Analisi teorica, implementazione ed esecuzione su computer quantistico del protocollo BB84

Università degli Studi di Milano – Bicocca

Laurea Triennale in Fisica

25 febbraio 2021

Candidato: Davide Rinaldi

Matricola: 826346

Relatore interno: Dr. Andrea Giachero

Relatore esterno: Prof. Paolo Solinas

Correlatrice: Dr. Elena Ferri

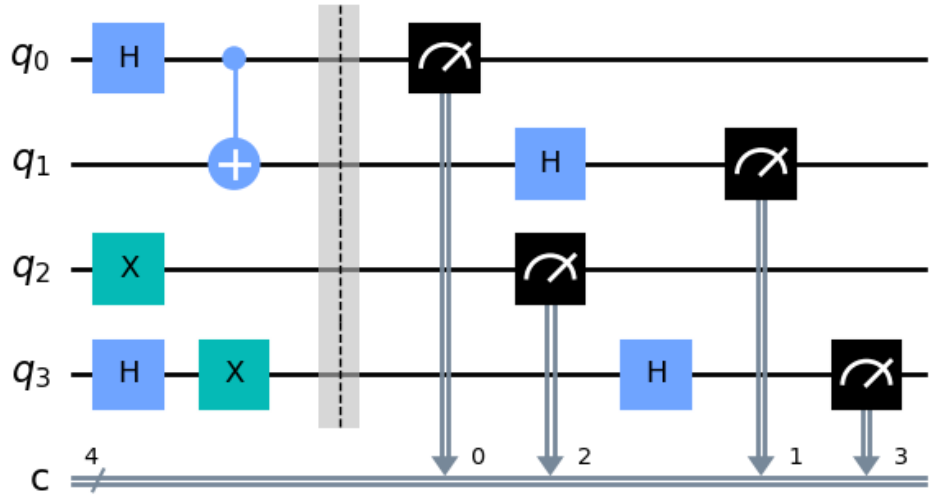
Outline

1. Quantum Computing
2. Il protocollo BB84 – Quantum Computing per la crittografia quantistica
3. Simulazione del protocollo
4. Esecuzione su computer quantistico

Qubit: sistema a due livelli soggetto alle leggi della Meccanica Quantistica

Base computazionale: $|0\rangle, |1\rangle$

Base $|+\rangle, |-\rangle$: $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$



IBM Quantum Experience : **Qiskit**

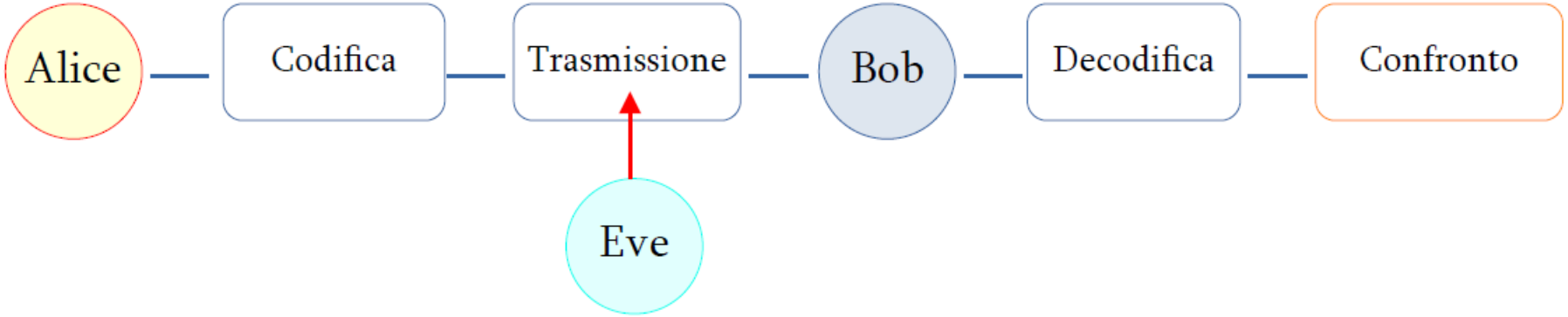
Il protocollo BB84 – Quantum Computing per la crittografia quantistica

