocità e utilizzano le chiavi derivate da quantum per dati a bassa velocità o per reimpostare regolarmente i classici algoritmi di crittografia.

- **Los Alamos National Laboratory**

Una rete hub-and-spoke è stata gestita dal Los Alamos National Laboratory dal 2011. Tutti i messaggi sono instradati tramite l'hub. Il sistema equipaggia ogni nodo della rete con trasmettitori quantici, cioè laser, ma non con rivelatori di fotoni costosi e voluminosi. Solo l'hub riceve messaggi quantici. Per comunicare, ciascun nodo invia un messaggio one-time pad all'hub, che quindi utilizza per comunicare in modo sicuro su un collegamento classico. L'hub può indirizzare questo

messaggio a un altro nodo utilizzando un altro messaggio one-time pad dal secondo nodo. L'intera rete è protetta solo se l'hub centrale è sicuro. I nodi dei prototipi hanno le dimensioni molto piccole, simili ad una scatola di fiammiferi.

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

Figura 4. 2 - Tabella delle implementazioni QN realizzate e protocolli supportati

5 Il Futuro del QKD

5.1 La necessità e l'utilizzo del QKD

Il problema più spinoso è se la QKD sia effettivamente necessario. Questa questione ha diviso gli accademici della comunità crittografica in due:

- chi sostiene che la QKD sia effettivamente una soluzione che non può avere un uso pratico in futuro;
- chi, invece, considerare la QKD come una soluzione più che valida, in quanto la crittografia come noi la conosciamo è condannata.

Gli algoritmi utilizzati nella crittografia moderna mostrano che è computazionalmente impossibile per un utente malintenzionato provare ogni possibile chiave crittografica, cioè sferrare un attacco di forza bruta, per ottenere l'accesso alle informazioni crittografate. Pertanto, la sicurezza fornita dagli schemi attuali è computazionalmente sicura, ma non incondizionatamente sicura. Tuttavia, a fini pratici, è un meccanismo di difesa estremamente forte: se un sistema di sicurezza fallisce, è molto più probabile che si tratti 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, gli algoritmi simmetrici continueranno a far fronte semplicemente raddoppiando la lunghezza della chiave (per annullare gli effetti dell'algoritmo di Grover). Allo stesso modo, quando l'algoritmo di Shor renderà inutilizzabili schemi asimmetrici, ci sono altri algoritmi adatti in fase di sviluppo, come i sistemi basati su reticolo che sono immuni ai progressi dell'elaborazione quantistica.

Le domande poste dalla comunità crittografica è se il requisito di sicurezza incondizionata è un obiettivo aziendale sufficientemente grande da giustificare le spese di attrezzature e infrastrutture specializzate, e quali vantaggi possa portare in termini di sicurezza rispetto agli attuali protocolli di distribuzione delle chiavi crittografiche. L'introduzione della distribuzione di chiavi quantistiche, ovvero l'aggiornamento dalla sicurezza computazionale a quella incondizionata, non aumenta necessariamente la protezione complessiva di un

cripto-sistema: come afferma Bruce Schneier "*La sicurezza è una catena: è forte quanto il suo anello più debole*". Ciò potrebbe comportare:

- rafforzando ulteriormente l'anello più forte della catena, induce gli aggressori a cercare vulnerabilità altrove nel sistema.
- l'aumento percepito della sicurezza potrebbe portare a effetti indesiderati altrove nel sistema, nello stesso modo in cui, per esempio, le persone adottano stili di guida più pericolosi una volta che l'uso delle cinture di sicurezza è diventato obbligatorio, poiché la loro percezione della sicurezza è aumentata così si sono verificate attività di compensazione dei rischi.

Quello che si percepisce 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. Recentemente è stato riconosciuto che forse le cose erano andate troppo oltre e che entrambi i campi dovevano lavorare insieme per fornire soluzioni di sicurezza per il mondo dell'informatica pre e post quantistica. Una soluzione è che il panorama crittografico potrebbe evolversi laddove gli strumenti QKD e asimmetrici possono combinarsi, senza la necessità di una divisione classica / quantistica, per fornire una sicurezza a prova di futuro, cioè che anche se un sistema di crittografia viene interrotto in un tempo futuro non specificato, i messaggi precedenti inviati attraverso di esso rimangono sicuri.

5.1.1 Quando utilizzare la QKD

Nonostante i dubbi, l'adozione generalizzata di 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.

Nessun protocollo esistente è sicuro al 100%: la QKD non lo sarà, ma 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.

5.1.2 Le possibilità di sviluppo della QKD

Ci sono tre scelte aperte alla tecnologia embrionale del QKD:

1. 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;
2. utilizzare il meglio tra le tecnologie e protocolli disponibili, cercare e trovare una nicchia competitiva e sfruttala;
3. abbandonare la tecnologia quantistica e concentrarsi sul miglioramento dei metodi crittografici classici pronti per il mondo dei computer post-quantico.

L'opzione numero uno è basata sulla ricerca, con un limitato appeal commerciale, quindi basandosi sul fatto che rinunciare al QKD non è un'opzione finché il suo potenziale non è stato esplorato completamente, questa analisi continuerà con un occhio fisso su quel potenziale mercato di nicchia.

5.2 La ricerca nei protocolli e QN

La crittografia è un mondo molto vasto e ancora da esplorare. Le ricerche svolte finora non hanno portato risultati eccellenti e praticamente fattibili, non ripagando gli sforzi impiegati. Come detto, molte primitive della crittografia quantistica sono teoriche soltanto la QKD è fattibile e nonostante tutto soltanto il protocollo BB84 ha dimostrato la praticità di utilizzo, a differenza degli altri che hanno dimostrato delle falle che ne compromettono la sicurezza.

La rete SECOQC e la rete DARPA BBN hanno dimostrato che la rete QKD può essere praticamente valida. Le loro architetture hanno, in una certa misura, superato i problemi innati del QKD e sono state estese su una Metropolitan Area Network (MAN). Se, in futuro, l'ottica quantistica a spazio libero via satellite viene utilizzata come collegamenti backbone quantistici, allora è possibile coprire un'area geografica più ampia. Il design SECOQC consente la scalabilità e l'interoperabilità delle strutture QKD: tuttavia, il design è rilevante solo per l'utilizzo di relay affidabili. Le reti commutate o miste, che sono più comunemente utilizzate, non si prestano a questo tipo di progetto. È necessario fare più ricerca per incorporare la tecnologia QKD in reti miste, che amplierà le opportunità di implementazione.

Un'ulteriore stimolo di utilizzo della QKD è di non utilizzarla soltanto per la segretezza dei dati, ma anche per fornire strumenti di autenticazione dei messaggi e firma digitale.

In ogni caso, 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. Questo potrebbe essere lo stimolo principale per perseguire il miglioramento della tecnologia QKD e la ricerca della QN.

6 Uno strumento per la simulazione del protocollo BB84

L'attività progettuale del seguente elaborato include la realizzazione software di uno strumento che effettua la simulazione dei passi del protocollo del QKD: **BB84 Simulator**.

In questo capitolo ne verrà data una descrizione, la struttura del progetto e esempi di scenari d'utilizzo.

6.1 Descrizione del tool: BB84 Simulator

Il tool descritto è una semplice simulazione dei passi del protocollo BB84 descritto nel paragrafo 2.2.4, in breve: due parti Alice e Bob, senza che condividano alcuna informazione precedente, vogliono poter generare una chiave segreta sicura, in modo tale da rilevare la presenza di un eventuale intercettatore, Eve, se si intromette nella comunicazione.

Lo scenario preso in considerazioni consiste in 3 figure:

- **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 e, eventualmente, 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 e, eventualmente, 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 re-inviarli a Bob (sta inscenando un attacco intercettazione-rinvio).

Essendo una simulazione, il tool non tiene in considerazione alcuni fattori. Di seguito riportiamo le limitazioni:

- 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.

6.1.1 Le modalità di utilizzo e le fasi di esecuzione

Nel seguente sottoparagrafo si descrivono le modalità di utilizzo e le fasi di esecuzione del tool.

Modalità e basi utilizzate

E' possibile utilizzare il tool in due modalità:

- **Senza eavesdropping:** in questo scenario Alice e Bob riusciranno sempre a condividere una chiave segreta, in quanto non vi sarà alcun intervento da parte di Eve sul canale.
- **Con eavesdropping:** in tale modalità la presenza di Eve gioca un ruolo fondamentale nella generazione della chiave da parte di Alice e Bob; E' possibile attribuire ad Eve una probabilità di intervenire o meno la possibilità di misurare i fotoni in transito.

Le basi e polarizzazioni utilizzate sono:

Base	Rappresentazione	Bit 0	Bit 1
Rettilinea	\oplus	\uparrow	\leftrightarrow
Diagonale	\otimes	\nearrow	\searrow

Fasi di esecuzione

L'esecuzione viene suddivisa in 8 fasi:

Fase 0 - Inizializzazione

La configurazione iniziale richiede di impostare alcuni parametri come:

- Il numero di qubit da generare che costituiscono la raw key di partenza.

- La percentuale del numero di bit da controllare della sifting key, utilizzati nella fase di distillation key per individuare un eventuale intercettatore; Vengono presi i bit in posizione dispari della sifting key

Valore	Percentuale
Minimo 0	0%
Massimo 50	50%

- Il livello di intervento di un intercettatore sul canale per misurare i fotoni inviati dal mittente;

Livello	Percentuale	Probabilità
Minimo 1	10%	0,10
Massimo 10	100%	1

Fissando tale valore a 10 vuol dire che l'intercettatore misura ogni singolo fotone inviato dal mittente; impostandolo ad 1, ha lo 0,10 di probabilità nell'intervenire nella misurazione di ogni singolo fotone.

Fase 1 – Alice generazione raw key e basi

Alice sceglie in maniera del tutto casuale e indipendentemente i bit della chiave iniziale, raw key, e ciascuna base con cui codificare il relativo bit.

Fase 2 – Alice invia fotoni e Bob esegue la lettura

Vengono inviati i fotoni polarizzati di Alice all'interno del canale quantistico; Bob esegue la misurazione dei fotoni ricevuti, che potrebbero essere diversi da quelli inviati da Alice se vi è stata l'intromissione di Eve, scegliendo causalmente e indipendentemente a caso le basi, ottenendo la sua raw key.

Fase 3 – Bob invia le sue basi ad Alice

Bob invia sul canale classico le basi da lui utilizzate nel processo di misurazione dei fotoni, ma non cosa ha misurato; Alice effettua un controllo confrontando le basi che riceve con le proprie che ha utilizzato nel processo di polarizzazione dei fotoni.

Fase 4 – Alice invia le sue basi ad Bob

Analogamente, Alice invia sul canale classico le basi da lei utilizzate nel processo di polarizzazione dei fotoni, ma non cosa ha polarizzato; Bob effettua un controllo confrontando le basi che riceve con le proprie che ha utilizzato nel processo di misurazione dei fotoni.

Fase 5 – Generazione della sifting key

Alice e Bob, relativamente, scartano i bit dalla propria raw key per i quali le basi utilizzate da entrambe le parti nel processo di polarizzazione/misurazione non coincidono; in questo modo entrambi ottengono una nuova chiave, più corta (stimata la metà della lunghezza della raw key), denominata sifting key (chiave setacciata).

