UNIVERSITA' DEGLI STUDI DI GENOVA

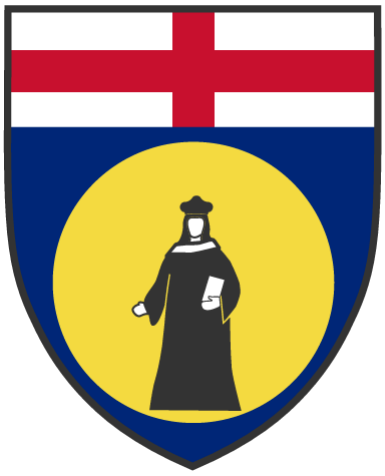
SCUOLA DI SCIENZE MATEMATICHE, FISICHE E NATURALI

DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

Corso di Laurea in Informatica

Prova Finale

Crittografia quantistica e protocollo SARG04



Referente: Dr. Paolo Solinas

Candidato: Giacomo Garbarino

Anno Accademico: 2020/2021

Indice

1 Introduzione

L'obiettivo di questa tesi è discutere l'importanza della crittografia quantistica, della quantum key distribution (in breve QKD) e del protocollo SARG04. Il testo sarà strutturato nel seguente modo: inizialmente verranno spiegati i punti di forza e debolezza della crittografia classica e dell'algoritmo crittografico RSA a seconda del modello computazionale, successivamente verrà introdotta la crittografia quantistica e la QKD, poi verrà illustrata l'importanza dell'utilizzo del fotone e infine verrà descritto il protocollo SARG04 e perché è stato progettato a partire da un altro protocollo chiamato BB84.

2 Crittografia Classica

La crittografia classica e i relativi algoritmi basano la loro sicurezza sulle capacità di calcolo dell'avversario, ossia è teoricamente possibile per un avversario decifrare una chiave crittografica senza essere scoperto. I tempi di calcolo necessari a decriptarla risultano tuttavia talmente elevati che tale operazione diventa infattibile. Uno degli algoritmi crittografici maggiormente usati per lo scambio sicuro di informazioni è l'RSA (Rivest-Shamir-Adleman). Questo metodo si basa sul fatto che dato un numero intero molto grande scritto come prodotto di due numeri interi e primi, sia computazionalmente infattibile trovare la sua fattorizzazione, cioè è infattibile trovare il moltiplicando e il moltiplicatore. Un computer classico impiegherebbe dunque molti mesi se non anni per portare a termine un'operazione di questo tipo che, al contrario, non rappresenterebbe alcun problema per un computer quantistico.

3 Crittografia Quantistica

Un computer classico codifica i bit di informazione come 0 o 1 a seconda se i transistor interni ad esso si trovano rispettivamente in uno stato di bassa o alta tensione. Un computer quantistico invece codifica l'informazione a partire dagli stati in cui si trovano oggetti quantistici da esso manipolati, come ad esempio i fotoni. La crittografia quantistica basa infatti la sua sicurezza sulle leggi fisiche della meccanica quantistica. Un algoritmo molto importante e utile nell'ambito della crittografia quantistica è l'algoritmo di Shor per la fattorizzazione di numeri interi. Questo algoritmo ha dimostrato che un computer quantistico è in grado di fattorizzare un numero in tempi esponenzialmente brevi rispetto ad un computer classico grazie alla sua potenza di calcolo enormemente maggiore. Difatti, il qubit consente di avere non solo 0 e 1, ma anche un numero virtualmente infinito di combinazioni lineari grazie al principio di sovrapposizione degli stati della meccanica quantistica. Questo significa che le chiavi crittografiche basate sull'algoritmo RSA che oggi si ritengono sicure per svariati anni, possono invece essere decifrate nel giro di settimane o mesi. Le carte di credito, ad esempio, hanno una durata di tre anni, ma possono essere violate da un computer quantistico in tempi relativamente brevi, di conseguenza andrebbero

