Crittografia Quantistica

Home Assignment svolto da:

- La Corte, S4784539
- Pignone, S4838155
- Scarrà, S4798949
- Stalfieri, S4484723

Indice:

La crittografia quantistica è il ramo della quantistica più evoluto, in quanto offre enormi vantaggi rispetto al corrispettivo classico.

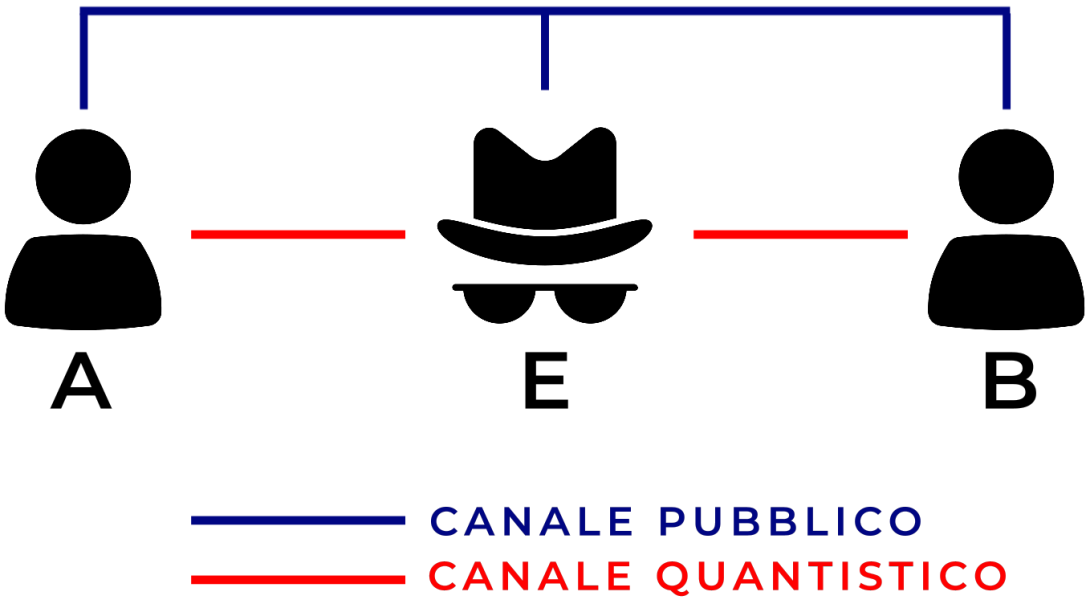
In particolare, si basa sul teorema no-cloning e sul concetto di misura con il fine ultimo di ottenere una chiave privata condivisa in un canale di comunicazione non sicuro.

Implementazione del Protocollo

Consideriamo tre entità:

- *A* e *B*, interlocutori che hanno lo scopo di ottenere una chiave simmetrica condivisa,

- *E*, possibile attaccante.



Definiamo un ***n***, che varia a seconda delle esecuzioni del protocollo: più esso sarà elevato più il protocollo risulterà sicuro, ovvero protetto da un possibile attacco di *E*.

Nelle varie esecuzioni abbiamo utilizzato diversi valori di ***n*** al fine di raccogliere una quantità significativa di dati, in particolare ***n* = [4, 8, 16, 32, 64, 128]**.

Il protocollo si sviluppa in 4 fasi:

1. *A* estrae:
    a. *n* bit logici generati casualmente,
    b. *n* bit per la base generati casualmente.

A codifica quindi i bit logici nella base estratta e invia la stringa di qubit risultante a *B*, attraverso un canale quantistico non sicuro;

Quello che sa A	Quello che sa E	Quello che sa B
Bit Logici di A		
Basi di A		

Quello che sa A	Quello che sa E	Quello che sa B
Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base

2. *B* a sua volta estrae una stringa di *n* bit classici che determina, per ogni bit, in che base effettuare la misura.

Quello che sa A	Quello che sa E	Quello che sa B
Bit Logici di A		
Basi di A		
Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base
		Basi di B
		Risultati delle misure di B

3. *A* e *B* si scambiano le basi, pubblicandole attraverso un canale di informazione classico e visibile a tutti (anche ad *E*).

   A e *B* a questo punto sanno quali dei loro bit logici sono deterministicamente correlati e quali invece lo sono soltanto probabilisticamente; i secondi vengono scartati.