La sifting key potrà essere differente tra le parti se Eve si è intromesso nella comunicazione.

Fase 6 – Alice invia i suoi bit di controllo a Bob

Alice estrae i bit di posizione dispari dalla propria sifting key, il cui numero è definito in base alla percentuale scelta nella fase di inizializzazione e la lunghezza della sifting key; Alice invia tale sottoinsieme di bit di controllo a Bob.

Fase 7 – Bob invia i suoi bit di controllo ad Alice

Analogamente, Bob estrae i bit di posizione dispari dalla propria sifting key, definito in base alla percentuale scelta nella fase di inizializzazione e la lunghezza della sifting key; Bob invia tale sottoinsieme di bit di controllo ad Alice.

Fase 8 – Generazione della distillation key

Alice e Bob verificano se i bit di controllo inviati e ricevuti coincidono; A questo punto possono esserci due casi:

- c'è almeno un bit differente: hanno trovato almeno una discrepanza nella loro sifting key, dunque hanno rilevato la presenza di Eve; la comunicazione risulta essere insicura e la chiave compromessa per cui bisogna ripetere nuovamente l'intero processo.

- non ci sono bit differenti: assumono che non ci sono discrepanze nelle loro sifting key e, dunque, che Eve non è intervenuto sul canale; a questo punto possono essere due scenari possibili:
 - Eve non ha effettivamente alterato la comunicazione, allora la chiave segreta (distillation key) viene generata da entrambe le parti scartando dalla propria sifting key i bit di controllo; tali chiavi saranno uguali e risulteranno essere sicure e utilizzabili come chiave segreta.
 - Eve ha alterato la comunicazione, allora la chiave segreta (distillation key) viene generata da entrambe le parti scartando dalla propria sifting key i bit di controllo; tali chiavi verranno considerate erroneamente sicure: possono essere uguali o anche diverse, ma in ogni caso Eve ne conosce alcuni bit; Questo accade quando la probabilità di intervento di Eve nel canale è molto bassa e/o il numero di bit di controllo non è sufficiente per garantire la rilevazione di Eve.

6.1.2 Le probabilità utilizzate per effettuare analisi

In questo paragrafo verranno trattate le probabilità utilizzate dal tool per descrivere gli scenari che si presenteranno in base ai settaggi utilizzati per comprendere ed analizzare meglio la simulazione.

Il tool definisce due tipi di probabilità:

- **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 (metà della raw key) e la percentuale impostata nella fase di inizializzazione;
 - si utilizza la probabilità di intervento di Eve in base al livello scelto nella fase di inizializzazione;
- **Probabilità effettive:** vengono calcolate a posteriori, dopo che il protocollo viene eseguito. Si considerano le reale misurazioni, ovvero:
 - la lunghezza della sifting key può essere variabile;
 - il numero dei bit da controllare è calcolato sulla lunghezza della sifting key (variabile) e la percentuale impostata nella fase di inizializzazione;

- o la probabilità di intervento di Eve è definita dal numero di intercettazioni che sono effettivamente avvenute ;

Probabilità di Bob nelle misurazioni

Durante il processo di misurare Bob nello scegliere la base può commettere degli errori di valutazione, ovvero il bit misurato e la base differiscono da quella utilizzata da Alice.

- Probabilità di errore di Bob nella ricezione di ogni singolo fotone senza la presenza di Eve risulta essere:

$$P(\text{Bob non commette errore}) = P(\text{Scelta della base giusta}) * P(\text{Bit misurato correttamente con la base scelta}) + P(\text{Scelta della base sbagliata}) * P(\text{Bit misurato correttamente con la base scelta}) = \frac{1}{2} * 1 + \frac{1}{2} * \frac{1}{2} = \frac{3}{4} = 75\%$$

$$P(\text{Bob commette errore}) = 1 - P(\text{Bob non commette errore}) = \frac{1}{4} = 25\%$$

Per leggere i fotoni inviati da Alice, Eve deve effettuare delle misurazioni dei fotoni e nel farlo introduce degli errori. Questo ha un forte impatto successivamente nelle probabilità di errore nelle misurazioni effettuate da Bob.

E' stata definita la probabilità di intervento di Eve, in base al livello settato, ed indichiamola con s ($0 \leq s \leq 1$).

Le scelte delle basi di Alice, Eve e Bob da utilizzare nella misurazione dei fotoni avviene in maniera casuale e indipendentemente l'una dall'altra.

- Probabilità di errore di Bob nella ricezione di ogni singolo fotone con la presenza di Eve risulta essere:
 - o $P(\text{Bob commette errore}) * P(\text{Eve non è intervenuta}) = \frac{1}{4} * (1-s);$
 - o $P(\text{Bob non commette errore}) * P(\text{Eve interviene}) * P(\text{Eve causa un errore}) = \frac{3}{4} * s * \frac{1}{2}$

$$P(\text{Bob commette errore con Eve}) = \frac{1}{4} * (1-s) + \frac{3}{4} * s * \frac{1}{2} = \frac{1}{4} + s/8$$

Più la probabilità di intervento di Eve è maggiore, più la probabilità di Bob di commettere errore si alza.

Probabilità di rilevamento

La presenza di Eve nel canale potrebbe produrre delle diversità (discrepanze) nella sifting key.

- Probabilità che ci sia discrepanza tra le chiavi setacciate:

$$P(C'è Discrepanza) = P(Eve interviene) * P(Eve sceglie base sbagliata) * P(Eve causa un errore) = s * \frac{1}{2} * \frac{1}{2} = s/4$$

Alice e Bob rileveranno la presenza di Eve se troveranno almeno una discrepanza tra le due chiavi setacciate. Per effettuare questo controllo confronteranno un certo numero di bit m della chiave setacciata.

- Il numero probabile di discrepanze tra le chiavi setacciate:

$$\text{Numero bit confrontati} * P(C'è discrepanza) = m * s/4.$$

Tuttavia se per gli m bit controllati non si trova nessuna discrepanza ed Eve si è intromesso nella comunicazione, essa non viene rilevato.

- Probabilità che Eve non viene rilevato:

$$P(\text{Non c'è discrepanza}) ^ \text{Numero bit confrontati} = (1-s/4)^m$$

6.2 La struttura del progetto e classi principali

6.2.1 Le tecnologie utilizzate e struttura del progetto

Le tecnologie utilizzate

- un **JDK**, il kit di sviluppo per la tradizionale programmazione Java, visto che questa è la tecnologia con cui è stato realizzato il tool;
- un **IDE** (ambiente di sviluppo integrato) che includa possibilmente tutti gli strumenti necessari al programmatore; è stato utilizzato Eclipse.

Il progetto è organizzato nel seguente modo:

- **BB84Simulator**: directory dell'intero progetto contenente la directory `src`, la libreria utilizzata JavaSE-1.7 e le immagini del tool;
- **src**: directory contenente i pacchetti e i sorgenti
- **src/animation**: pacchetto che contiene i sorgenti della gestione dell'interfaccia grafica del tool; `Mainframe.java` permette l'esecuzione del tool;
- **src/coding**: cuore dell'intero progetto che contiene i sorgenti che permettono la definizione delle entità in gioco e le fasi del protocollo;
- **src/test**: contiene alcuni test della simulazione;
- **resources/images**: contiene le varie immagini necessarie .

6.2.1 Overview sulle classi principali

In questo sotto-paragrafo verranno descritte le principali classi, mostrandone il codice dei costruttori e alcuni metodi.

Per comprendere in maniera semplice il funzionamento del tool, alla fine della descrizione delle classi, si mostrerà il workflow della codifica e invio dei fotoni da parte di Alice e la lettura da parte di Bob attraverso il canale quantistico. Per questo motivo i metodi mostrati nella descrizione delle classi sono incentrati su tale fase.

Sender, Receiver e Eavesdropper

Sender: rappresenta il mittente, ovvero Alice. I metodi contenuti al suo interno permettono di utilizzare il canale di comunicazione Channel e generare le varie chiavi utilizzate nei passi del protocollo BB84.

- Costruttore

```

public Sender(int NQubits){
    this.NQubits = NQubits;
    arrayFotoni = new TreeMap<Integer, Fotone>();
    indexFotoni = 0;
    indexBasi = 0;
    indexBit = 0;
}

```

Il costruttore prende in input il numero di qubit da inviare; vengono inizializzati dei contatori e un TreeMap contenente i fotoni da inviare.

- Metodi

```

public void creationRawKey(){
    rawKey = new TreeMap<Integer, Integer>();
    for(int i=0; i<NQubits; i++){
        rawKey.put(i, Engine.randomBit());
    }
}

```

Tale metodo è responsabile della generazione della raw key del mittente, invocando un metodo statico della classe Engine, randoBit(), che restituisce in maniera casuale un bit 0 o 1.

```

public void creationCasualBase(){
    arrayBasiSender = new TreeMap<Integer, Character>();
    for(int i=0; i<NQubits; i++){
        arrayBasiSender.put(i, Engine.randomBase());
    }
}

```

Analogamente al precedente, questo è responsabile della generazione della sequenza di basi del mittente.

```

public void sendFotone(){
    Fotone f = Engine.polarizzazione(rawKey.get(indexBit),
                                      arrayBasiSender.get(indexBasi));
    arrayFotoni.put(indexFotoni, f);
    channel.sendFotoneToReceiver(f);
    indexBit++;
    indexFotoni++;
    indexBasi++;
}

```

Questo metodo permette di inviare un fotone al destinatario utilizzando il canale di comunicazione. Innanzitutto viene effettuata la polarizzazione del fotone invocando il metodo statico della classe Engine, polarizzazione(int,char), fornendogli il bit che si vuole codificare con la relativa base da utilizzare e restituisce il Fotone. Quest'ultimo verrà

passato al canale tramite l'invocazione del metodo sendFotoneToReceiver(Fotone) della classe Channel.

Receiver: rappresenta il ricevente, Bob, e risulta essere del tutto analoga alla classe Sender.

- Costuttore

```
public Receiver() {  
    arrayBasiReceiver = new TreeMap<Integer, Character>();  
    rawKey = new TreeMap<Integer, Integer>();  
    indexBasi= 0;  
    indexBit = 0;  
}
```

Il costruttore non prende alcun input; vengono inizializzati dei contatori e due TreeMap: uno contenete i bit della raw key e l'altro le basi utilizzate per effettuare la misurazione dei fotoni.

- Metodi

```
public void notifyFotone(Fotone f){  
    arrayBasiReceiver.put(indexBasi, Engine.randomBase());  
    int bit = Engine.detection(  
        f, arrayBasiReceiver.get(indexBasi));  
    rawKey.put(indexBit, bit);  
    indexBit++;  
    indexBasi++;  
}
```

Questo metodo permette di misurare il fotone passato in input. Si sceglie una base casuale invocando il metodo statico randomBase() della classe Engine, e dopo di che si richiama il metodo Engine.detection(Fotone, char) che è responsabile della lettura del fotone ricevuto con la base passata in input, restituendo il bit decodificato; viene aggiornato la raw key con il nuovo bit restituito.

