UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea Magistrale
in Ingegneria Informatica

Relazione di Sicurezza Informatica

Quantum-Based Security

Protocolli e sistemi totalmente quantistici contro un attaccante con tecnologie quantistiche arbitrarie

Professore: Chiar.mo Prof. Federico Cerutti

Studenti:
Alberto Barbieri 719576
Edoardo Coppola 719599
Andrea Fiori 719219

Anno Accademico 2021/2022

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

Per numerosi anni, i crittografi hanno sperimentato tecniche di (de)cifratura per creare metodi efficaci e robusti per mettere in sicurezza la comunicazione tra più entità legittime. Uno di questi è la crittografia tradizionale (o classica), che consiste nella condivisione di un messaggio tra due enti attraverso un canale insicuro per natura (ad esempio Internet).

Il messaggio condiviso (*plaintext*) deve essere spedito da un mittente a un destinatario senza l'intervento di terze parti malintenzionate. Per prevenire potenziali impersonificazioni o azioni di *eavesdropping*, il mittente cifra un testo in chiaro X, che diviene un *chipertext* C. Dall'altro lato, il destinatario riceverà il testo cifrato C per rivelare il messaggio X d'origine.

I meccanismi di crittografia classici basano la propria sicurezza sull'assunzione non dimostrata che l'attaccante debba impiegare tempi insostenibilmente lunghi per far breccia nella comunicazione (o sistema) crittografata. Tale assunzione è stata però smentita a seguito della nascita dell'algoritmo di Shor [30] che dimostra la possibilità di scardinare la sicurezza imposta dalla crittografia classica in tempi polinomiali se si disponi di computer quantistici sufficientemente potenti. Per questi motivi, i ricercatori hanno sviluppato da tempo nuovi protocolli crittografici basati sulle leggi della fisica (quantistica): la crittografia quantistica, infatti, applica le teorie della fisica quantistica per produrre una chiave segreta, che può essere condivisa dalle parti comunicanti. Per raggiungere tale scopo sono nati i protocolli di Quantum Key Distribution (QKD).

Il documento corrente ha come obiettivo il confronto esplicito e critico dei principali protocolli di QKD sulla base di alcune dimensioni di comparazione descritte nel capitolo 3.

Dapprima si presenteranno i teoremi e i principi su cui i protocolli di QKD basano il proprio funzionamento, quali il principio di indeterminazione, il teorema "no cloning" e l'Entanglement; a questi, si affiancheranno le descrizioni di vulnerabilità di cui i protocolli soffrono e alcuni attacchi che le sfruttano. Quindi, verranno descritte le dimensioni di comparazione sopracitate seguite dai funzionamenti dei protocolli di QKD BB84, E91, B92 e SARG04. Infine, tali protocolli saranno comparati esplicitamente tra loro, sulla base delle dimensioni individuate e di altre considerazioni tecnico-pratiche.

Capitolo 2

Background

In questo capitolo affronteremo i concetti base necessari alla comprensione del funzionamento dei protocolli quantistici di distribuzione delle chiavi, degli attacchi che possono essere portati a termine contro tali protocolli e dei meccanismi di difesa.

2.1 Principi e teoremi di base

Di seguito si mostrano i principi e teoremi essenziali allo scopo della comprensione dei protocolli di QKD.

2.1.1 Principio di Heisenberg

Uno dei principi fondamentali della fisica quantistica è il principio di indeterminazione di Heisenberg (PIH). Esso afferma che, in meccanica quantistica, solo una proprietà di una coppia di proprietà coniugate può essere misurata con precisione arbitraria. Con il termine astratto "proprietà" si indicano, ad esempio, la posizione e il momento di una particella. È dunque impossibile conoscere con precisione il momento data una misura precisa della posizione e viceversa. Quanto detto è riassunto dalla seguente formula:

$$\Delta x \cdot \Delta p_x \geq \frac{\hbar}{2}$$

Δx è l'incertezza sulla misura della posizione e Δp_x è l'incertezza sulla quantità di moto, mentre $\hbar$ è la costante di Plank ridotta, pari a $6.582 \times 10^{-16} eV \cdot s$. È facile osservare come per ottenere una misurazione precisa di x (i.e. Δx piccolo) sia necessaria una elevatissima imprecisione nella misurazione di p_X (i.e. Δp_x grande).

2.1.2 Teorema "no cloning"

Una conseguenza di PIH è il teorema "no cloning", che sottolinea l'impossibilità di creare copie identiche di un stato quantico (ad esempio momento e posizione) arbitrario. Infatti, si potrebbe pensare che sia possibile aggirare il principio di incertezza generando duplicati di uno stato quantico, così da misurare una differente proprietà coniugata per ogni copia. Tuttavia, tentare di copiare, dunque "leggere" lo stato di una particella, comporta modificare le proprietà della stessa e, di conseguenza, verrebbe a generarsi un duplicato diverso dall'originale.

2.2 Quantum entanglement

Dicasi quantum entanglement il legame che si forma tra due particelle tali che, quando una particolare proprietà viene misurata nella prima, lo stato opposto viene rilevato istantaneamente nella corrispondente particella correlata, detta "entangled". Questo è vero indipendentemente dalla distanza delle due particelle (*action at distance*); tuttavia, risulta impossibile predire a priori (prima di una misurazione) quale stato verrà osservato. Di conseguenza, è impossibile comunicare sfruttando il quantum entanglement senza un'operazione preliminare nel canale classico che dia indicazioni ad un ricevente su come effettuare la misurazione degli stati quantistici inviati.

2.3 Concetti di base sui protocolli di QKD

Il modello di base di un generico protocollo di QKD (si veda la figura 2.1) coinvolge tipicamente due parti, riferite come Alice (sender) e Bob (receiver), le quali vogliono accedere al canale di comunicazione al fine di scambiarsi informazioni in modo sicuro. Esiste inoltre un terzo ente, detto Eve (abbreviazione di eavesdropper), che si assume avere accesso al canale ed essere dotato di risorse quantistiche arbitrarie. In riferimento alla sezione 2.1, il canale di comunicazione quantistico è la fibra ottica, la particella corrisponde al fotone.