Quello che sa A	Quello che sa E	Quello che sa B
Bit Logici di A		
Basi di A		
Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base
		Basi di B
		Risultati delle misure di B
Basi di A e B	Basi di A e B	Basi di A e B

4. A questo punto entrambe le parti hanno circa $n/2$ qubit in correlazione, e di questi ne pubblicano la metà (ovvero un quarto di quelli di partenza).

Se tutti i qubit corrispondono *E* non si è intromessa nella comunicazione e gli altri $n/4$ qubit costituiscono la chiave condivisa e privata tra *A* e *B*.

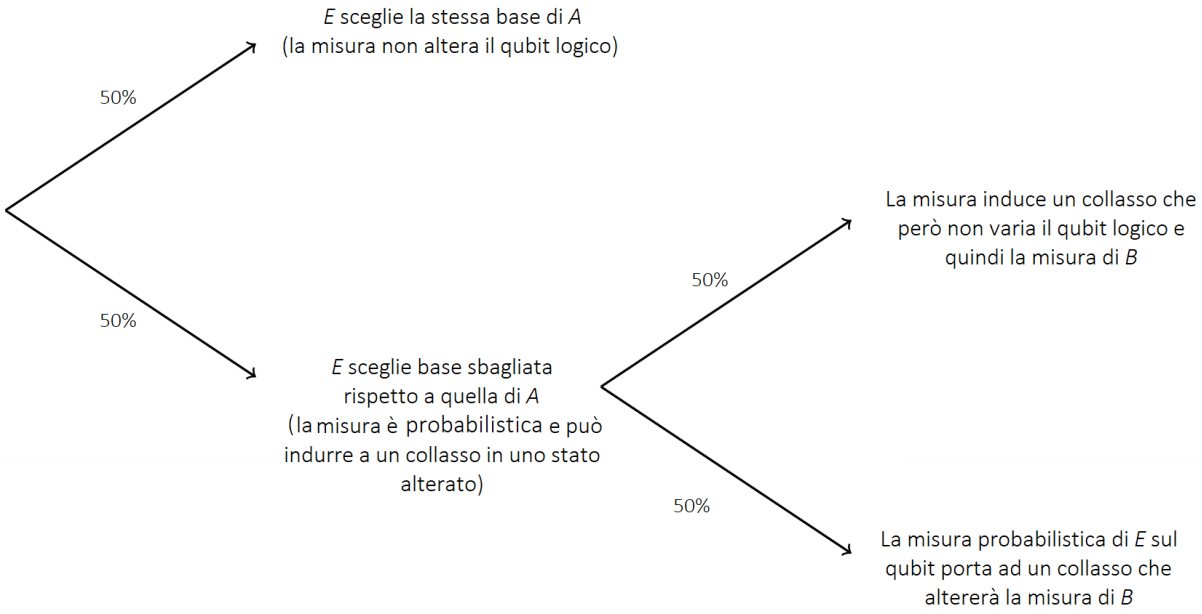
Quello che sa A	Quello che sa E	Quello che sa B
Bit Logici di A		
Basi di A		
Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base	Bit Logici di A codificati nella sua Base
		Basi di B
		Risultati delle misure di B
Basi di A e B	Basi di A e B	Basi di A e B
Pubblicazione dei bit di A e B	Pubblicazione dei bit di A e B	Pubblicazione dei bit di A e B
Chiave condivisa		Chiave condivisa

Possibile Vulnerabilità

L'attaccante *E* può inserirsi nella comunicazione e osservare la stringa di qubit inviata da *A* a *B:* può simulare quindi il comportamento di *B* estraendo una stringa di bit, ovvero le basi per la misura.

A questo punto, per ogni qubit:

- con il 50% di probabilità *E* indovinerà la base, effettuerà una misura sul qubit e non altererà il messaggio,
- con il 50% di probabilità *E* non indovinerà la base ed effettuando una misura sul qubit:
  - nella metà dei casi (25% del totale), la misura provocherà un collasso nello stesso stato misurato da *B*, che quindi non si accorgerà di nulla;
  - nell'altra metà dei casi, la misura provocherà un collasso nello stato sbagliato, alterando la misura di *B*, che otterrà un valore sicuramente diverso da *A*.