Eavesdropper: rappresenta l'intercettatore, Eve. E' simile alle classi precedenti ad esclusione del fatto che non contiene metodi per generare le chiavi del protocollo BB84.

- Costruttore

```

public Eavesdropper(int level) {
    checkLevel(level);
    indexBasi = 0;
    indexBit = 0;
    indexFotoni = 0;
    indexIntercept = 0;
    arrayBasiEve= new TreeMap<Integer, Character>();
    rawKey = new TreeMap<Integer, Character>();
    arrayFotoni = new TreeMap<Integer, Fotone>();
}

```

Il costruttore prende in input un intero, livello, che rappresenta la probabilità di intervenire nella misurazione dei fotoni nel canale;

- Metodi

```

public Fotone notifyFotone(Fotone f) {
    arrayBasiEve.put(indexBasi, Engine.randomBase());
    int bit = Engine.detection(f,
                                arrayBasiEve.get(indexBasi));
    char car = (""+bit).charAt(0);
    rawKey.put(indexBit, car);
    Fotone f2 = Engine.polarizzazione(bit,
                                        arrayBasiEve.get(indexBasi));
    arrayFotoni.put(indexFotoni, f2);
    indexFotoni++;
    indexBit++;
    indexBasi++;
    indexIntercept++;
    return f2;
}

```

Questo metodo permette di misurare il fotone passato in input e ri-polarizzazione del fotone, restituendolo come risultato; si sceglie una base casuale invocando il metodo statico randomBase() della classe Engine, e dopo di che si richiama il metodo Engine.detection(Fotone, char) che è responsabile della lettura del fotone ricevuto con la base passata in input, restituendo il bit decodificato; viene aggiornato la raw key con il nuovo bit restituito.

Dopodiché viene effettua la polarizzazione del fotone invocando il metodo statico della classe Engine, polarizzazione(int,char), fornendogli il bit restituito precedentemente con la relativa base utilizzate e restituisce il Fotone. Quest'ultimo verrà restituito come risultato.

Channel

Questa classe si occupa di indirizzare la comunicazione tra la due parti, Sender e Receiver. I suoi metodi non fanno altro che notificare l'arrivo di informazioni alla parte interessata.

- Costruttore

```
public Channel(Sender sender, Receiver receiver,
               double bitCompare) {
    this.sender = sender;
    this.receiver = receiver;
    this.sender.setChannel(this);
    this.receiver.setChannel(this);
    this.BIT_COMPARE = bitCompare;
}
```

Prende in input un'istanza della classe Sender, che rappresenta il mittente (Alice), un'istanza della classe Receiver, il ricevente (Bob) e un intero bitCompare che fa riferimento alla percentuale del numero di bit da comparare nella fase di distillation key. All'interno setta tutti i riferimenti e invoca il metodo setChannel sugli oggetti sender e receiver passandogli il riferimento a se stesso, in modo tale da permettere alle parti di interagire con il canale.

- Metodi

Come detto precedentemente i metodi non fanno altro che notificare le due parti, per esempio:

```
public void sendFotoneToReceiver(Fotone f) {
    if(QCActive)
        receiver.notifyFotone(f);
    else{
        System.out.println("Canale Quantico non attivo");
    }
}
```

Tale metodo può essere invocato dal sender utilizzando il riferimento al canale Channel impostato nel costruttore all'atto della istanziazione, per inviare un oggetto Fotone al receiver. All'interno del metodo viene effettuato un controllo per verificare che la comunicazione avvenga su un canale quantistico e si invoca il metodo dell'oggetto receiver notifyFotone passandogli il riferimento del Fotone ricevuto in input.

ChannelEavesdropper

Tale classe estende la classe Channel, ed ha il compito di far interagire nella comunicazione anche l'intercettatore Eavesdropper.

- Metodi

Tale classe non fa altro che riscrivere i metodi della classe Channel in modo tale da notificare sia l'intercettatore che la parte di competenza invocando il metodo della classe padre tramite il comando super.

```
@Override  
public void sendFotoneToReceiver(Fotone f) {  
    if(eve.tryGetPolarization()) {  
        Fotone f2 = eve.notifyFotone(f);  
        super.sendFotoneToReceiver(f2);  
  
    } else {  
        eve.notifyNoIntercept();  
        super.sendFotoneToReceiver(f);  
    }  
}
```

Tale metodo che permette di simulare un attacco di intercettazione-rinvio: Eve effettua la misurazione del fotone inviato dal mittente tramite il metodo notifyFotone(Fotone f) il quale restituisce un nuovo fotone che verrà inoltrato al ricevente.

L'intervento di Eve o meno è randomizzato dall'invocazione del metodo tryGetPolarization().

ProtocolloBB84

Questa classe è responsabile nel mappare i passi del protocollo BB84 in dei metodi, i quali interagiscono con le parti Sender e Receiver. Inoltre contiene i metodi che permettono di calcolare le probabilità stimate e le probabilità effettive, descritte nel paragrafo 6.1.2.

- Costruttore

```
public ProtocolloBB84(Channel c) {  
    this.c = c;  
    this.s = c.getSender();  
    this.r = c.getReceiver();  
    if(c instanceof ChannelEavesdropper){  
        eveActive = true;  
        this.e = ((ChannelEavesdropper) c).getEve();  
    }  
}
```

Prende in input il canale Channel o ChannelEavesdropper, in modo tale da permettere l'utilizzo della modalità con e senza Eve.

- Metodi

```

public void codifyAndSend() {
    Engine.setDefaultSchema();
    s.creationRawKey();
    s.creationCasualBase();

    int i=0;
    while( i < s.getNQubits()) {
        s.sendFotone();
        i++;
    }
}

```

Questo metodo permette di simulare la codifica e l'invio dei fotoni nel canale da parte del mittente; viene impostato lo schema da utilizzare, cioè le basi coniugate, invocando il metodo statico setDefaultSchema() della classe Engine; successivamente vengono effettuate delle chiamate sull'oggetto Sender utili a creare la raw key, creationRawKey(), le basi casuali, creationCasualBase(), e infine vengono polarizzati ed inviati i fotoni nel canale, sendFotone(), in base al numero di qubit assegnati.

Un esempio di come viene calcolata una probabilità, ad esempio che Eve non viene rilevato:

```

public double probabilitàStimataEveNonRilevato() {
    double eve_perc;
    if(isEveActive())eve_perc =
        (int)e.getEVE_INTERCEPT()/100.00;
    else eve_perc = 0;

    int numeroBitComparati =
        (int) Math.round((s.getNQubits()/2.0)*
                         c.getBIT_COMPARE() /100);
    double x = 1-(eve_perc/4.0);
    return Math.pow(x, numeroBitComparati);
}

```

Engine

Questa è una classe di utilità contenente metodi statici. Viene utilizzata per effettuare operazioni sugli array , restituire valori casuali o effettuare controlli di uguaglianza. Viene utilizzata principalmente dalla classe Sender e Receiver ad esempio per estrarre i bit dalla sifting key, per comparare i bit di controllo, simulare strumenti di polarizzazione/misurazione ecc...

- Metodi

```

public static Fotone polarization(int bit, char base) {
    if(base == s.getBase1().getCode()) {
        if(bit == 0)
            return new Fotone(s.getBase1().getFotone0().getSimbolo(),
                               s.getBase1().getFotone0().getAngolo());
        if(bit == 1)
            return new Fotone(s.getBase1().getFotone1().getSimbolo(),
                               s.getBase1().getFotone1().getAngolo());
    }
    if(base == s.getBase2().getCode()) {
        if(bit == 0)
            return new Fotone(s.getBase2().getFotone0().getSimbolo(),
                               s.getBase2().getFotone0().getAngolo());
        if(bit == 1)
            return new Fotone(s.getBase2().getFotone1().getSimbolo(),
                               s.getBase2().getFotone1().getAngolo());
    }
    return null;
}

```

Questo metodo statico è responsabile delle polarizzazioni di un fotone, codificando il bit ricevuto in input con la relativa base; il riferimento s è un oggetto di tipo Schema; restituisce in output il Fotone.

```

public static int detection(Fotone f, Character base) {
    if(s.getBase1().getCode() == base) {
        if(s.getBase1().checkFotoneBase(f.getSimbolo()))
            return s.getBase1().getFotone(f.getSimbolo()).getQubit();
        else return randomBit();
    }

    if(s.getBase2().getCode() == base) {
        if(s.getBase2().checkFotoneBase(f.getSimbolo()))
            return s.getBase2().getFotone(f.getSimbolo()).getQubit();
        else return randomBit();
    }
    return -99;
}

```

Questo metodo statico è responsabile delle misurazioni di un fotone, utilizzando una base; il riferimento s è un oggetto di tipo Schema; restituisce in output un intero, ovvero il bit decodificato; il metodo statico randomBit() restituisce casualmente un bit tra 0 e 1;

Workflow: codifica, invio fotoni e lettura

Come anticipato all'inizio, vediamo il workflow della codifica e invio dei fotoni da parte di Alice e la lettura da parte di Bob attraverso il canale quantistico.

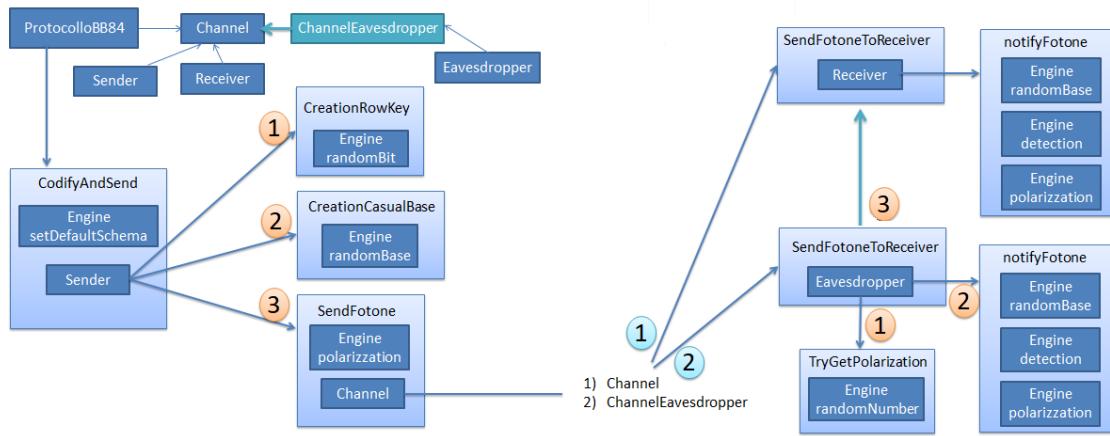


Figura 6. 1 - illustrazione del workflow

6.3 Esempi di scenari principali e analisi

In questo paragrafo verranno simulati e descritti i principali scenari possibili, mostrando gli screenshot dell'esecuzione del tool.