cambiate dopo settimane o mesi ed è per questo che determinati settori come quello militare e bancario si sono interessati sin da subito alla crittografia quantistica. La crittografia quantistica è a chiave privata, ovvero due utenti devono avere una chiave privata comune e sicura con cui scambiarsi le informazioni. In particolare, la crittografia quantistica si focalizza sullo scambio di chiavi private e si basa sulla QKD: un sistema della meccanica quantistica per garantire comunicazione sicure tra due o più utenti. In particolare, lo scopo della QKD è quello di produrre e distribuire chiavi crittografiche agli utenti in modo sicuro. Come nel caso classico, lo scambio della chiave avviene attraverso un canale pubblico (quindi insicuro e intercettabile) e può essere usata per qualsiasi algoritmo di cifrazione e decifrazione. La QKD gode tuttavia di due proprietà della meccanica quantistica che vanno a svantaggio di un hacker:

- l'impossibilità di copiare un generico qubit di informazione grazie al teorema del no-cloning.
- un processo di misura di un generico qubit lo perturba a causa del collasso della funzione d'onda.

Durante una comunicazione, due utenti possono dunque rilevare la presenza di una terza parte che tenta di ottenere informazioni sulla chiave.

4 Qubit e Fotone

Un qubit è fisicamente rappresentabile in diversi modi. Tuttavia, uno dei modi più efficienti è utilizzare le particelle che compongono la luce: i fotoni (e la loro polarizzazione). La luce ordinaria, così come quella emessa dai laser che però ha proprietà particolari, interagisce poco con la materia e questo permette una trasmissione veloce del segnale senza un'eccessiva distorsione attraverso lunghe distanze. L'esperimento dei tre polarizzatori ci ha permesso di capire che un fotone può trovarsi in quattro possibili stati di polarizzazione: polarizzazione orizzontale, polarizzazione verticale, polarizzazione obliqua di 135° e polarizzazione obliqua di 45° e che questi quattro possibili stati possono essere rappresentati tramite qubit nel modo seguente:

$$|\rightarrow\rangle = \frac{|\nwarrow\rangle - |\nearrow\rangle}{\sqrt{2}}$$

$$|\uparrow\rangle = \frac{|\nwarrow\rangle + |\nearrow\rangle}{\sqrt{2}}$$

$$|\nwarrow\rangle = \frac{|\rightarrow\rangle + |\uparrow\rangle}{\sqrt{2}}$$

$$|\nearrow\rangle = \frac{|\rightarrow\rangle - |\uparrow\rangle}{\sqrt{2}}.$$

Ognuno di questi stati è rappresentato in uno stato di sovrapposizione. Ciò è possibile perché il fotone, dal momento che è un oggetto quantistico, risponde

ai principi della meccanica quantistica e uno dei più importanti è il principio di sovrapposizione che afferma appunto che due oggetti quantistici possono essere sommati ("sovrapposti"). Il risultato è appunto un oggetto quantistico con uno stato rappresentato come sovrapposizione di due o più stati distinti (nel nostro caso due).

5 Protocollo BB84 e Photon Number Splitting Attack

Il protocollo BB84 è stato il primo protocollo crittografico quantistico. A livello pratico, è stato implementato tramite impulsi laser attenuati, cioè sorgenti non a particella singola. Queste sorgenti non emettono radiazione continua, ma generano impulsi multifotone a intensità assai ridotta, ossia sorgenti in cui ogni impulso emesso può contenere più di un fotone. La probabilità di produrre n fotoni in un segnale è data dalla funzione di probabilità di massa della distribuzione di Poisson, ossia $P(n|\mu) = e^{-\mu}\mu^n/n!$ dove μ è l'intensità o numero medio di fotoni presenti in un impulso. Nella maggior parte delle implementazioni, vengono utilizzati impulsi laser attenuati ad un livello molto basso per poter inviare gli stati quantistici: 0.2 fotoni ad impulso, quindi molto attenuati. Questo significa che la maggior parte degli impulsi non contiene effettivamente fotoni, qualche impulso contiene un fotone e pochi impulsi contengono due o più fotoni. Una delle vulnerabilità di tale implementazione di questo protocollo è l'attacco photon number splitting. Consideriamo una situazione reale in cui un utente A invia stati quantistici ad un altro utente B usando fotoni: se l'impulso contiene più di un fotone, una terza parte può separare i fotoni extra e trasmettere il singolo fotone rimanente a B. Questa terza parte, detta Eve, immagazzina questi fotoni extra in una memoria quantistica finché B non rileva il singolo fotone rimanente e A non rivela la base di codifica. Eve può quindi misurare i fotoni nella base corretta e ottenere informazioni sulla chiave senza errori. Un'ottima soluzione a questo tipo di problema è utilizzare il protocollo SARG04.