La probabilità che *E* **non** venga scoperta è quindi $(0,75)^{\lambda}$, dove λ è il numero di bit pubblicati.

Al contrario, la probabilità che *E* venga scoperta è quindi $1-(0,75)^{\lambda}$.

Risultati Attesi

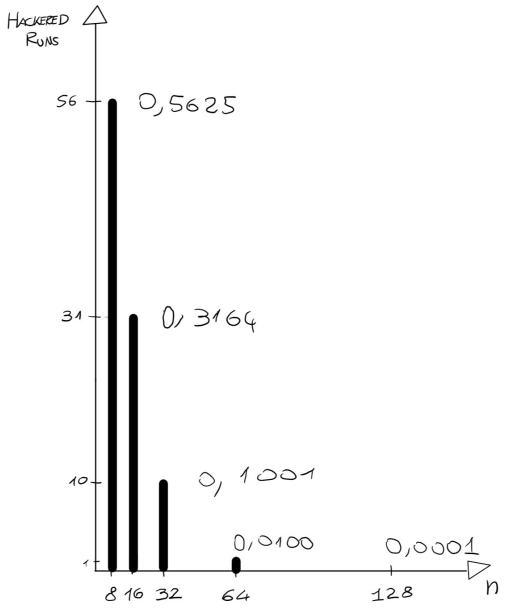
Ci aspettiamo che la probabilità di scovare l'attaccante cresca al crescere del numero di bit (*n*) usati.

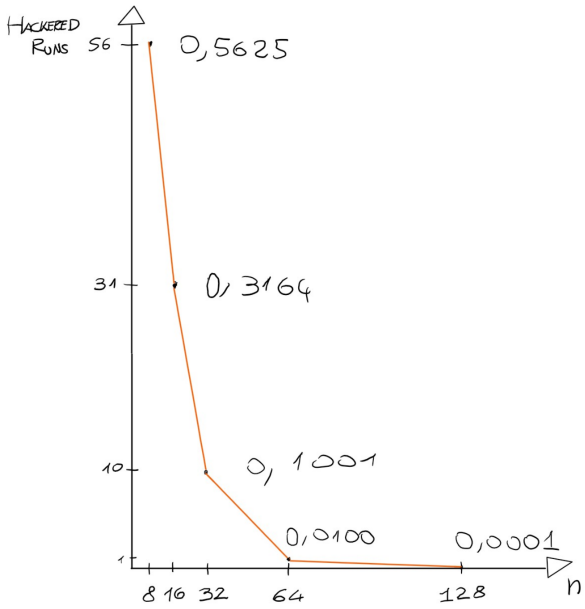
Previsioni Statistiche

Andiamo ora a commentare quello che ci aspettiamo con 1000 esecuzioni del protocollo:

n	λ	Probabilità Teorica che l'attaccante (ovvero *E*) **non** venga scoperto	Hackered Runs sulle 1000 totali
4	1	0,7500	750
8	2	0,5625	562
16	4	0,3164	316
32	8	0,1001	100
64	16	0,0100	10
128	32	0,0001	0

Rappresentate graficamente nel sottostante abbozzo di grafico:





Risultati Ottenuti

Andiamo ad analizzare prima i dati delle singole esecuzioni e poi i dati statistici.

Nell'implementazione del protocollo *E* non induce direttamente ad un collasso nei qubit logici del messaggio poiché questo non era facilmente realizzabile in qiskit; al contrario *E* altera la base del qubit e sovrascrive il messaggio sul canale pubblico, rendendo la futura misura di *B* probabilistica e quindi, nella metà dei casi, errata.

I qubit alterati da *E* sono infatti poi misurati da *B,* ed è lì che, probabilisticamente, essi possono risultare alterati rispetto a quelli di *A.*

Nella pratica il comportamento che otteniamo è del tutto analogo a quello che ci aspettiamo a livello teorico.