Gli scenari considerati sono:

- Scenario 1 – scambio senza eavesdropping
- Scenario 2 – scambio con eavesdropping livello 5
- Scenario 3 – scambio con eavesdropping livello 1

L'interfaccia iniziale presentata quando viene lanciato il programma è la seguente:

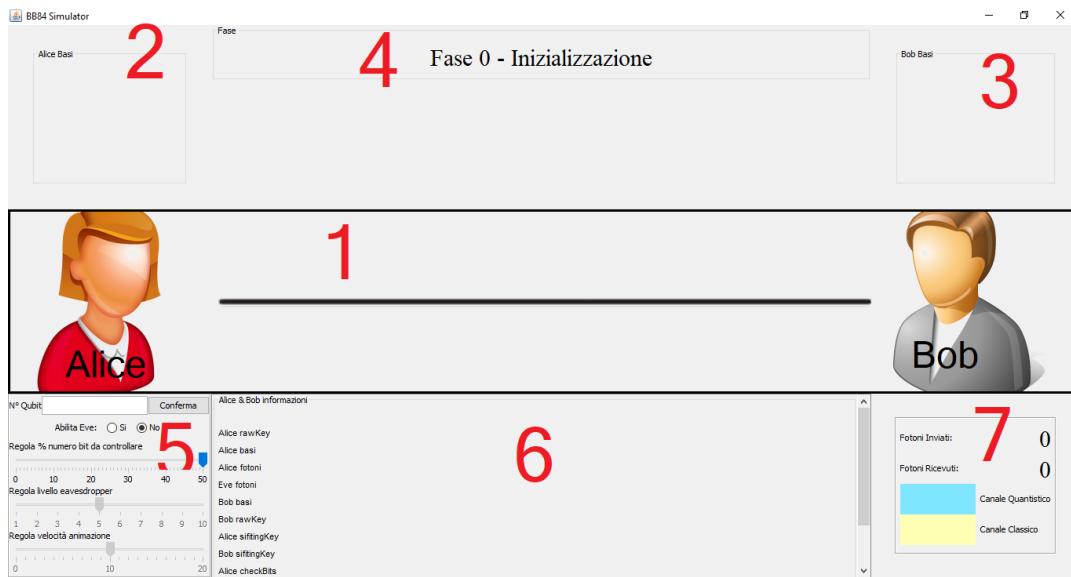


Figura 6. 2 - schermata iniziale del BB84 Simulator

- 1: è il canale di comunicazione quantistico/classico a seconda della fase in esecuzione; agli estremi troviamo Alice e Bob.
- 2-3: sono dei contenitori che contengono le scelte delle basi (private) che effettueranno Alice e Bob nelle varie fasi;
- 4: un display che rappresenta la fase in esecuzione;
- 5: pannello delle impostazioni dei parametri necessari per l'esecuzione, vale a dire il numero di qubit da spedire, abilitare eve o meno, la percentuale dei bit da controllare, il livello di eavesdropping e uno slider per regolare la velocità di esecuzione dell'animazione.
- 6: display che mostra le informazioni raccolte su Alice e Bob che verrà aggiornata durante l'esecuzione del protocollo;
- 7: pannello che contiene alcuni contatori e la legenda per indicare quando la comunicazione sta avvenendo sul canale quantistico o quello classico.

Il passaggio tra le varie fasi è regolato da un pulsante posto nel riquadro al centro della schermata:



Figura 6. 3 - screenshot display della fase successiva

La schermata finale mostra un messaggio se lo scambio è avvenuto con successo o meno, inoltre è possibile visualizzare alcune informazioni sulla comunicazione avvenuta come le lunghezze delle varie chiavi e le probabilità descritte nel paragrafo 6.1.2.

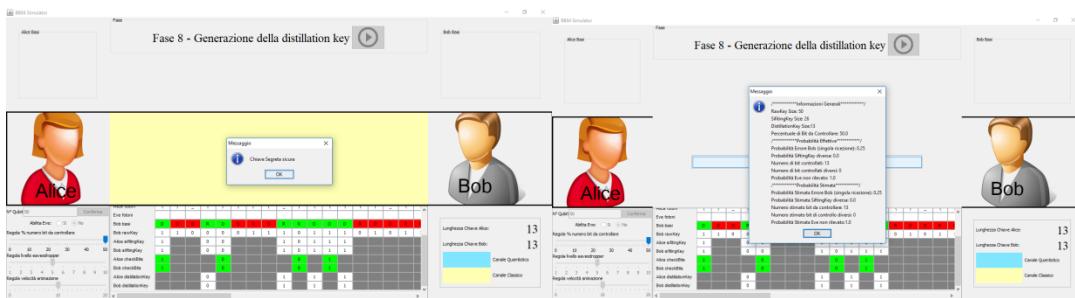


Figura 6. 4 - Schermata finale del BB84 Simulator

Quando viene selezionata la modalità con eavesdropping, viene aggiunto un ulteriore pannello contenente la figura di Eve, la tabella con le informazioni

raccolte su Eve e un riquadro dedicato alla scelta delle basi per effettuare le misurazioni sul canale quantistico.



Figura 6. 5 - screenshot display di Eve nella modalità con eavesdropping

6.3.1 Scenario 1 – Scambio senza eavesdropping

Vediamo adesso uno scenario in cui non vi è la presenza di Eve nell'intervenire sul canale o meno. L'aspettativa è che Alice e Bob riescano a generare una chiave segreta sicura.

Fase 0 - Inizializzazione

Impostiamo i valori iniziale scegliendo il numero di qubit da inviare impostato a 50, la percentuale dei bit da controllare 50% (default) e scegliamo di non abilitare Eve (default); clicchiamo conferma.

Una volta premuto il tasto conferma ci troviamo difronte un messaggio che riporta le varie probabilità stimate calcolate in base ai parametri inseriti, le quali vengono riportate anche alla fine dell'esecuzione del protocollo.

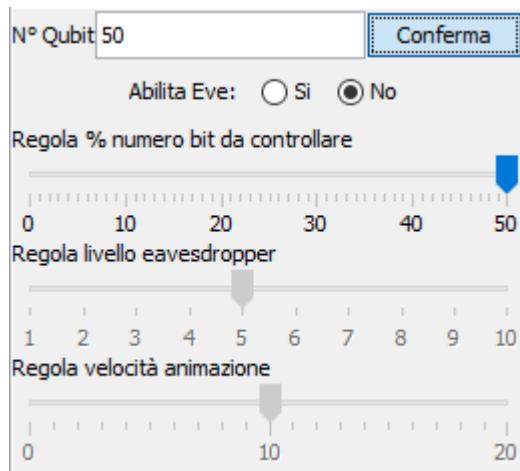


Figura 6. 6 - Pannello per impostare i settaggi iniziali

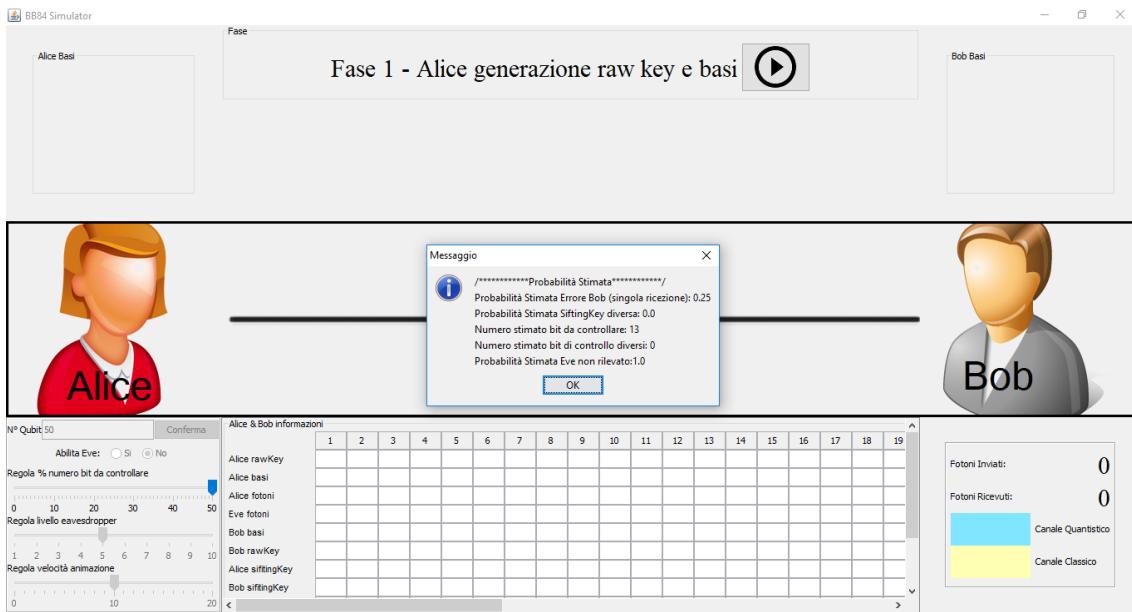


Figura 6. 7 - Schermata iniziale senza eavesdropping

Come si può notare nella parte centrale alta della schermata è presente la fase e il relativo bottone per esegirla.

Fase 1 – Alice generazione raw key e basi

Dopo aver premuto il pulsante, verrà generata in maniera casuale la raw key di alice di lunghezza 50 e le relative basi di polarizzazione da utilizzare per ciascun bit, andando ad aggiornare la tabella delle informazioni di Alice e Bob.

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	0	1	0	0	0	0	0	1	0	1	1	1	1	0	1	1	0	1
Alice basi	D	R	R	R	D	R	D	R	R	R	D	D	D	D	R	R	D	R	R
Alice fotoni																			
Eve fotoni																			
Bob basi																			
Bob rawKey																			
Alice siftKey																			
Bob siftKey																			

Figura 6. 8 - tabella contenente la raw key e le basi generate

Si può passare alla seconda fase.

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

Avviando la seconda fase, 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.

In alto alle figure delle parti vengono riportate la basi utilizzate per la polarizzazione/misurazione dei fotoni.

L'indicatore (background giallo in tabella) fa riferimento al fotone in transito.

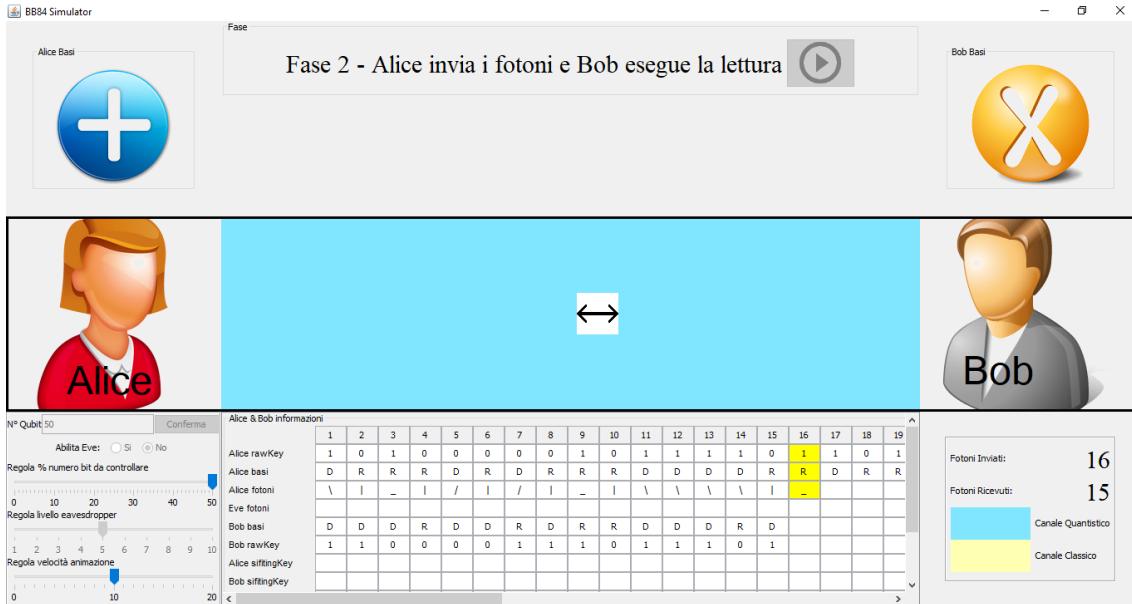


Figura 6.9 - Esecuzione dell'invio dei fotoni

Dopo aver inviato tutti i fotoni è possibile passare alla fase successiva.