6 Protocollo SARG04

Il protocollo SARG04 (Scarani, Agis, Ribordy and Gisin, 2004) è un protocollo crittografico quantistico creato a partire dal protocollo BB84. I ricercatori lo progettarono quando scoprirono che usando i quattro stati del protocollo BB84 ma con una differente codifica, avrebbero potuto ottenere maggiore robustezza, specialmente verso l'attacco photon number splitting. Per questo protocollo possiamo identificare due basi: $B_1 : \{|0\rangle, |1\rangle\}$ e $B_2 : \{|0_+\rangle, |1_+\rangle\}$. La relazione fra le due basi è la seguente:

$$|\Psi_{00}\rangle = |0\rangle = \frac{|0_+\rangle + |1_+\rangle}{\sqrt{2}}$$

$$|\Psi_{10}\rangle = |1\rangle = \frac{|0_+\rangle - |1_+\rangle}{\sqrt{2}}$$

$$|\Psi_{01}\rangle = |0_+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\Psi_{11}\rangle = |1_+\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Attraverso questa notazione vogliamo evidenziare che l'informazione logica 0 può essere codificata come 0 o 0_+ e l'informazione logica 1 come 1 o 1_+.
Partendo dalle relazioni appena descritte, secondo il primo postulato della misura, vediamo che se misuriamo nella base B_1 gli stati $|0\rangle$ e $|1\rangle$, otterremo il corrispondente autovalore con probabilità 1; se invece gli stessi stati vengono misurati nella base B_2, l'output sarà l'autovalore associato $|0_+\rangle$ il 50% delle volte e l'autovalore associato a $|1_+\rangle$ il rimanente 50%. In maniera analoga, se misuriamo nella base B_2 gli stati $|0_+\rangle$ e $|1_+\rangle$, otterremo il corrispondente autovalore con probabilità 1, mentre se gli stessi stati vengono misurati nella base B_1, l'output sarà l'autovalore associato a $|0\rangle$ il 50% delle volte e l'autovalore associato a $|1\rangle$ il rimanente 50%.
Inizialmente abbiamo due utenti A e B, chiamati ad esempio Alice e Bob. Alice desidera mandare una chiave privata a Bob. Alice genera due stringhe di bit casuali, a e b, entrambe di lunghezza n che rappresentano rispettivamente la stringa contenente il messaggio e la stringa che determina la base in cui codificare i bit del messaggio. Una volta che queste due stringhe sono state generate, Alice codifica a come una stringa di n qubit,

$$|\Psi\rangle = \bigotimes_1^n |\Psi_{a_i b_i}\rangle .$$

a_i e b_i sono rispettivamente l'i-esimo bit di a e di b. In particolare, il bit b_i ci indica in quale base codificare a_i: se b_i vale 0 allora a_i verrà codificato nella base B_1 (base canonica), altrimenti verrà codificato nella base B_2 (base di Hadamard). Una volta preparato $|\Psi\rangle$, Alice invierà questa stringa di qubit attraverso un canale quantistico pubblico. Dal momento che solo Alice conosce b e questi stati non sono mutuamente ortogonali, è virtualmente impossibile sia per Bob e che per un eventuale hacker distinguerli con certezza senza conoscere appunto b. Una volta ricevuta la stringa di qubit $|\Psi\rangle$, Bob genera una stringa di bit casuali b' di lunghezza n che userà per scegliere su quale base misurare questi qubit trasmessi da Alice. A questo punto, Bob annuncia pubblicamente che ha ricevuto i qubit $|\Psi\rangle$. Per ogni qubit di $|\Psi\rangle$, Alice sceglie uno stato della base B_1 e uno stato della base B_2 e li annuncia. Ora Bob sa gli stati possibili di tutti i qubit ricevuti da Alice, ma deve riuscire a distinguerli. Per fare ciò, Bob misura ogni qubit sulla base B_1 o B_2 a seconda dei valori dei singoli bit della stringa b' da lui generata. Una volta che ogni qubit è stato misurato, Bob può controllare se gli stati risultanti sono consistenti o meno con gli stati scelti da Alice. Se lo stato misurato è consistente con uno dei due stati annunciati da Alice, Bob annuncia che il risultato della misura è invalido dato che non