E non Scoperta

In questo esempio utilizziamo $n = 8$, un numero di bit basso per il quale la probabilità che *E* non sia scoperta è del 56% circa; andiamo ad eseguire i vari passi:

Bit Logici di A: [0 0 1 1 1 0 0 0]
Bit di Base di A: [1 0 0 1 1 0 1 0]

E si intromette, sceglie 5 basi corrette e 3 sbagliate:

Bit di Base di E: [1 0 0 **0 0 1** 1 0]
Misura di E: [0 0 1 0 0 0 0 0]

BASE SBAGLIATA: *E* POTREBBE ALTERARE LA MISURA DI *B*

Adesso è il turno di *B*, che sceglie le basi (ne sceglie giuste 5), misura e poi scarta i bit che sono derivati dalla misura in base sbagliata (contrassegnati con ?):

Bit di Base di B: [**0** 0 **1** 1 1 0 **0** 0]
Misura di B: [? 0 ? 1 1 1 ? 0]

Delle 3 misure probabilistiche causate da *E,* una risulta errata: a questo punto l'unico bit che risulta sbagliato per *B* (a causa dell'attaccante) è il terzultimo.

Bit Logici di A: [0 0 1 1 1 0 0 0]
Misura di E: [0 0 1 0 0 0 0 0]
Misura di B: [? 0 ? 1 1 1 ? 0]

LA MISURA, PROBABILISTICA PER COLPA DI *E*, E' SBAGLIATA
LA MISURA, PROBABILISTICA PER COLPA DI *E*, E' CORRETTA

B pensa quindi che i suoi 5 bit rimasti siano uguali a quelli di *A* e ne pubblica 2 per verificare che non ci sia stato un attacco.

Se *A* e *B* pubblicassero il terzultimo bit scoprirebbero l'attacco di *E* ma sfortunatamente le due parti non estraggono il bit alterato;

Chiave Pulita di A: [0 1 1 **0** 0]
Chiave Pulita di B: [0 1 1 **1** 0]
Indici dei Bit da Pubblicare Selezionati: [2 0]

non viene estratto l'indice 3 che avrebbe scovato E

Risultati Finali:

Chiave Privata di A: [1 0 0]
Chiave Privata di B: [1 1 0]

Bit pubblicati da A: [1 0]
Bit pubblicati da B: [1 0]

Eve **non scoperta**.

E Scoperta

In questo esempio utilizziamo nuovamente $n = 8$, ma *E* viene scoperta:

Bit Logici di A: [1 1 1 0 0 1 0 0]
Bit di Base di A: [1 0 0 0 1 1 1 1]

E si intromette, sceglie 3 basi corrette e 5 sbagliate:

Bit di Base di E: [**0 1 1** 0 **0 0** 1 1]
Misura di E: [0 1 0 0 1 0 0 0]

BASE SBAGLIATA: *E* POTREBBE ALTERARE LA MISURA DI *B*

A questo punto è il turno di *B*, che sceglie le basi (ne sceglie giuste 5), misura, e poi scarta i bit che sono derivati dalla misura in base sbagliata (contrassegnati con ?):

Bit di Base di B: [1 0 **1** 0 **0** 1 **0** 1]
Misura di B: [0 1 ? 0 ? 0 ? 0]

Delle 5 misure probabilistiche causate da *E:*

- 2 non ci interessano perché quei bit sono scartati,
- una risulta corretta e non altera il bit logico,

- due alterano il bit logico.

Quindi due bit, in posizioni 0 e 5, risultano sbagliati (a causa dell'attaccante).

💡 Bit Logici di A: [1 1 1 0 0 1 0 0]
Misura di E: [0 1 0 0 1 0 0 0]
Misura di B: [0 1 ? 0 ? 0 ? 0]

LA MISURA, PROBABILISTICA PER COLPA DI *E*, E' SBAGLIATA
LA MISURA, PROBABILISTICA PER COLPA DI *E*, E' CORRETTA

A questo punto *B* pensa che i 5 bit rimasti siano uguali a quelli di *A*; ne pubblica 2 per verificare che non ci sia stato un attacco:

💡 Chiave Pulita di A: [**1** 1 0 **1** 0]
Chiave Pulita di B: [**0** 1 0 **0** 0]
Indici dei Bit da Pubblicare Selezionati: [0 2]

viene estratto l'indice 0 che scova E

Risultati Finali:

💡 Chiave Privata di A: [1 1 0]
Chiave Privata di B: [1 0 0]

Bit pubblicati da A: [1 0]
Bit pubblicati da B: [0 0]

Eve **scoperta**, la chiave è sbagliata e verrà ricalcolata.