Fase 3 – Bob invia le sue basi ad Alice

Avviando la terza fase, l'animazione simula l'invio della 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 man mano che le riceve:

- background rosso: non coincidono;
- background verde: coincidono.

L'indicatore (background giallo in tabella) fa riferimento alla base in transito.

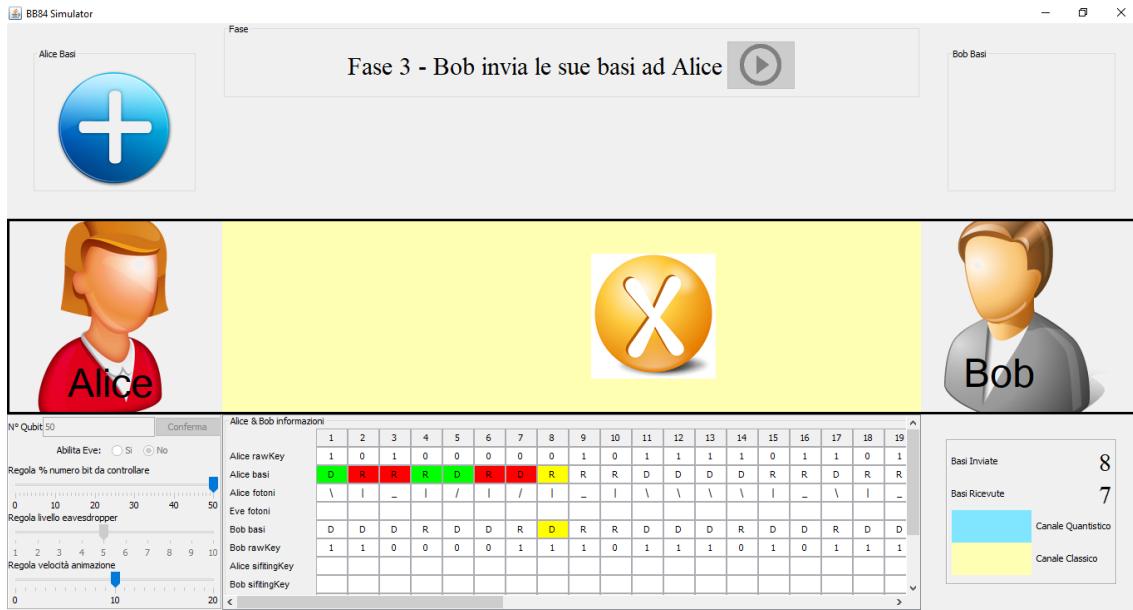


Figura 6. 10 - Esecuzione dell'invio delle basi ad Alice

Dopo aver inviato tutti le basi è possibile passare alla fase successiva.

Fase 4 – Alice invia le sue basi a Bob

Avviando la quarta fase, 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.

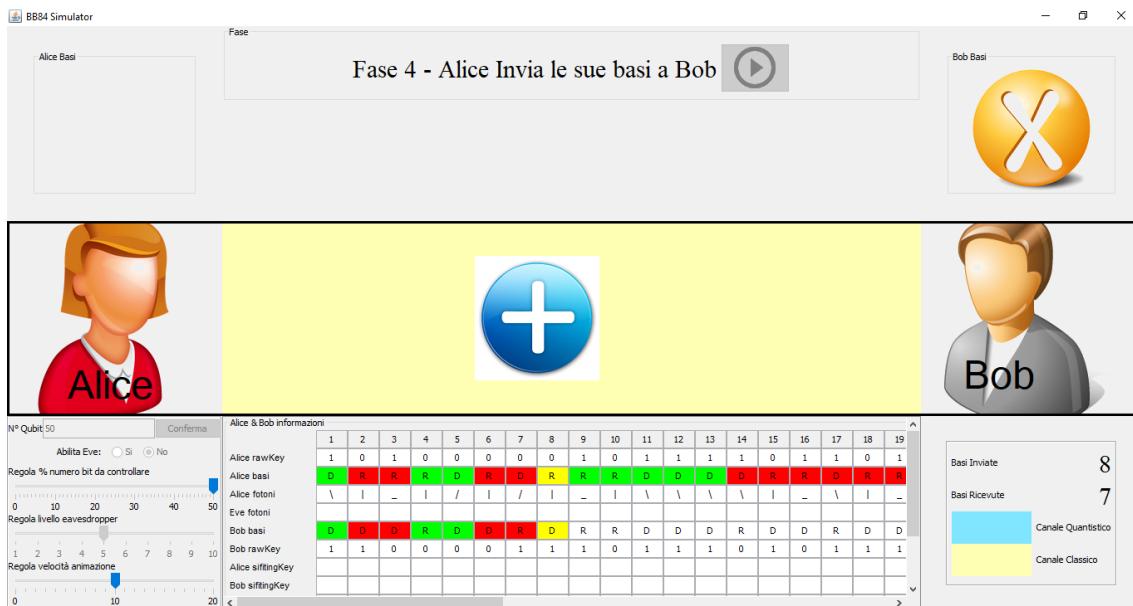


Figura 6. 11 - Esecuzione dell'invio delle basi a Bob

Dopo aver inviato tutti le basi è possibile passare alla fase successiva.

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.

Nel caso che stiamo considerando le sifting key generate coincidono in quanto non c'è alcuna presenza di Eve in gioco.

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

Figura 6. 12 - tabella che mostra la generazione della sifting key

Fase 6 e 7 – Alice (Bob) invia i suoi bit di controllo a Bob (Alice)

Per semplicità riportiamo entrambe le fasi in quanto risultano essere simili.

Viene avviata la sesta (settima) fase: 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%, per cui ci aspettiamo che il numero di bit da controllare sia la metà della lunghezza della sifting key.

L'indicatore (background giallo in tabella) fa riferimento al bit in transito.

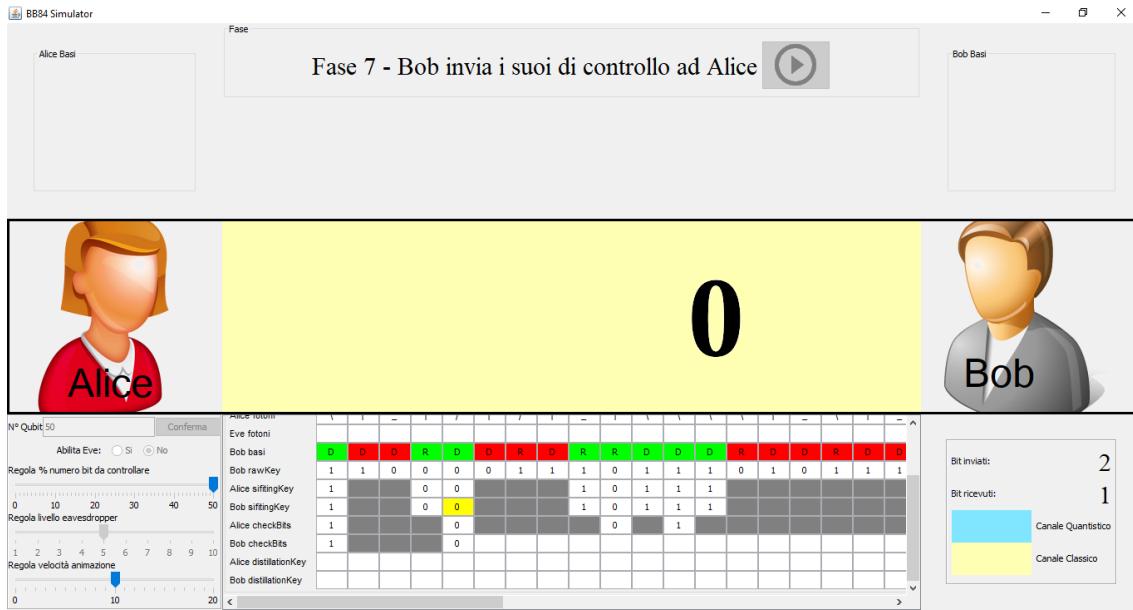


Figura 6. 13 - Esecuzione dell'invio dei bit di controllo ad Alice

Fase 8 – Generazione della distillation key

Alice e Bob controllano se i bit inviati e ricevuti coincidono; nel nostro caso non ci sono discrepanze, cioè non ci sono bit differenti (background verde), in quanto Eve non è presente.

Sia Alice che Bob generano la propria distillation key, scartando dalla sifting key i bit di controllo inviati. Il tool mostrato un messaggio che la chiave segreta è sicura, infatti risultano essere uguali. Il protocollo è terminato.