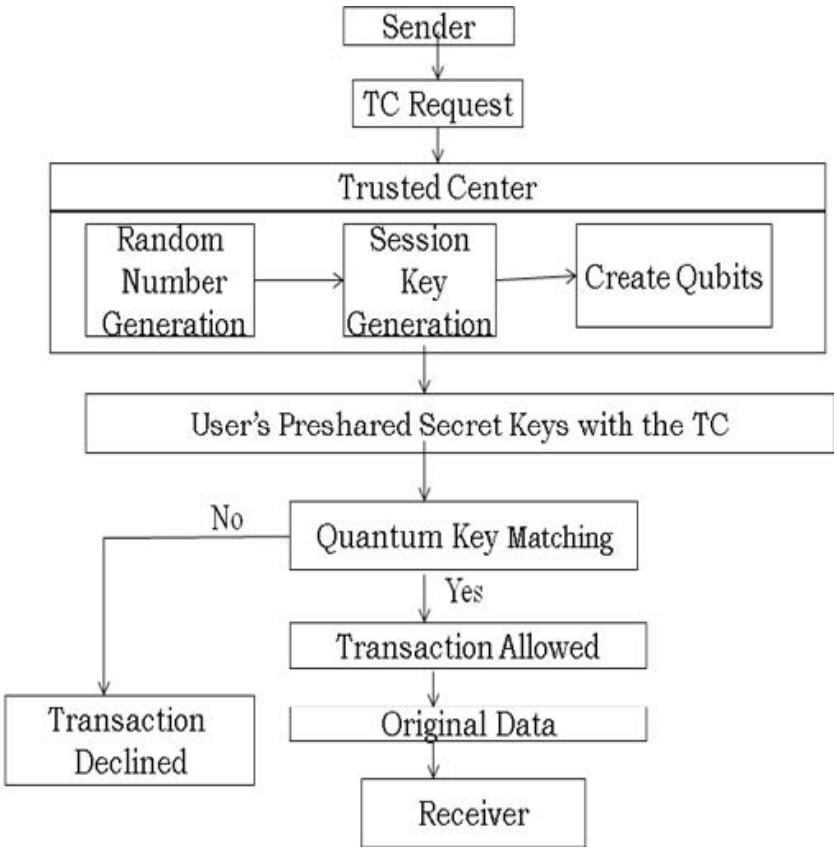

Figura 2.1: Architettura di un protocollo di QKD [17].

Nel corso della trattazione ci focalizzeremo su protocolli a chiave privata, detti anche a chiave condivisa: questa permette di cifrare il contenuto informativo che si desidera scambiare tra le due parti così da garantire *confidentiality*, ossia che eventuali malintenzionati, seppur capaci di intercettare i messaggi, non siano in grado di interpretarli. Alice e Bob conservano una copia della medesima chiave, ossia una stringa alfanumerica generata secondo i dettami

del protocollo. Il problema fondamentale risulta proprio la condivisione della chiave: di ciò si occupano i protocolli di QKD. In alcuni di questi, gli utenti ottengono la chiave segreta tramite un terzo ente, detto trusted center (TC), presentato nell'articolo [17] e di cui si riporta nella figura (2.1). Dal momento che tre parti sono coinvolte nella negoziazione della chiave di sessione, i corrispondenti protocolli sono detti three-party key distribution protocol. In caso vi siano solamente Alice e Bob, le mansioni del TC sono assorbite dalle due parti.
Le comunicazioni tra Alice e Bob avvengono mediante invio e ricezione di fotoni, opportunamente polarizzati a seconda che debbano rappresentare uno 0 o un 1 binario: tale polarizzazione è rappresentata da una combinazione lineare di stati quantistici di una base, ossia un insieme di stati tra loro ortogonali. Alcuni esempi di basi saranno illustrati nel capitolo 4. Il TC ed i partecipanti sincronizzano la base di polarizzazione attraverso una chiave segreta precondivisa. Durante la distribuzione della seconda chiave, quella di sessione, la chiave precondivisa viene combinata con una stringa random per produrre una terza chiave, che sarà utilizzata per cifrare quella di sessione. Ciò garantisce che Bob non riceva lo stesso messaggio cifrato anche a parità di chiave di sessione, poiché la stringa random varia ad ogni trasmissione. La struttura delle chiavi dipende dal protocollo in uso.

Il qubit - quantum bit - è l'unità informativa di base della comunicazione attraverso canali quantistici. Similmente al bit classico, può codificare due stati che sono determinati dalle caratteristiche fisiche della particella che rappresenta l'unità informativa. Lo stato quantistico di un qubit viene determinato, come già indicato, mediante la combinazione lineare degli stati quantistici di una base. Le basi sono determinate dai protocolli di QKD.

2.4 Vulnerabilità e attacchi ai protocolli di QKD

Come già indicato, l'idea di base dei protocolli di QKD è che Alice e Bob comunichino per mezzo di fotoni che, se opportunamente polarizzati, rappresentano la codifica di precisi bit individuati dalle due parti della comunicazione

Il PIH permette di garantire che Eve non possa misurare questi fotoni ed inoltrarli a Bob senza che ne venga alterato lo stato, perciò senza che Eve riveli la propria presenza. Dunque i protocolli di QKD possono considerarsi incondizionatamente sicuri, nel senso che se anche Eve disponesse di capacità computazionali e tempo illimitato, non riuscirebbe a scardinare la sicurezza di tali protocolli per via del fatto che essa di base sulle leggi della fisica.

Nonostante ciò, i protocolli considerati sono suscettibili agli attacchi man-in-the-middle (MitM), in cui l'eavesdropper si finge Bob nei confronti di Alice e viceversa, simultaneamente. Tale attacco risulta implausibile da prevenire, a meno di una mutua autenticazione preventiva tra le due parti. Per di più, non è immediato comprendere se la sicurezza incondizionata sia rispettabile anche in presenza di rumore o di strumentazione imperfetta (ad esempio, circuiti di generazione della chiave condivisa mal progettati).

2.4.1 Denial of Service

L'attacco Denial of Service (DoS) è una tipologia di cyber-attacco in cui l'attaccante mira a rendere i servizi offerti da un dispositivo (o da una rete di dispositivi) non disponibili. Nei canali classici, questo avviene saturando le risorse o la banda. Per quanto concerne le comunicazioni previste dai protocolli di QKD, si ha una terza opzione: è sufficiente che Eve vada a misurare le particelle in transito nel canale per alterarne lo stato e dunque impossibilitarne la corretta lettura a Bob. Risulta perciò infattibile schermarsi completamente da un attacco di questo tipo, a meno di poter impedire la presenza dell'attaccante lungo il canale di comunicazione. In alternativa, [12] dimostra che è possibile, se si dispone di fibre ottiche multi-core, passare a un secondo canale appena Eve viene rilevato.

2.4.2 Photon Number Splitting

Emettere singole particelle, nella maggior parte dei casi fotoni, rende vulnerabili ad attacchi di tipo Photon Number Splitting (PNS), descritto per la prima volta da Brassard et al. in [5]. L'attacco prevede che Eve prelevi una porzione dei fotoni in transito da Alice verso Bob durante tutta la durata della loro comunicazione.
Posto che sia Bob che Alice siano a conoscenza dell'inaffidabilità del canale trasmissivo e delle possibili perdite di informazioni, Eve può impedire il passaggio di parte del flusso di fotoni diretto verso Bob facendogli credere che questo fenomeno sia dovuto interamente alla natura del canale. In questo modo, Eve può celare la propria presenza alle parti coinvolte nella comunicazione.
Al fine di contrastare PNS, l'articolo [9] spiega come sia possibile rilevare la distribuzione dei fotoni nel canale e il tempo di trasmissione, permettendo di confrontarli con i valori attesi per aumentare la capacità di identificare la presenza dell'attaccante.