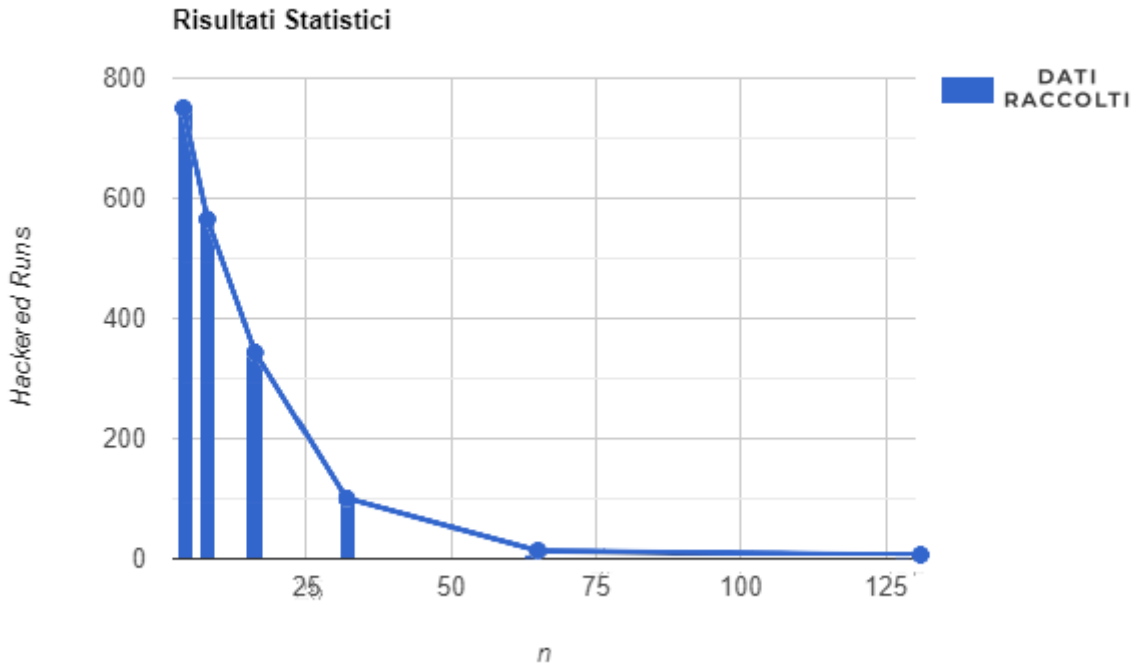
Risultati Statistici

Abbiamo eseguito il protocollo al variare di *n*, con 1000 esecuzioni, raccogliendo i dati nella tabella sottostante:

n	λ	Probabilità Teorica che l'attaccante (ovvero E) **non** venga scoperto	Probabilità Empirica che l'attaccante (ovvero E) **non** venga scoperto	Errore in Percentuale:
4	1	0,7500	0,757	0,93%
8	2	0,5625	0,572	1,68%
16	4	0,3164	0,350	10,6%
32	8	0,1001	0,094	6,1%
64	16	0,0100	0,007	30%
128	32	0,0001	0	/

L'unico errore che risulta elevato in percentuale si riferisce a un campione di dati troppo risicato per costituire una buona base statistica; negli altri casi il numero di volte in cui *E* non viene scoperta è molto maggiore, il campione statistico è molto più grande e gli errori molto più contenuti.

Abbiamo quindi raccolto i dati nel grafico sottostante (istogramma + curva):



Difficoltà Incontrate

Inizialmente abbiamo commesso un errore grave che ha pregiudicato per giorni la misurazione dei risultati statistici; in pratica la misura di *E* non veniva riportata a *B*, che quindi leggeva il messaggio come se esso non fosse stato intercettato.

Per risolvere il problema, una volta che *E* riceve il messaggio e lo misura con le sue basi, ricostruisce il circuito quantistico, per poi rimandare il messaggio ricodificato a *B.*

In questo modo *B* riceve i qubit alterati e, a seconda della sua misura su essi e della pubblicazione dei bit, scova o meno l'attaccante.

Conclusioni

L'andamento asintotico empirico risultante corrisponde a quello teorico.

Nel confronto i risultati sono leggermente differenti ma questo non è sorprendente considerando la quantità non troppo elevata di dati raccolti e le possibili imprecisioni di estrazioni e misure probabilistiche.

Codice sorgente del laboratorio in versione pdf:

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/05981867-c613-416f-b36a-60ded2f57f40/BB84.pdf