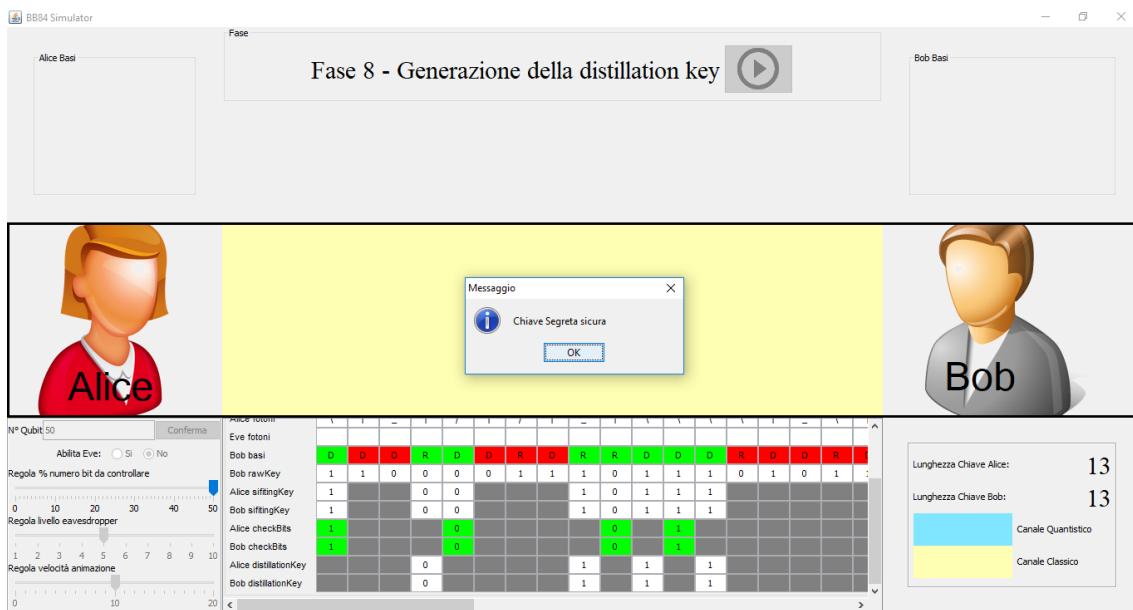


Figura 6. 14 – Schermata finale della generazione della chiave segreta andata a buon fine

Analisi

A fine esecuzione del protocollo, cliccando sul bottone “mostra info” ci viene mostrato un messaggio contenente:

- informazioni generali: le varie lunghezze delle chiavi e i settaggi utilizzati;
- le probabilità effettive: ovvero le probabilità calcolare a posteriori, dopo l’esecuzione del protocollo;
- le probabilità stimate: ovvero le probabilità calcolare a priori, prima dell’esecuzione del protocollo;

Confrontiamo le probabilità stimate (a priori) ed effettive (a posteriori):

- **Probabilità di errore di Bob:** non essendoci nessuna intrusione queste due coincidono;
- **Probabilità sifting key diversa:** non essendoci nessuna intrusione queste due coincidono ed inevitabilmente è posta a 0.
- **Numero di bit da controllare:** la lunghezza della sifting key reale (26) differisce soltanto di 1 dalla media, cioè la metà della raw key (25); da ciò ne deriva che il numero dei bit da controllare, che è fissato al 50% della sifting key, coincide.
- **Numero di bit da controllare diversi:** non essendoci nessuna intrusione queste due coincidono ed inevitabilmente è posta a 0.
- **Probabilità di non rilevamento di Eve:** non essendoci nessuna intrusione queste due coincidono ed inevitabilmente è posta a 1.

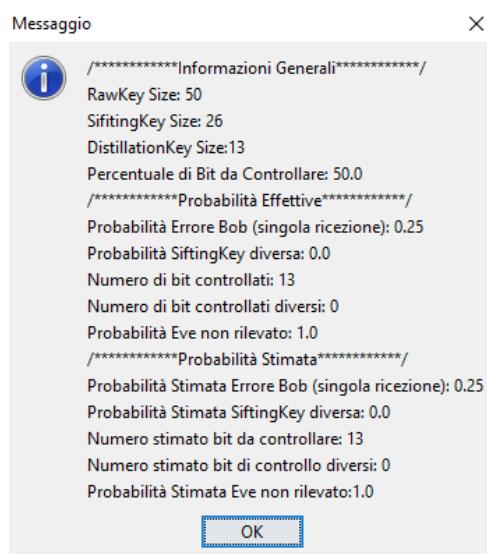


Figura 6.15 - Messaggio contenente le informazioni sull'esecuzione

6.3.2 Scenario 2 – Scambio con eavesdropping livello 5

Vediamo adesso uno scenario in cui la probabilità di Eve è equilibrata nell'intervenire sul canale o meno. L'aspettativa è che Eve con le impostazioni utilizzate venga rilevato.

Fase 0 - Inizializzazione

Impostiamo i valori iniziale scegliendo il numero di qubit da inviare impostato a 50, la percentuale dei bit da controllare 50% (default) , scegliamo di abilitare Eve , regoliamo il livello di Eve a 5 (default); clicchiamo conferma.

Una volta premuto il tasto conferma ci troviamo difronte un messaggio che riporta le varie probabilità stimate calcolate in base ai parametri inseriti.



Figura 6. 16 - pannello per impostare i settaggi iniziali

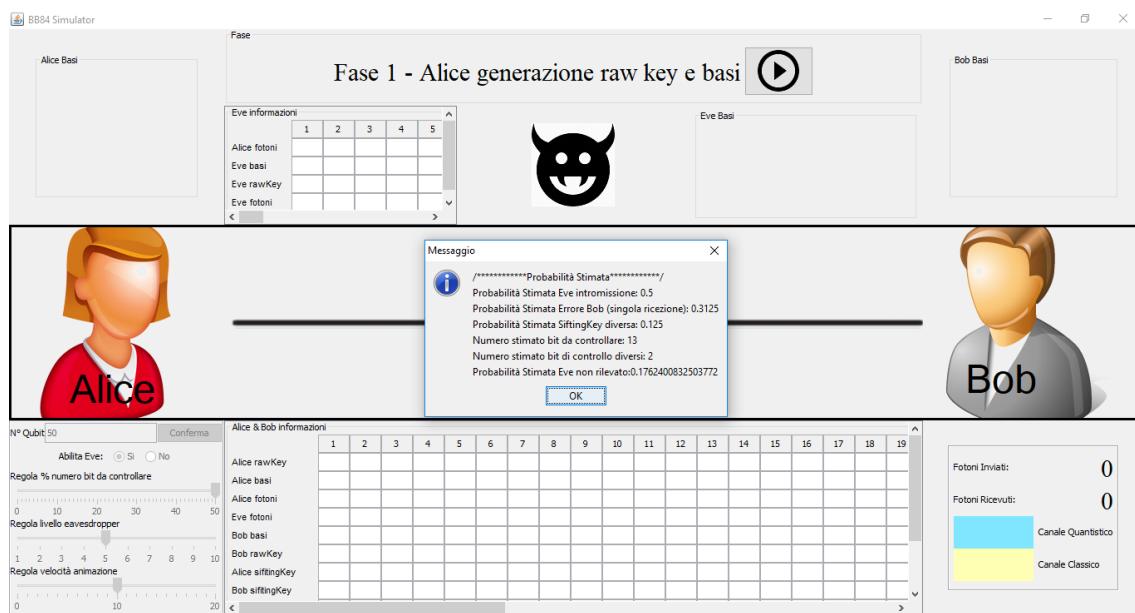


Figura 6. 17 - Schermata iniziale della modalità con eavesdropping

Come si può notare nella parte centrale alta della schermata è presente la fase e il relativo bottone per eseguirla. Inoltre viene aggiunto la figura di Eve, la tabella contenente le informazioni su Eve e un riquadro dedicato alle sue basi per effettuare le misurazioni sul canale quantistico.

Fase 1 – Alice generazione raw key e basi

Dopo aver premuto il pulsante, verrà generata in maniera casuale la raw key di alice di lunghezza 50 e le relative basi di polarizzazione da utilizzare per ciascun bit. Queste informazioni vengono inserite nella tabella delle informazioni di Alice e Bob in basso.

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		R	D	D	D	R	R	R	D	R	D	D	R	R	D	R	D	R	D	D
Alice fotoni																				
Eve fotoni																				
Bob basi																				
Bob rawKey																				
Alice siftingKey																				
Bob siftingKey																				

Figura 6. 18 - tabella contenente la raw key e le basi generate

Si può passare alla seconda fase.

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

Viene avviata la seconda fase: 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. Siccome vi è la presenza di Eve i fotoni possono essere intercettati, la simulazione mostra due casi, in base se Eve interviene o meno:

- **Eve non interviene**

Il fotone transita regolarmente da Alice a Bob senza essere intercettato.

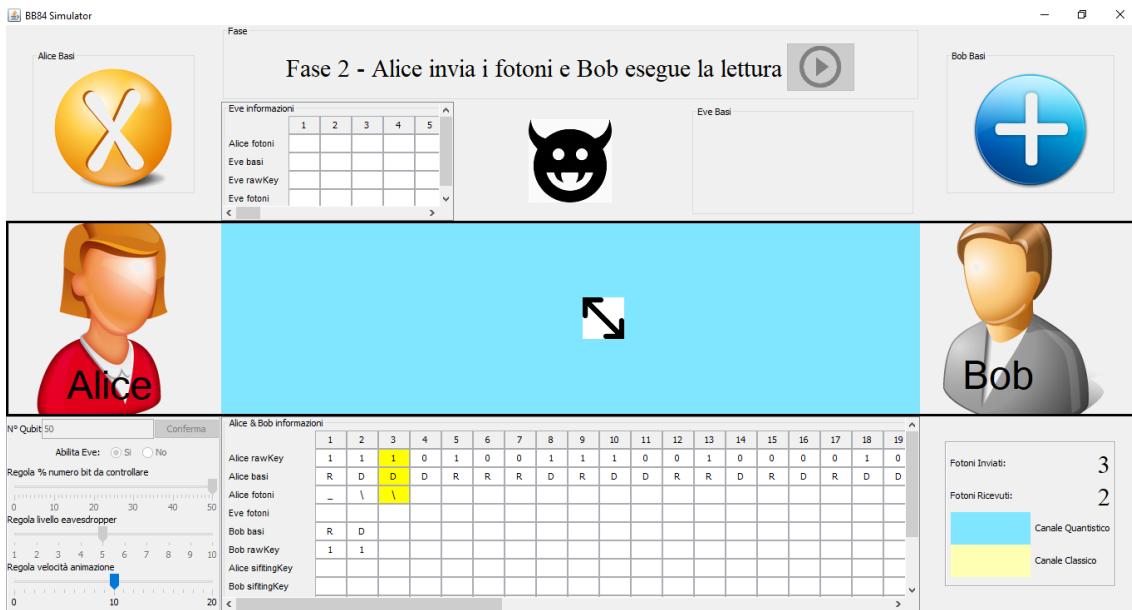


Figura 6.19 - Esecuzione dell'invio dei fotoni

In alto alle figure delle parti vengono riportate la basi utilizzate per la polarizzazione/misurazione dei fotoni.

L'indicatore (background giallo in tabella) fa riferimento al fotone in transito.

- **Eve interviene**

Il fotone viene intercettato da Eve, in questo caso verrà mostrato un'immagine (l'occhio) per simulare che Eve vuole misurando il fotone in transito.

Quando Eve effettua la misurazione il fotone viene ripolarizzato secondo la base scelta da Eve, possono esserci due casi:

Caso 1 – 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; Dopodichè viene inoltrato sul canale a Bob mantenendo la polarizzazione originaria del fotone.

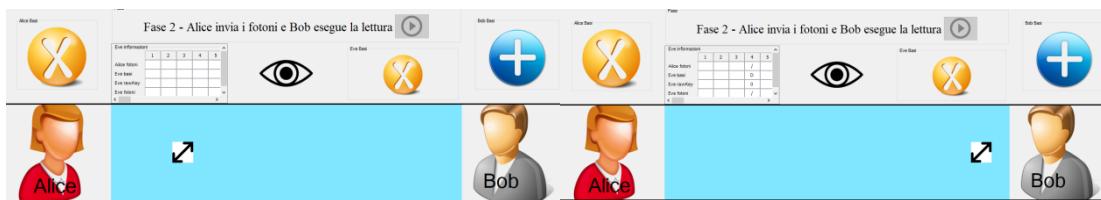


Figura 6.20 - Esecuzione della misurazione di un fotone da parte di Eve con base giusta

Caso 2 – 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; Dopodichè viene inoltrato sul canale a Bob cambiando la polarizzazione originaria del fotone.