può distinguere i due stati. Al contrario, se lo stato misurato è incosistente con entrambi gli stati, allora Bob annuncia che il bit della misura è valido e quindi lo inverte con un bit-flip. Una volta che Bob ha ottenuto tutti i bit validi, Alice e Bob scelgono i primi $k/2$ bit comunicando tramite un canale pubblico. Infine, Bob e Alice stabiliscono un grado di correlazione minimo (ad esempio 90%) e se questi $k/2$ bit rispettano tale grado, allora condividono una chiave segreta. Se invece questi $k/2$ bit non rispettano tale grado, il protocollo viene annullato e riattivato su canali intercettabili. In assenza di un hacker, la correlazione è totale. Un esempio di esecuzione può essere riassunto tramite la tabella 1 dove, a partire dalla stringa 0011, Alice e Bob scelgono la prima metà e stabiliscono che il grado di correlazione deve essere almeno del 90% ed essendo che il controllo va a buon fine, entrambi condividono la chiave 00.

stringa logica A	0	1	1	0	1	1	1	0
stringa base A	0	0	1	0	0	0	1	0
qubit A	$\|0\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|0\rangle$
stati annunciati A	$\|0\rangle/\|0_+\rangle$	$\|1\rangle/\|1_+\rangle$	$\|1\rangle/\|1_+\rangle$	$\|0\rangle/\|0_+\rangle$	$\|1\rangle/\|1_+\rangle$	$\|1\rangle/\|1_+\rangle$	$\|1\rangle/\|1_+\rangle$	$\|0\rangle/\|0_+\rangle$
stringa base B	1	0	1	1	0	1	0	0
stato risultante B	$\|1_+\rangle$	$\|1\rangle$	$\|1_+\rangle$	$\|1_+\rangle$	$\|1\rangle$	$\|0_+\rangle$	$\|0\rangle$	$\|0\rangle$
misura B	1	1	1	1	1	0	0	0
stringa logica B	**0**	1	1	**0**	1	**1**	**1**	0

Table 1: Esecuzione del protocollo

7 Sicurezza e Prestazioni

Il protocollo SARG04 è meno efficiente rispetto al BB84 in quanto scarta un numero maggiore di bit, ma risulta assai più robusto agli attacchi PNS. Nelle implementazioni a singolo fotone, è stato tuttavia dimostrato sperimentalmente che il protocollo SARG04 è meno robusto a questo tipo di attacco rispetto al BB84. È stato inoltre dimostrato che in una two-way communication, il protocollo SARG04 può tollerare un maggiore tasso di errore sui bit (19.4% per una sorgente a un fotone e 6.56% per una sorgente a due fotoni) rispetto ad una comunicazione one-way (10.95% per una sorgente a un fotone e 2.71% per una sorgente a due fotoni).

Bibliografia

[1] Minal Lopes e Dr. Nisha Sarwade, *Cryptography from Quantum Mechanical viewpoint* (2014).

[2] Valerio Scarani, Antonio Acin, Gregoire Ribordy e Nicolas Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations* (2004).

[3] Piccoli Gioele, *Distribuzione Quantistica di Chiavi con Metodo Measurement-Device-Indipendent* (2015).

Sitografia

[1] `https://en.wikipedia.org/wiki/SARG04`