2.4.3 Intercept-resend

L'obiettivo di Eve è ottenere, almeno in parte, la chiave condivisa tra Alice e Bob. La strategia più immediata è intercettare i qubit in transito da Alice a Bob: tuttavia, questi non possono essere banalmente copiati, in quanto ciò contraddirebbe il teorema "no-cloning". Dunque, per estrarre il contenuto informativo, l'*eavesdropper* Eve è forzato alla lettura (quindi alla distruzione dell'informazione) delle particelle. La misurazione di queste ultime prevede però la scelta casuale di una base, come si vedrà nel capitolo 4: se questa scelta si rivela inesatta (cioè viene scelta una base diversa da quella utilizzata da Alice), allora il successivo rinvio delle particelle verso Bob, codificate con la nuova base, lo porterà ad effettuare misurazioni dall'esito completamente casuale.

2.4.4 Beam splitting

Dal momento che utilizzare sorgenti a singolo fotone nelle comunicazioni quantistiche tra Alice e Bob espone ad attacchi di tipo PNS e non garantisce la ricezione dei fotoni da parte di Bob, si è pensato di inviare flussi di fotoni per mezzo di impulsi laser. Tuttavia, l'impiego di impulsi apre la strada ad attacchi Beam Splitting [6], ossia alla possibilità da parte di un *eavesdropper* di "trafugare" parte dei fotoni nell'impulso in transito. Solitamente un attacco di questo tipo garantisce a Eve di acquisire informazioni sui bit scambiati e, al tempo stesso, di celare la propria presenza dal momento che Bob vedrebbe giungere comunque a destinazione parte dell'impulso originale e penserebbe che la componente persa sia dovuta alle inevitabili perdite del canale trasmissivo.
In presenza di lunghi canali di trasmissione l'attacco risulta difficilmente realizzabile per via del fatto che le perdite di segnale sarebbero elevate a prescindere dall'intervento di Eve e quindi un'eccessiva riduzione del segnale ricevuto da Bob farebbe nascere in lui il sospetto della presenza di un attaccante.
[29] afferma di aver realizzato un meccanismo di difesa che consente di rilevare la presenza di un *eavesdropper* anche in presenza di un canale estremamente rumoroso. Il concetto si basa su misurazioni statistiche del rumore previsto all'interno del canale e delle perdite attese di segnale: se queste superano una data soglia, calcolate statisticamente, allora viene notificata la presenza di un *eavesdropper*.

2.4.5 Physical side-channels

Date le limitazioni degli attacchi che sfruttano il canale in fibra ottica, al fine di dischiudere il contenuto informativo tra Alice e Bob è possibile sfruttare mezzi trasmissivi alternativi come radiazioni elettromagnetiche, dissipazione del calore, rumore acustico, registrazione dei tempi computazionali o dei consumi energetici. Ad esempio, si rileva il tempo impiegato dal dispositivo per produrre la chiave di sessione, così da poterla ricavare. Allo stato dell'arte odierno, sia che si parli di protocolli classici di *key exchange* che di QKD, non esiste una soluzione ufficiale in grado di far fronte in via permanente a questo attacco.

2.4.6 Disturbi nella comunicazione come sintomo di eavesdropping

Nei sistemi reali, se Alice e Bob scoprono che le loro misurazioni non sono correttamente correlate risulta arduo determinare se la discrepanza sia dovuta al canale trasmissivo rumoroso, alla strumentazione difettosa oppure alla presenza di un *eavesdropper* che genera delle perturbazioni nei fotoni, misurandoli. Si assume dunque la presenza dell'attaccante e che quest'ultimo sia in possesso di informazioni sulla chiave condivisa da Alice e Bob al termine di un protocollo di QKD. Per questo motivo, i protocolli di QKD possono includere come ultimo passo dell'algoritmo una tecnica nota come *privacy amplification* [20] che mira a ridurre l'informazione che Eve ha riguardo la chiave condivisa. La tecnica prevede che venga fornito in ingresso a una funzione di hash scelta casualmente una stringa casuale di bit della stessa lunghezza della chiave condivisa. L'output della funzione risulta poi essere una stringa binaria (la nuova chiave condivisa) di lunghezza fissata e minore della lunghezza della chiave condivisa. La nuova chiave è più corta di quella originale di una quantità che varia in base a quanta informazione si stima essere in possesso dell'attaccante. Tali calcoli sono possibili misurando la discrepanza tra i bit letti da Bob rispetto a quelli intesi da Alice. La *privacy amplification* garantisce che la probabilità che l'attaccante possegga informazioni riguardo la nuova chiave sia molto bassa.

Capitolo 3

Metodologie

L'obiettivo di questo documento è confrontare in modo critico ed esplicito i diversi protocolli di QKD descritti all'interno dello stesso.
Al fine di raggiungere gli scopi sopracitati, la nostra metodologia di analisi prevede di:

1. illustrare i funzionamenti dei protocolli di QKD BB84, E91, B92 e SARG04 nel capitolo 4;
2. effettuare un confronto esplicito dei succitati protocolli di QKD nel capitolo 5 per mezzo di tabelle facilmente consultabili che fungono anche da tassonomia;
3. esplicitare considerazioni di natura tecnico-pratica sull'impiego dei succitati protocolli di QKD nel capitolo 5.

Relativamente al confronto esplicito, esso sarà costruito sulla base delle seguenti dimensioni di comparazione:

1. principio quantistico di funzionamento;
2. polarizzazione dei fotoni;
3. numero di stati;
4. vulnerabilità rispetto agli attacchi descritti nel capitolo 2;
5. presenza di implementazioni reali (sperimentali o industriali) e/o simulate.

Ciascuna di queste dimensioni di comparazione, stabilite perché largamente utilizzate in letteratura per confrontare protocolli di QKD, saranno brevemente descritte nelle sezioni sottostanti.

3.1 Principio quantistico di funzionamento

I protolli di QKD basano il proprio funzionamento su uno dei due principi cardine della meccanica quantistica: il principio di indeterminazione di Heisenberg e il quantum entanglement.

L'idea dei protocolli che usano il principio di indeterminazione di Heisenberg è che un *eavesdropper* non può misurare lo stato di fotoni che vengono inviati sul canale di comunicazione senza disturbarne lo stato e, quindi, senza essere scoperti [10].

L'idea dei protocolli che si basano su quantum entanglement è che le due parti della comunicazione ricevano fotoni "entangled". Ognuna delle due parti sceglie delle basi casuali per misurarli. Per ogni base scelta sia dal mittente che dal destinatario dei fotoni, gli stati letti devono essere opposti. Gli stati letti in corrispondenza di una stessa base possono essere interpretati come due stringhe binarie complementari: una di queste due stringhe può essere utilizzata come chiave segreta di comunicazione [10] [15].