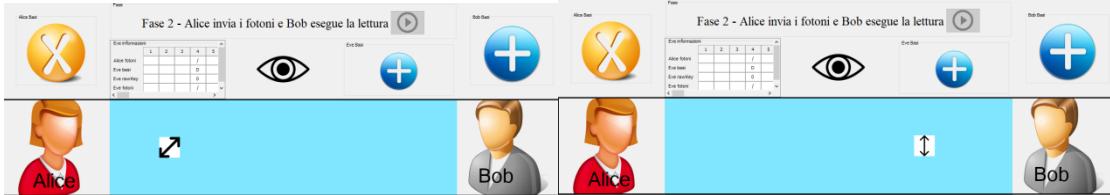


Figura 6. 21 - Esecuzione della misurazione di un fotone da parte di Eve con base sbagliata

Ogni qual volta Eve effettua una misurazione viene aggiornata la tabella relativa alle sue informazioni. Dopo aver inviato tutti i fotoni è possibile passare alla fase successiva.

Fase 3 – Bob invia le sue basi ad Alice

Viene avviata la terza fase: l'animazione simula l'invio della 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 man mano che le riceve:

- background rosso: non coincidono;
- background verde: coincidono.

L'indicatore (background giallo in tabella) fa riferimento della base in transito.

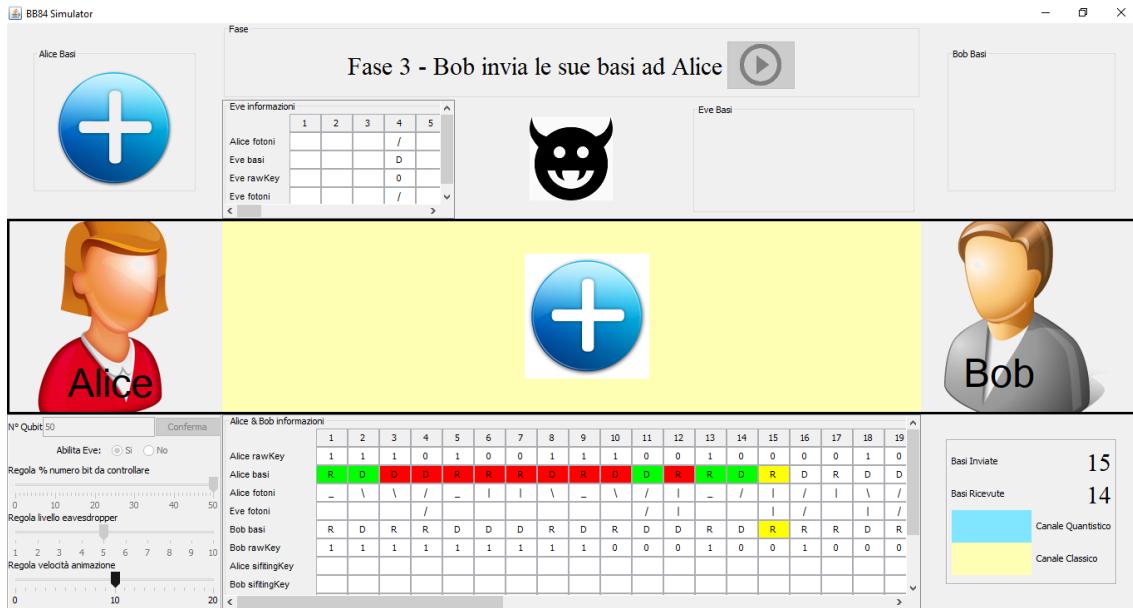


Figura 6. 22 - Esecuzione dell'invio delle basi ad Alice

Dopo aver inviato tutti le basi è possibile passare alla fase successiva.

Fase 4 – Alice invia le sue basi a Bob

Viene avviata la quarta fase: 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.

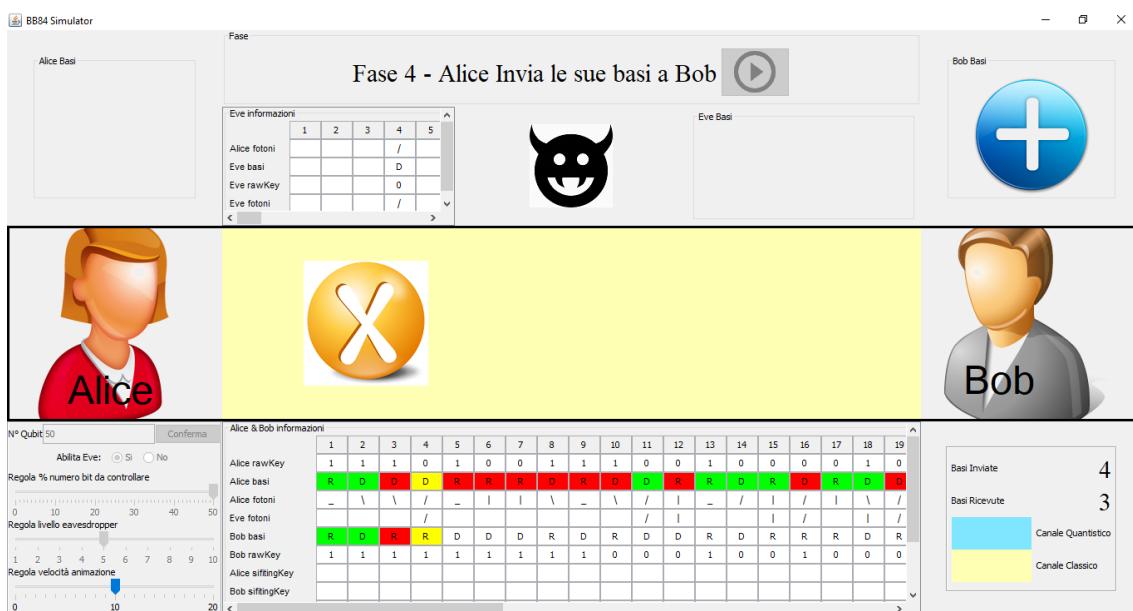


Figura 6. 23 - Esecuzione dell'invio delle basi a Bob

Dopo aver inviato tutti le basi è possibile passare alla fase successiva.

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.

Nel caso che stiamo considerando le sifting key generate non è detto che coincidono in quanto c'è la presenza di Eve in gioco; infatti come si vede dalla seguente immagine non coincidono (ultimo bit visibile) ed inoltre notiamo l'intervento di Eve.

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		R	D	D	D	R	R	R	D	R	D	D	R	R	D	R	D	R	D	D
Alice fotoni		-	\	\	/	-			\	-	\	/		-	/		/		\	/
Eve fotoni					/							/					/			/
Bob basi		R	D	R	R	D	D	D	R	D	R	D	D	R	D	R	R	R	D	R
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	

Figura 6. 24 - tabella che mostra la generazione della sifting key

Fase 6 e 7 – Alice (Bob) invia i suoi bit di controllo a Bob (Alice)

Per semplicità riportiamo entrambe le fasi in quanto risultano essere simili.

Viene avviata la sesta (settima) fase: 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%, per cui ci aspettiamo che il numero di bit da controllare sia la metà della lunghezza della sifting key.

L'indicatore (background giallo in tabella) fa riferimento al bit in transito.



Figura 6. 25 - Esecuzione dell'invio dei bit di controllo ad Alice

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.

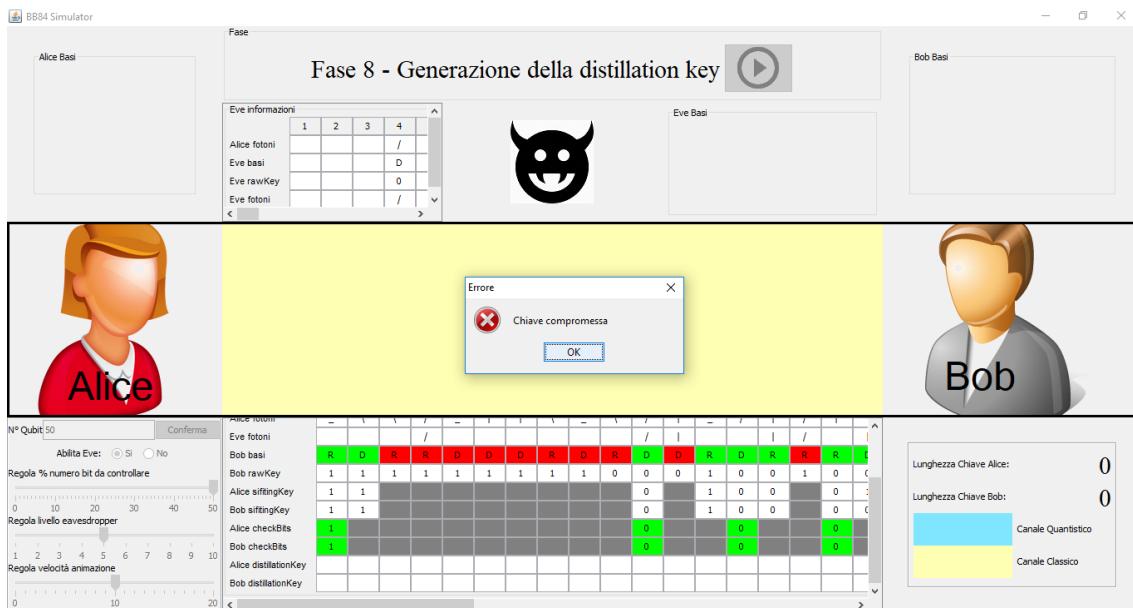


Figura 6. 26 - Schermata finale che mostra un messaggio di errore sulla generazione della chiave finale

Ciò vuol dire che è stata trovata almeno una discrepanza, cioè c'è un bit differente (background rosso).

I	-	/	/	/	/	\	/	-	/	/	/	\	I	I	\
D	R	D	R	R	R	D	R	D	R	R	D	R	R	D	R
0	1	0	0	1	0	0	0	1	0	0	0	0	0	1	0
1	0	0		0	1		1	0	0		0	0		1	1
1	0	0		0	0		1	0	0		0	0		1	0
0		0		0		1		0		0	0		1		0
0		0		0		1		0		0	0		0		0

Figura 6.27 - tabella che mostra dove i bit di controllo differiscono

Come si può notare in figura anche altri bit erano differenti della sifting key, soltanto che non sono stati estratti come bit di controllo essendo di posizione pari.

Analisi

A fine esecuzione del protocollo, cliccando sul bottone “mostra info” ci viene mostrato un messaggio contenente:

- informazioni generali: le varie lunghezze delle chiavi e i settaggi utilizzati;
- le probabilità effettive: ovvero le probabilità calcolate a posteriori, dopo l’esecuzione del protocollo;
- le probabilità stimate: ovvero le probabilità calcolate a priori, prima dell’esecuzione del protocollo.