- Ideato nel 1984 da C. H. Bennett e G. Brassard
- Protocollo a chiave privata di *Quantum Key Distribution* (QKD)
- Condivisione sicura di una chiave crittografica
- **Individuazione sistematica dell'hacker**

Il protocollo BB84 – Fenomeni quantistici coinvolti

- Sovrapposizione degli stati fisici
- Collasso della funzione d'onda dopo una misura
- Teorema di no-cloning → non è possibile copiare lo stato dei qubit trasmessi
- Misura sui qubit trasmessi → modifica dello stato dei qubit → perturbazione nei risultati

Il protocollo BB84 – Funzionamento



	Pubblici				Privati			
Stringa dei bit codificati da Alice:	**1**	*0*	**1**	*0*	**1**	*1*	**0**	**0**
Stringa delle basi di Alice:	$\underline{0}$	1	$\underline{1}$	0	$\underline{0}$	0	$\underline{1}$	$\underline{0}$
Qubit:	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
Stringa delle basi di Bob:	$\underline{0}$	0	$\underline{1}$	1	$\underline{0}$	1	$\underline{1}$	$\underline{0}$
Stringa dei risultati di Bob:	**1**	*0*	**1**	*1*	**1**	*0*	**0**	**0**
Salvati (✓) o scartati (✗):	✓	✗	✓	✗	✓	✗	✓	✓