3.2 Polarizzazione dei fotoni e numero di stati

Abbiamo visto al capitolo 2 la necessità di scegliere delle basi per rappresentare l'informazione (e successivamente leggerla). Il numero di stati non è altro che il numero totale di possibili polarizzazioni che può assumere un fotone e, conseguentemente, il numero di vettori dell'unione delle basi scelte. Per esempio, il protocollo BB84 prevede quattro stati di polarizzazione che corrispondono a quattro vettori di base: un vettore a 0 gradi e un vettore a 90 gradi (base rettilinea), un vettore a 45 gradi e un vettore a 135 gradi (base diagonale) [14] [23] [20] (per maggiori dettagli, si veda il capitolo 4). Quanto spiegato è mostrato in figura 3.1 e si può notare con facilità come gli stati entro la stessa base siano ortogonali.

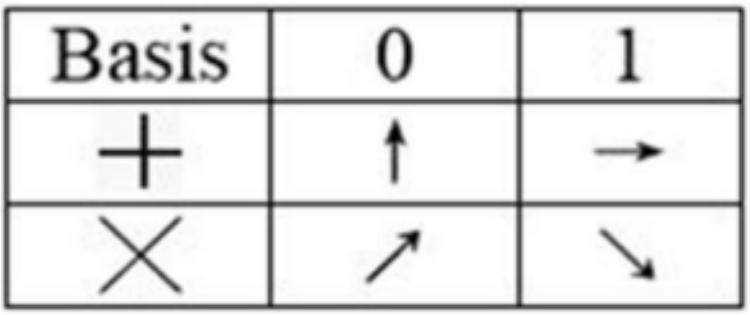

Figura 3.1: I quattro diversi stati di polarizzazione dei fotoni nel protocollo BB84. La base rettilinea (prima riga) e la base diagonale (seconda riga) formano due basi di stati ortogonali [14].

3.3 Vulnerabilità rispetto ad attacchi noti

Ogni algoritmo presentato può essere suscettibile a qualche attacco e da tale suscettibilità dipende la sicurezza del protocollo di QKD. Pertanto, per un progettista risulta fondamentale conoscere le vulnerabilità dei protocolli che adotterà.

3.4 Presenza di implementazioni reali e/o simulate

I protocolli di QKD, per essere effettivamente testati in molteplici campi di applicazione e sotto svariate condizioni di impiego, necessitano di essere implementati. Pertanto, i protocolli di QKD analizzati nel documento saranno classificati anche in base alla presenza in letteratura di articoli che attestino l'implementazione di tali protocolli in ambienti reali e/o simulati.

Capitolo 4

Protocolli di QKD

Diversamente da molti dei protocolli crittografici classici oggi in uso, la cui sicurezza si basa spesso su ipotesi non dimostrate riguardanti la complessità computazionale di problemi matematici, la sicurezza della crittografia quantistica si basa sulle leggi della fisica. Su tali leggi i protocolli di QKD, che rappresentano una porzione corposa della crittografia quantistica, basano la propria sicurezza incondizionata.

In questo capitolo verranno descritti i funzionamenti dei protocolli di QKD BB84, B92, E91 e SARG04. Alcuni di questi si basano sul principio di indeterminazione di Heisenberg, mentre altri sul principio di Entanglement. Tali protocolli, selezionati fra tutti perché rappresentano le basi di numerosi protocolli di QKD più recenti, verranno presentati in ordine cronologico di pubblicazione.

4.1 BB84

Il protocollo BB84 [2], ideato a C. H. Bennet e G. Brassard nel 1984, è un protocollo di QKD basato sul principio di indeterminazione di Heisenberg che sfrutta gli stati di polarizzazione dei fotoni per trasmettere l'informazione.
Il mittente e il ricevente (Alice e Bob) sono intenzionati a scambiarsi una chiave segreta e sono connessi l'una all'altro mediante un canale quantistico, su cui viaggiano i fotoni polarizzati, e un canale classico di comunicazione (ad esempio Internet). Nessuno dei due canali ha la necessità di essere sicuro, dal momento che BB84 è progettato ipotizzando la presenza di un *eavesdropper* (Eve) che può interferire nelle comunicazioni su ambo i canali. Come indicato nel capitolo 2, il canale quantistico può essere manomesso ma non monitorato passivamente; per il canale classico, invece, valgono le considerazioni inverse.
Le polarizzazioni dei fotoni, o stati, sono quattro e sono raggruppate in due diverse basi non ortogonali: quella rettilinea ($\bigoplus$) e quella diagonale ($\bigotimes$). La base $\bigoplus = \{|0\rangle, |1\rangle\}$, mentre la base $\bigotimes = \{|+\rangle, |-\rangle\}$, dove $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. La figura 4.1 riporta i 4 possibili stati quantistici previsti da BB84 raggruppandoli per base di polarizzazione: BB84 assegna allo stato $|0\rangle$ e $|+\rangle$ la codifica dello 0 binario, mentre a $|1\rangle$ e $|-\rangle$ la codifica del 1 binario.

Di seguito sono indicati i passi del protocollo come riassunti da [8]:

1. Alice costruisce una stringa casuale di bit $s \in \{0,1\}^n$ e una stringa casuale di basi $b \in \{\bigoplus, \bigotimes\}^n$ per la codifica;

2. Alice prepara n qubit q_i polarizzando altrettanti fotoni usando la base $b_i \in b$ per la codifica del bit $s_i \in s$;

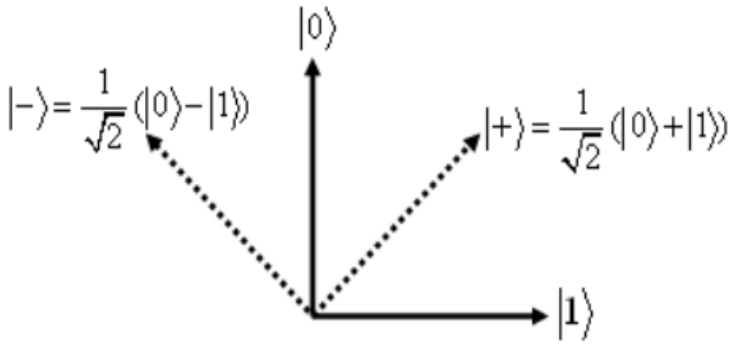

Figura 4.1: I quattro diversi stati di polarizzazione dei fotoni nel protocollo BB84 [8]

3. Alice spedisce i qubit a Bob su un canale quantistico pubblico;

4. Bob costruisce una stringa casuale $b' \in \{\bigoplus, \bigotimes\}^n$ di basi che verranno utilizzate per la misurazione degli n qubit inviati da Alice. Misurandoli, ottiene una stringa di bit $s' \in \{0,1\}^n$;

5. per ogni bit $s_i \in s$, Alice invia a Bob su un canale classico il valore di b_i e Bob verifica se $b_i = b'_i$. In caso negativo, i bit s_i e s'_i vengono rimossi rispettivamente da s e da s';

6. Alice quindi individua un sottoinsieme casuale di bit in s e li comunica a Bob sul canale classico. Se anche solo uno di questi bit non coincide con la misurazione effettuata da Bob sul qubit corrispondente, allora viene rilevata la presenza di un *eavesdropper* Eve sul canale quantistico e cessano le comunicazioni tra Alice e Bob;

7. se invece tutti i confronti danno esito positivo, allora i bit rimasti in s compongono la chiave segreta $k = \{0,1\}^t$, con $t < n$.