Confrontiamo le probabilità stimate (a priori) ed effettive (a posteriori):

- **Probabilità di intromissione di Eve:** coincidono perfettamente in quanto il numero di interventi di Eve (25) sono esattamente la metà dei fotoni inviati (50), per cui risulta uguale allo 0.5 come impostato inizialmente.
- **Probabilità di errore di Bob:** per le motivazioni precedenti anche queste due coincidono;
- **Probabilità sifting key diversa:** per le motivazioni precedenti anche queste due coincidono;
- **Numero di bit da controllare:** la lunghezza della sifting key reale (24) differisce soltanto di 1 dalla media, cioè la metà della raw key (25); Il numero di bit da controllare è calcolato come il 50% della sifting key, da ciò ne deriva che il numero dei bit stimati da controllare (13) viene rivalutato (12) in quanto la sifting key reale è più corta.

- **Numero di bit da controllare diversi:** per le motivazione precedente anche qui c'è stata una rivalutazione;
- **Probabilità di non rilevamento di Eve:** la probabilità effettiva aumenta rispetto a quella stimata in quanto il numero di bit effettivamente controllati (12) è inferiore a quelli stimati (13).

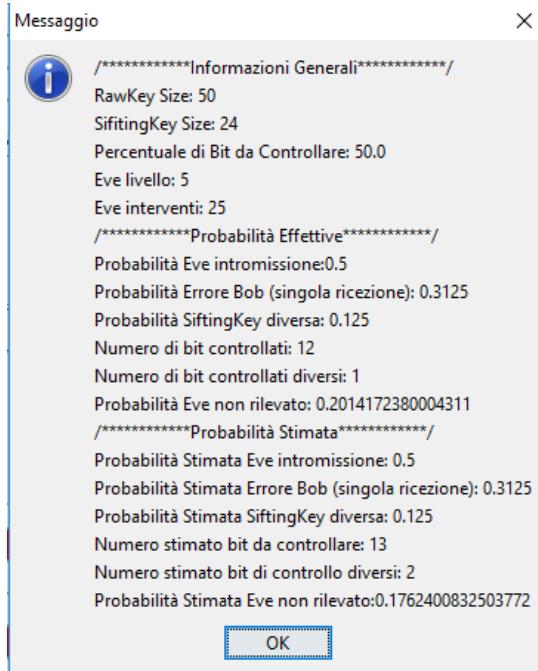


Figura 6. 28 - Messaggio contenente le informazioni sull'esecuzione

Con i valori impostati Eve è stato rilevato in quanto il numero di bit da controllare è stato sufficiente per rilevarlo siccome interviene sul canale con la probabilità stimata.

6.3.3 Scenario 3 – Scambio con eavesdropping livello 1

Vediamo adesso uno scenario in cui la probabilità di Eve è molto bassa di intervenire sul canale. L'aspettativa è che Eve non venga rilevato.

Si riporteranno gli screenshot soltanto dell'analisi finale per commentarli.

Fase 0 - Inizializzazione

Impostiamo i valori iniziale scegliendo il numero di qubit da inviare impostato a 50, la percentuale dei bit da controllare 50% (default), scegliamo di abilitare Eve , regoliamo il livello di Eve a 1; clicchiamo conferma.

Una volta premuto il tasto conferma ci troviamo difronte un messaggio che riporta le varie probabilità stimate calcolate in base ai parametri inseriti.

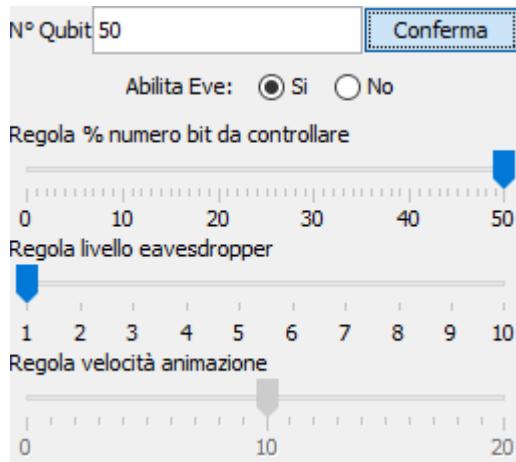


Figura 6. 29 - panello per impostare i settaggi iniziali

Analisi

Viene mostrato un messaggio che la chiave è compromessa.

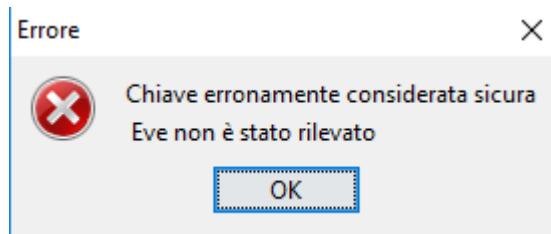


Figura 6. 30 - Messaggio di errore di mancato rilevamento di eavesdropping

A fine esecuzione del protocollo, cliccando sul bottone “mostra info” ci viene mostrato un messaggio contenente:

- informazioni generali: le varie lunghezze delle chiavi e i settaggi utilizzati;
- le probabilità effettive: ovvero le probabilità calcolate a posteriori, dopo l'esecuzione del protocollo;
- le probabilità stimate: ovvero le probabilità calcolate a priori, prima dell'esecuzione del protocollo.

Confrontiamo le probabilità stimate (a priori) ed effettive (a posteriori):

- **Probabilità di intromissione di Eve:** il numero di interventi di Eve (3) fa sì che la probabilità di intromissione effettiva si abbassi rispetto a quella stimata in quanto il numero di interventi di Eve stimato è calcolato come il 10 % (livello di Eve scelto 1) del numero di fotoni inviati (50).

- **Probabilità di errore di Bob:** per le motivazione precedente anche queste due coincidono;
- **Probabilità sifting key diversa:** per le motivazioni precedenti anche queste due coincidono;
- **Numero di bit da controllare:** la lunghezza della sifting key reale (27) differisce soltanto di 2 dalla media, cioè la metà della raw key (25); Il numero di bit da controllare è calcolato come il 50% della sifting key, da ciò ne deriva che il numero dei bit stimati da controllare (13) viene rivalutato (14) in quanto la sifting key reale è più lunga rispetto la media.
- **Numero di bit da controllare diversi:** le due probabilità coincidono in quanto la probabilità di Eve di intromissione effettiva è ancora più bassa.
- **Probabilità di non rilevamento di Eve:** la probabilità effettiva aumenta rispetto a quella stimata in quanto Eve interviene meno volte rispetto a quelle stimate.

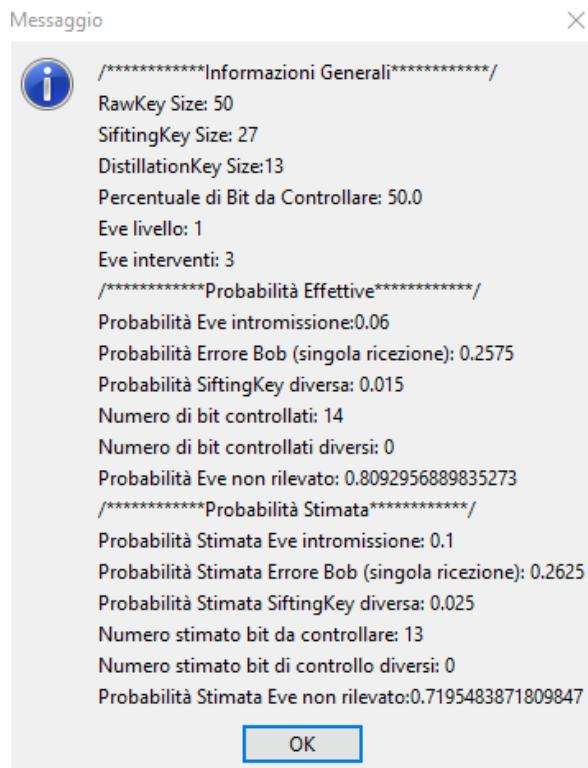


Figura 6. 31 - Messaggio contenente le informazioni sull'esecuzione

Con i valori impostati Eve non è stato rilevato in quanto il numero di bit da controllare non è sufficiente a rilevarlo siccome interviene con una bassa probabilità sul canale. Una soluzione è quella di aumentare il numero di qubit iniziale.

Conclusioni

Il seguente documento ha cercato di introdurre il lettore nel mondo della crittografia quantistica e QKD.

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. In ogni caso, 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. Questo potrebbe essere lo stimolo principale per perseguire il miglioramento della tecnologia QKD e la ricerca della QN.

Gli argomenti trattati risultano essere estremamente utile per comprendere il tool sviluppato, il quale permette di avere una visione pratica dell'esecuzione del protocollo BB84.

Dei possibili sviluppi futuri del tool BB84 Simulator possono essere:

- simulare perdite di informazioni all'interno del canale quantistico;
- simulare tecniche di correzione degli errori e amplificazione della privacy.

Bibliografia

- Wikipidia, "Storia della crittografia",
https://it.wikipedia.org/wiki/Storia_della_crittografia
- Jonathan Katz and Yehuda Lindell, "Introduction to Modern Cryptography"
- D. Deutsch, A. Ekert, "Quantum Computation, Physics World"
- C. E. Shannon, "Communication theory of secrecy systems"
- S. Singh, Codici e segreti - The code book
- C. Bennett, G. Brassard, A. Ekert: Crittografia quantistica
- Digilander , "I prncipi della meccanica quantistica",
<http://digilander.libero.it/syntmentis/Fisica/Quanti.html>
- C. Bennett, F. Bassette, G. Brassard, L. Salvail e J. Smolin: "Experimental Quantum Cryptography Journal of Cryptology"
- Swissquantum "Raw Key, Raw Key Exchange, Raw Sifitng"
<http://www.swissquantum.com/>
- Aniello Castiglione, Gerardo Maiorano, "Distribuzione quantistica a chiave pubblica", http://www.di-srv.unisa.it/~ads/corso-security/www/HTML/QUANTUM_CRYPT/node3.html
- N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum Cryptography"
- V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf , M. Dusek, N. Lutkenhaus , M. Peev, "The Security of Practical Quantum Key Distribution"
- D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres", <http://iopscience.iop.org/1367-2630/11/7/075003>
- M. Dianati and R. Alleaume , "Architecture of the SECOQC Quantum Key Distribution network"
- C. Elliot, "The DARPA Quantum Network"
- C. Elliot, "Building the Quantum Network"
- Wikipedia, Quantum Network,
https://en.wikipedia.org/wiki/Quantum_network
- B. Schneier, Interview,
http://www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016
- B. Schneier, "Schneier on Security"

- K. G. Paterson, F. Piper and R. Schack, “Quantum cryptography: a practical information security perspective”
- S. Ghernaoutie-Helie, I. Tashi, Th. Langer, C. Monyk, “SECOQC Business White Paper”,
http://www.secoqc.net/downloads/SECOQC_Business_Whitepaper_01b.pdf
- V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf , M. Dusek, N. Lutkenhaus , M. Peev, “The Security of Practical Quantum Key Distribution”
- D. Stebila, M. Mosca, N. Lutkenhaus, “The case for quantum key distribution”
- P. Villoresi, R.Ursin, A. Zeilinger “Single photons from a satellite: quantum communication in space”,
<http://spie.org/x33629.xml?pf=true&ArticleID=x33629>