Per capire correttamente il funzionamento di BB84 occorre spiegare come avviene la misurazione di un qubit secondo una qualche base. Se si ha $|qubit\rangle = a\,|c\rangle + b\,|d\rangle$ la misura di questo stato utilizzando la base $B = \{|c\rangle, |d\rangle\}$ produce lo stato $|c\rangle$ con probabilità $|a|^2$ e lo stato $|d\rangle$ con probabilità $|b|^2$. Ovviamente i quadrati delle ampiezze di a e b se sommati restituiscono 1. Quindi, se misurassimo lo stato $|qubit\rangle$ con una base diversa, il risultato ottenuto sarebbe casuale. Nel caso di Bob, se sceglie di utilizzare la base $\bigotimes$ per misurare un qubit in stato $|1\rangle$, il risultato della misurazione sarà equiprobabilmente 0 oppure 1. Al contrario, se sceglie di utilizzare la base $\bigoplus$ allora otterrà certamente 1 dal momento che $|1\rangle = 1\,|1\rangle + 0\,|0\rangle$.

I test condotti durante il passo 6 sono pensati precisamente per rilevare la presenza di Eve. Se uno di essi fallisce, il motivo può essere un disturbo esterno oppure un rumore sul canale quantistico, ma si suppone in entrambi i casi che la causa sia la presenza di Eve. Infatti, tra gli attacchi che può effettuare, c'è anche il cosiddetto *intercept-resend*, dove Eve misura lo stato dei fotoni inviati da Alice e poi invia a Bob nuovi fotoni polarizzati in base allo stato che lei stessa ha misurato. Dal momento che Eve non ha idea delle basi che Alice ha utilizzato per la polarizzazione dei fotoni, può solamente provare ad indovinarle proprio come fa Bob. Se Eve sceglie la base corretta, allora misura il corretto stato di polarizzazione e rinvia a Bob lo stato corretto. Tuttavia, se la base che sceglie non è corretta, allora lo stato che viene misurato è casuale così come lo stato del qubit che verrà rinviato a Bob. In quest'ultimo caso, il principio di indeterminazione garantisce che l'informazione codificata in tale qubit venga persa. Giunti a questo punto, se la misurazione dello stato effettuata da Bob sfrutta la stessa base utilizzata

da Alice, allora lo stato misurato sarà casuale.

Eve sceglie le proprie basi erroneamente con una probabilità di 0.5 per ciascuna e, se Bob misura i fotoni precedentemente intercettati da Eve utilizzando le stesse basi di Alice, allora anche lui ottiene un risultato sbagliato con una probabilità di 0.5. Quindi, la probabilità che un qubit intercettato generi un bit errato nella chiave finale è di $0.5 * 0.5 = 0.25$. Se poi Alice e Bob confrontano pubblicamente n bit della loro chiave, allora la probabilità di ottenere un confronto dall'esito negativo e di rilevare la presenza di Eve è pari a $1 - (\frac{3}{4})^n$. Quindi, maggiore è il numero dei bit della chiave e maggiore sarà la probabilità di rilevare l'eventuale presenza di un *eavesdropper* [8].

BB84 a oggi è il protocollo di QKD più famoso e il più implementato. La sua capacità di rilevare la presenza di *eavesdropper* è stata provata in [22] e [27]. Il canale quantistico maggiormente utilizzato è la fibra ottica [11], anche se è possibile utilizzare elettroni e quindi canali di trasmissione basati su conduttori elettrici o spazio libero [18].

4.2 E91

Il protocollo E91 [7], che prende il nome dal suo ideatore (A. Ekert) e dall'anno in cui è stato pubblicato, si basa sul principio di Entanglement e sfrutta coppie di particelle, dette EPR (Einstein-Podolsky-Rosen), correlate dal punto di vista quantistico. Queste coppie di stati quantistici costituiscono quegli stati, mostrati di seguito, su cui si basa E91.

1. $|S_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. $|S_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
3. $|S_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$
4. $|S_3\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$

Il funzionamento del protocollo [7] viene indicato di seguito:

1. Alice crea una sequenza di n coppie EPR, cioè di fotoni polarizzati e quantisticamente correlati. Per ogni coppia, invia un fotone a Bob e memorizza l'altro in una memoria quantistica;
2. Sia Alice che Bob scelgono casualmente una sequenza di n basi ($\bigoplus$ o $\bigotimes$). Tali basi saranno utilizzate sia da Alice che da Bob per misurare i fotoni della sequenza: quelli memorizzati da Alice e quelli ricevuti da Bob;
3. Alice e Bob comunicano su un canale classico le proprie misurazioni e conservano unicamente quelle che sono state ottenute utilizzando la stessa base. I bit conservati compongono una cosiddetta *raw key*, mentre quelli scartati compongono una *rejected key*.
4. Alice e Bob confrontano le proprie *rejected key* per verificare che la disuguaglianza di Bell sia o meno soddisfatta: in caso affermativo, viene rilevata la presenza di un *eavesdropper* Eve perché normalmente la disuguaglianza non è valida per coppie EPR; in caso negativo, Eve non è presente.

Dalla descrizione del funzionamento di E91 emerge quindi come anche questo protocollo sia concepito per rilevare la presenza di un *eavesdropper*. Questa verifica però avviene in modo diverso rispetto agli atri protocolli trattati in questo documento: in questo caso, infatti, viene testata la disuguaglianza di Bell, invece che verificate le "incongruenze" fra bit. Semplicemente, la disuguaglianza di Bell verifica la correlazione quantistica tra particelle che compongono una coppia EPR. La misurazione di una di esse da parte di Eve "rompe" lo stato di Entanglement che esiste fra le due, portando la disuguaglianza di Bell ad essere valida quando normalmente non lo è. Questa verifica funge quindi da campanello di allarme per segnalare ad Alice e Bob la presenza di Eve.

I passi succitati descrivono il funzionamento del protocollo E91 nella sua versione originale. Tuttavia, negli anni, numerosi ricercatori hanno pubblicato leggere varianti del protocollo ([13], [16]).

A oggi, esistono implementazioni simulate di E91 all'interno dell'ambiente Matlab [24], ma sono state realizzate anche delle implementazioni reali, seppur sperimentali, tramite una rete satellitare [31]. Infatti, l'impiego di un satellite nella composizione di canali quantistici risolve il problema del degrado del *photon trasmission rate*, che affligge invece la fibra ottica quando questa supera una data lunghezza (dell'ordine di centinaia di chilometri).

4.3 B92

Il protocollo B92 [1], nato nel 1992 ad opera di C. Bennet, si basa su due stati quantistici non ortogonali. B92 condivide lo stesso principio quantistico di funzionamento di BB84, ma utilizza solamente due stati quantistici invece che quattro. Di seguito sono indicati i passi del protocollo come descritti da [8]:

1. Alice sceglie casualmente gli elementi di un vettore $A \in \{0,1\}^n$. Per ogni $i = 1, ..., n$, se $A_i = 0$ Alice invia a Bob lo stato $|0\rangle$ sul canale quantistico, mentre se $A_i = 1$ allora Alice invia $|+\rangle$;

2. Bob crea un proprio vettore di bit casuali detto $B \in \{0,1\}^n$. Per ogni $i = 1, ..., n$, se $B_i = 0$ Bob sceglie la base $\bigoplus$, mentre sceglie invece la base $\bigotimes$ se $B_i = 1$;

3. con tali basi ($\bigoplus$ o $\bigotimes$), Bob misura ogni stato quantistico inviato da Alice ($|0\rangle$ o $|+\rangle$);

4. Bob costruisce il vettore $T \in \{0,1\}^n$ in questo modo: per ogni $i = 1, ..., n$, se la misura effettuata da Bob sul qubit q_i inviato da Alice produce $|0\rangle$ o $|+\rangle$ allora $T_i = 0$; diversamente, se la misurazione effettuata da Bob produce $|1\rangle$ o $|-\rangle$, allora $T_i = 1$;

5. Bob invia T ad Alice sul canale di comunicazione classico;

6. Alice e Bob conservano solamente i bit di A e di B in corrispondenza di $T_i = 1$. In questo modo, e supponendo l'assenza di Eve, vale che $A_i = 1 - B_i$. I bit preservati compongono quindi una chiave grezza condivisa formati dagli $A_i = 1 - B_i$;

7. Alice sceglie un campione dei bit della chiave grezza condivisa e ne rivela i bit a Bob su un canale classico. Se esiste anche solo uno di essi per cui vale che $A_i \neq 1 - B_i$, allora viene rilevata la presenza di Eve e le comunicazioni fra Alice e Bob vengono interrotte.

8. la chiave segreta condivisa $K \in \{0,1\}^t$, con $t < n$ è quindi costruita rimuovendo dalla chiave grezza i bit campionati al passo precedente.

Per capire correttamente B92 occorre notare che se un $T_i = 0$ significa che Bob non sa cosa Alice gli abbia inviato. Quindi se Bob sceglie $\bigoplus$ ($\bigotimes$) come base, può ottenere $|0\rangle$ ($|+\rangle$) come risultato della propria misurazione qualunque sia lo stato realmente inviato da Alice ($|0\rangle$ oppure $|+\rangle$). Invece, se $T_i = 1$ allora Bob saprà con esattezza qual è lo stato che gli è stato inviato da Alice. Inoltre, al passo 6, Alice e Bob verificano l'eventuale presenza di Eve. L'idea è che se esiste un i tale che $T_i = 1$, allora $A_i = 1 - B_i$; altrimenti, è evidente che esiste del rumore sul canale quantistico o che vi è stato applicato un disturbo esterno (entrambi i casi si suppone siano riconducibili alla presenza di Eve). La tabella in figura 4.2 riassume e chiarifica il funzionamento di B92.

Bits chosen by Alice	$A_i = 0$				$A_i = 1$			
States sent by Alice	$\|0\rangle$				$\|+\rangle$			
Bits chosen by Bob	$B_i = 0$		$B_i = 1$		$B_i = 0$		$B_i = 1$	
Basis chosen by Bob	$\oplus$		$\otimes$		$\oplus$		$\otimes$	
Results of the measures of Bob	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Probability to measure the state	1	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
The value of the test	**0**	**-**	**0**	**1**	**0**	**1**	**0**	**-**

Figura 4.2: Descrizione riassuntiva del protocollo B92 [8]

Anche questo protocollo è capace di rilevare la presenza di eventuali *eavesdropper*. Le implementazioni, dal momento che si utilizzano ancora fotoni polarizzati per l'invio degli stati quantistici, coinvolgono ancora l'utilizzo di fibre ottiche come canali, sorgenti e ricettori di fotoni per l'invio e la ricezione degli stessi. Anche in questo caso, però, come per BB84, sono state realizzate implementazioni reali, seppur sperimentali, basate su elettroni polarizzati che viaggiano su conduttori elettrici o nello spazio libero [18] [11].

4.4 SARG04

Il protocollo SARG04 [25] è una variante di BB84 che si fonda quindi sul medesimo principio quantistico. La prima fase, quella che va dal passo 1 fino al passo 4 incluso, è pressoché identica. Una differenza sostanziale si nota nel passo 5, ossia quando Alice e Bob comunicano su un canale tradizionale per quali bit le basi che hanno utilizzato nelle misurazioni coincidono. In SARG04 Alice non annuncia direttamente a Bob le proprie basi, bensì gli invia una coppia di stati non ortogonali di cui uno è stato utilizzato per la codifica del bit corrispondente. In questo modo, se Bob ha scelto la base corretta, allora misurerà lo stato corretto e anche il bit originariamente inteso da Alice. Diversamente, non sarà in grado di misurare correttamente nessuno dei due stati non ortogonali inviati da Alice e non riuscirà a risalire al bit originale. Un'altra differenza sostanziale sta nel fatto che SARG04 non utilizza una sorgente a singolo fotone come BB84 o B92, bensì un laser a impulsi attenuati. Questa differenza, a livello fisico invece che algoritmico, rende SARG04 più robusto di BB84 ad attacchi di tipo PNS [8] dal momento che è più difficile prelevare un gran numero di fotoni che sono raggruppati in impulso luminoso senza rivelare la propria presenza. Anche SARG04, in quanto derivato di BB84 rende possibile la rilevazione di eventuali *eavesdropper*.

Capitolo 5

Confronto esplicito

Alla luce delle considerazioni evidenziate nei capitoli 2 e 4 e del funzionamento dei protocolli, possiamo confrontarli esplicitamente sulla base delle dimensioni di confronto individuate e descritte nel capitolo 3.

	BB84	**E91**	**B92**	**SARG04**
Principio quantistico	Heisenberg	Entanglement	Heisenberg	Heisenberg
Numero di stati	4	2 coppie EPR	2	4
Polarizzazione	ortogonale	ortogonale	non ortogonale	ortogonale
DoS	vulnerabile	vulnerabile	vulnerabile	vulnerabile
PNS	vulnerabile	vulnerabile	vulnerabile	meglio di BB84
Intercept/resend	vulnerabile	vulnerabile	vulnerabile	vulnerabile
Beam splitting	vulnerabile	vulnerabile	vulnerabile	vulnerabile
Side channel	vulnerabile	vulnerabile	vulnerabile	vulnerabile

Tabella 5.1: Confronto dei protocolli di QKD.

Dalla tabella 5.1 possiamo constatare che:

- la prevalenza dei principali algoritmi si basa sul principio di indeterminazione. Solo E91 si fonda sull'Entanglement;
- il numero di stati oscilla tra 2 e 4;
- la polarizzazione dei fotoni maggiormente adottata fa uso di basi i cui stati sono ortogonali;
- sebbene tutti i protocolli siano idealmente incondizionatamente sicuri [22], [28] [19], sono tutti vulnerabili agli attacchi descritti in precedenza (ad eccezione di. Questo implica che nella pratica la sicurezza incondizionata non sempre è facile da raggiungere [4]. Non sono stati ancora trovati meccanismi di difesa validi e, come già indicato, per alcuni attacchi non è possibile implementare una controffensiva definitiva, ossia che garantisca la sicurezza nei confronti di essi.

SARG04 appare attualmente come il miglior protocollo tra quelli indicati perché, nonostante le vulnerabilità, fornisce una robustezza maggiore dei concorrenti. Ad esempio, SARG04 ha una resistenza maggiore all'attacco PNS, per via del fatto che viene implementato utilizzando laser ad impulsi invece che sorgenti a singoli fotoni. Sebbene l'impiego degli impulsi non lo rendano automaticamente immune agli attacchi di tipo *beam splitting*, abbiamo osservato nel capitolo 2 alcuni meccanismi di difesa. Un ulteriore vantaggio dal punto della sicurezza si può osservare a livello algoritmico in quanto Alice non rivela direttamente le proprie basi a Bob su un canale classico, bensì rivela una coppia di stati non ortogonali in cui i bit vengono codificati.

Dal momento che tutti i protocolli sono vulnerabili ad attacchi di tipo *intercept-resend*, emerge come la probabilità con la quale Eve può indovinare la corretta base di polarizzazione per misurare i qubit che intercetta debba essere piccola. Per garantire probabilità ridotte a tale scopo, è necessario aumentare il numero di basi di polarizzazione. Infatti, se venissero utilizzate tre basi di coppie di stati quantici ortogonali per la codifica dei bit, la probabilità con cui Eve potrebbe indovinare la corretta base da utilizzare per la misurazione dei qubit intercettati sarebbe del 33% (contro quella del 50% nei casi in cui si utilizzino solamente due basi). A tal proposito, ricordiamo che nel capitolo precedente sono state accennate delle versioni di E91 con 3 basi di polarizzazione. Dunque, un fattore fondamentale della sicurezza è preferire quei protocolli di QKD (o varianti degli stessi) con un numero di stati superiore.

Ciò nonostante, il problema principale che accomuna tutti i protocolli di QKD visti è la verifica dell'identità delle due parti, l'autenticazione. Infatti, il livello di sicurezza garantito per le comunicazioni entro un protocollo di QKD non si cura della vera identità della parti coinvolte: uno tra Alice e Bob potrebbe essere sostituito da Eve facendo credere all'altro di comunicare con una entità differente. L'autenticazione può essere ottenuta sovrapponendo al protocollo di QKD un secondo protocollo oppure per mezzo di terze parti, come il TC.

Inseriamo un'analisi aggiuntiva rispetto alle dimensioni di confronto appena viste, che tiene conto delle effettive applicazioni dei protocolli di QKD.

	BB84	**E91**	**B92**	**SARG04**
Implementazioni simulate	sì	sì	sì	sì
Implementazioni reali	sì	sì	sì	sì
Applicazioni industriali	n/d	n/d	n/d	n/d

Tabella 5.2: Implementazioni e sbocchi applicativi dei protocolli di QKD.

La tabella 5.2 sottolinea che esistono versioni simulate dei suddetti protocolli: queste principalmente le ritroviamo sviluppate con toolbox di Matlab [24], oppure con i servizi offerti da IBM Quantum. Esistono anche implementazioni reali dei protocolli trattati che sfruttano sorgenti di singoli fotoni o laser ad impulsi e dove il mezzo trasmissivo è la fibra ottica, conduttori o lo spazio vuoto [18] [11] [31]. Ritroviamo infine realtà aziendali come IDQuantique, QuintessenceLabs, MagicQ e SeQureNet che dichiarano di fornire soluzioni hardware (ad esempio generatori quantici di numeri casuali) e software in ambito di quantum computing, senza dichiarare tuttavia i protocolli utilizzati.

A livello sperimentale il BB84 appare come il protocollo più quotato per effettuare test di funzionamento su territorio nazionale. Sulla spinta della Commissione Europea, il Joint Research Center in [21] ha redatto un resoconto dello stato dell'arte delle sperimentazioni di ciascuno Stato. È emerso che BB84 è stata la scelta primaria essendo uno dei primi protocolli ad essersi imposto in ambito QKD, dunque uno dei più diffusi.

Riguardo ad aspetti tecnico-pratici, i protocolli che si basano sulla fibra ottica sono molto utilizzati. Ad oggi, [3] riporta la lunghezza massima della fibra ottica (421 km) che si può raggiungere prima che i disturbi e le perdite a cui è soggetta non garantiscano la terminazione desiderata dei protocolli di QKD (posto che la fibra ottica sia ad alte prestazioni). Emerge quindi nuovamente come il canale trasmissivo sia un punto critico delle implementazioni dei protocolli di QKD. Per quanto riguarda invece la scelta di impiego di sorgenti a singoli fotoni rispetto a laser ad impulsi, la scelta più saggia dovrebbe ricadere sugli ultimi per via della maggiore robustezza verso gli attacchi di tipo *beam splitting* e *Denial of Service*, dal momento che è più facile prevenire attacchi DoS quando si usano gruppi di fotoni (impulsi) che non singoli fotoni per la codifica dell'informazione (a meno di danni fisici ai canali di trasmissione).
Altre implementazioni, come accennato, sfruttano l'aria o il vuoto come mezzo di trasmissione [18] ma le applicazioni rimangono limitate.

Diversamente, invece, le implementazioni dei protocolli basati su QE consentono distanze maggiori fra le parti della comunicazione perché sfruttano il principio di *action at distance* che caratterizza il comportamento di particelle "entangled" [31].

Capitolo 6

Conclusioni

In questo documento sono state descritte basi teoretiche e principi fondamentali della meccanica quantistica quali il principio di indeterminazione di Heisenberg, il teorema no-cloning e il principio di Entanglement. Sono poi stati descritti il funzionamento generico dei protocolli di QKD nonché vulnerabilità e attacchi perpetuabili da parte di attaccanti in possesso di tecnologie (quantistiche e non) arbitrarie. Essi sono il *Denial of Service*, il *Photon Number Splitting*, *Intercept-Resend*, *Beam Splitting* e *Physical side-channels*.

In secondo luogo, sono stati descritti attentamente, ma in modo semplice e conciso, i funzionamenti di protocolli di QKD quali: BB84, E91, B92 e SARG04. Questi sono stati presentati in ordine di pubblicazione, perché rappresentano le basi di numerosi altri protocolli di QKD più recenti non menzionati all'interno del documento.

Contestualmente, è stato costruito per mezzo di tabelle un confronto esplicito dei protocolli descritti. E91 risulta essere l'unico protocollo basato sul principio di Entanglement, contrariamente agli altri che si fondano sul principio di indeterminazione. La polarizzazione dei fotoni, usati ovunque tranne che in SARG04, avviene sempre per mezzo di basi ortogonali ($\bigoplus$ o $\bigotimes$) tranne nel caso di B92. In quest'ultimo, infatti, la polarizzazione avviene per mezzo di basi non ortogonali e porta ad ottenere, peculiarmente, solamente due stati per la codifica binaria contro i soliti quattro previsti dagli altri protocolli. Inoltre, per tutti i protocolli studiati si è osservato che esistono implementazioni sia in ambiente simulato, sia nella realtà. Al contrario, non è stato possibile risalire con certezza all'impiego di alcun protocollo in prodotti software o hardware commercializzati.

Per quanto riguarda la vulnerabilità dei protocolli studiati nei confronti degli attacchi sopracitati, è risultato che nessuno di essi è completamente resistente ad tali attacchi. Infatti, nonostante sia stata dimostrato l'incondizionata sicurezza dei protocolli di QKD, questa rimane una proprietà teorica che cade o risulta indebolita in contesti reali quando ci si scontra coi limiti fisici dei canali di trasmissione [19] [26].

Infine, per orientare la scelta di un protocollo di QKD rispetto ad altri, si è osservato come questa debba ricadere su protocolli che:

- utilizzino un numero di basi di polarizzazione maggiore di due così da diminuire la probabilità che Eve indovini la corretta base per la misurazione dei qubit intercettati;
- impieghino laser ad impulsi attenuati rispetto alle sorgenti a singoli fotoni per ottenere maggiori garanzie di sicurezza contro attacchi di tipo PNS (posto che si implementino meccanismi di difesa contro attacchi di tipo *beam splitting*);
- basino la propria implementazione concreta su canali trasmissivi dalle prestazioni adeguate per limitare disturbi e perdite di contenuto informativo anche su lunghe distanze.

6.1 Sviluppi futuri

Il campo della crittografia quantistica è in continua evoluzione e non comprende unicamente i protocolli di QKD, sebbene questi rappresentino una grossa porzione di questa disciplina. Il numero di tali protocolli è in costante aumento nel tentativo di proporne delle versioni maggiormente resistenti ad attacchi noti e resilienti alle inevitabili limitazioni dei mezzi trasmissivi. Future direzioni di ricerca possono riguardare l'esplorazione di ulteriori protocolli di QKD, specialmente quelli più recenti, al fine di osservarne similitudini e differenze e analizzare come questi affrontano le limitazioni di cui soffrono i loro predecessori. Un'ulteriore finalità di una futura ricerca sarebbe sicuramente indagare nuove implementazioni reali dei protocolli di QKD, rese possibili dai miglioramenti tecnologici avvenuti negli ultimi dieci anni.

Bibliografia

[1] C. H. Bennet. «Quantum cryptography using any two non-orthoganol states». In: (1992).

[2] C. H. Bennet e G. Brassard. «Quantum Cryptography: Public key distribution and coin tossing». In: (1984).

[3] Alberto Boaron et al. «Secure Quantum Key Distribution over 421 km of Optical Fiber». In: (2018).

[4] G. Brassard et al. «Security aspects of Practical Quantum Criptography». In: (2000).

[5] Gilles Brassard et al. «Limitations on Practical Quantum Cryptography». In: *Physical review letters* 85 (set. 2000), pp. 1330–3. DOI: 10.1103/PhysRevLett.85.1330.

[6] John Calsamiglia, Stephen Barnett e Norbert Lütkenhaus. «Conditional beam splitting attack on quantum key distribution». In: *Physical Review A* 65 (lug. 2001). DOI: 10.1103/PhysRevA.65.012312.

[7] A. K. Ekert. «Quantum cryptography based on Bell's theorem». In: (1991).

[8] M. Elboukhari, M. Azizi e A. Azizi. «Quantum Key Distribution Protocol: A Survey». In: (2010).

[9] A. A. Gaidash, V. I. Egorov e A. V. Gleim. «Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices». In: (2016).

[10] Mart Haitjema. «A Survey of the Prominent Quantum Key Distribution Protocols». In: (2007).

[11] R. Hughes et al. «Practical free-space quantum key distribution over 10km in daylight and at night». In: (2002).

[12] E. Hugues-Salas et al. «Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN)». In: *2018 Optical Fiber Communications Conference and Exposition (OFC)*. 2018, pp. 1–3.

[13] T. Hwang e K. C. Lee. «EPR quantum key distribution protocols with potential 100% qubit efficiency». In: (2007).

[14] Maithili S. Jha et al. «A survey on quantum cryptography and quantum key distribution protocols». In: (2019).

[15] LI Jian et al. «A Survey on Quantum Cryptography». In: (2018).

[16] S. J. Lomonaco Jr. «A quick glance at quantum cryptography». In: (1999).

[17] D N Kartheek, M Abhilash Kumar e M R Pavan Kumar. «Security using Quantum Key Distribution Protocols (QKDPs)». In: (2012).

[18] P. Knight. «Manipulating cold atoms for quantum information processing"». In: (2005).

[19] Hoi-kwong Lo e H. F. Chau. «Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances». In: (1998).

[20] Norbert Lütkenhau. «Security against individual attacks for realistic quantum key distribution». In: (1999).

[21] Travagnin Martino e Lewis Adam M. «Quantum Key Distribution in-field implementations». In: (2019).

[22] D. Mayers. «Unconditional security in quantum cryptography». In: (2001).

[23] R.Alléaumea et al. «Using quantum key distribution for cryptographic purposes: A survey». In: (2014).

[24] P.P. Rohde. «Quack! A Quantum Computer Simulator for Matlab». In: (2005).

[25] A. Scarani et al. «Quantum cryptography protocols robust against photon number splitting attacks». In: (2004).

[26] V. Scarani e R. Renner. «Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing». In: (2018).

[27] P. W. Shor e J. Preskill. «Simple proof of security of the BB84 quantum key distribution protocol». In: (2000).

[28] k. Tamaki, M. Koashi e n. Imoto. «Unconditionally secure key distribution based on two non orthogonal states». In: (2003).

[29] Ladyslav C. Usenko e Radim Filip. «Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense». In: (2016).

[30] Wikipedia. *Algoritmo di fattorizzazione di Shor*. 2022.

[31] Juan Yin et al. «Satellite-to-Ground Entanglement-Based Quantum Key Distribution». In: (2005).