Il protocollo BB84 – Attese teoriche

1. **Assenza dell'hacker**

Percentuale bit correlati **identici** = $P_{identici}$ = 100%

Percentuale bit correlati **diversi** = $P_{diversi}$ = 0%

2. **Attacco hacker**

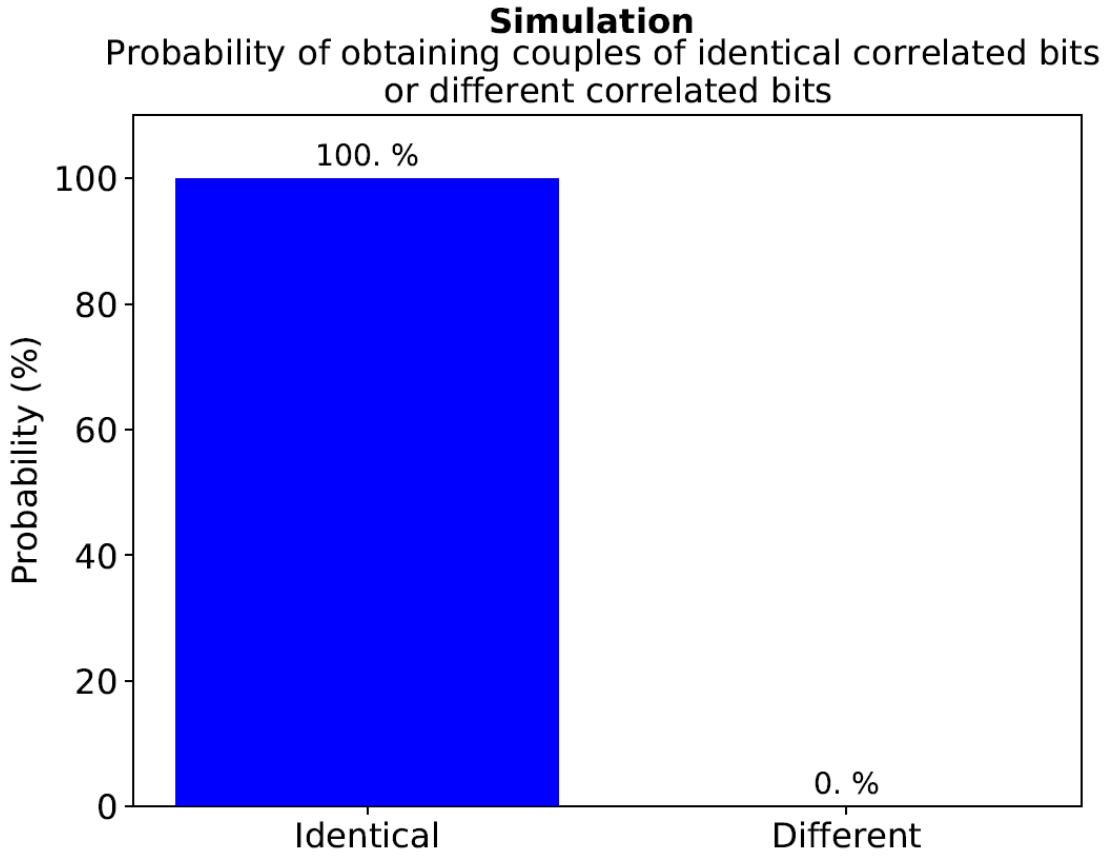
$P_{identici}$ = 75%

$P_{diversi}$ = 25% ⟶ Eve riduce la correlazione

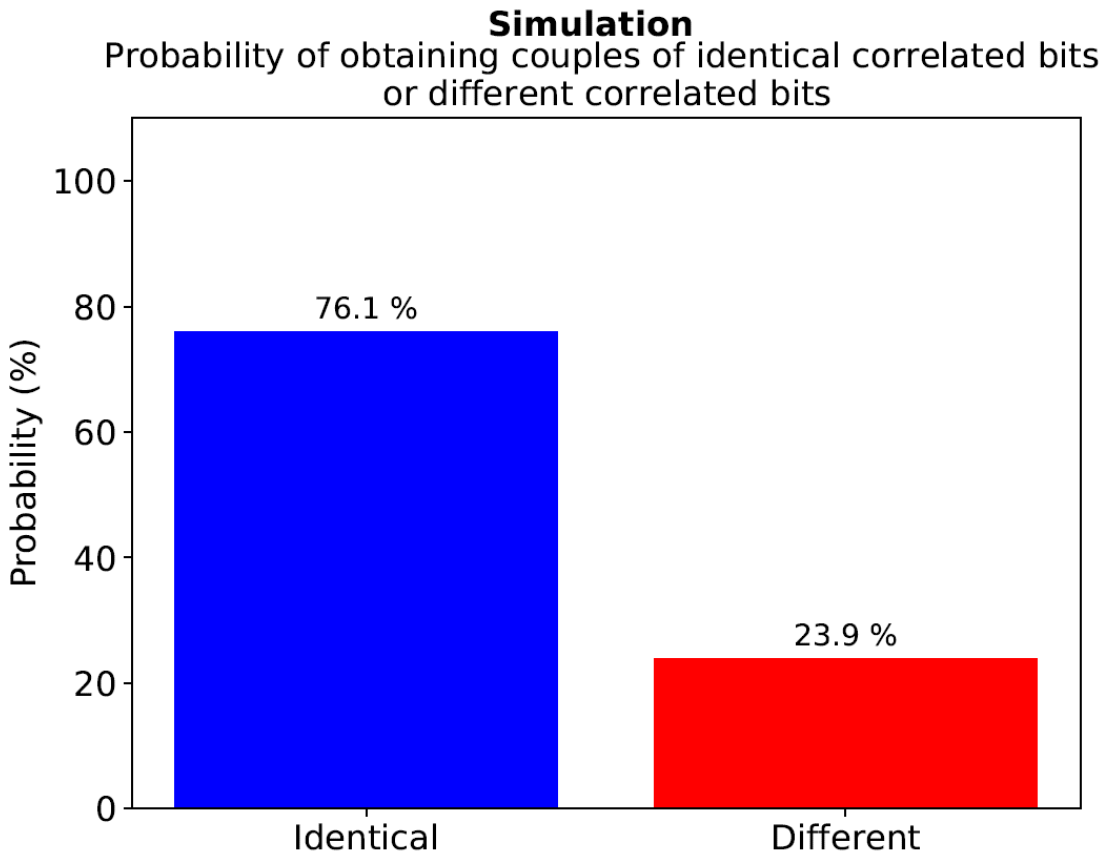
Simulazione del protocollo

Il programma è stato eseguito su un simulatore di IBM per verificarne il corretto funzionamento.

Senza Eve:



Con Eve:



Simulazione del protocollo - risultati

Sono state eseguite 10 simulazioni per ogni scenario.
Ognuna di esse ha simulato la trasmissione di 10000 qubit.

Attese teoriche:

Scenario	$P_{identici}$	$P_{diversi}$
Senza Eve	100%	0%
Con Eve	75%	25%

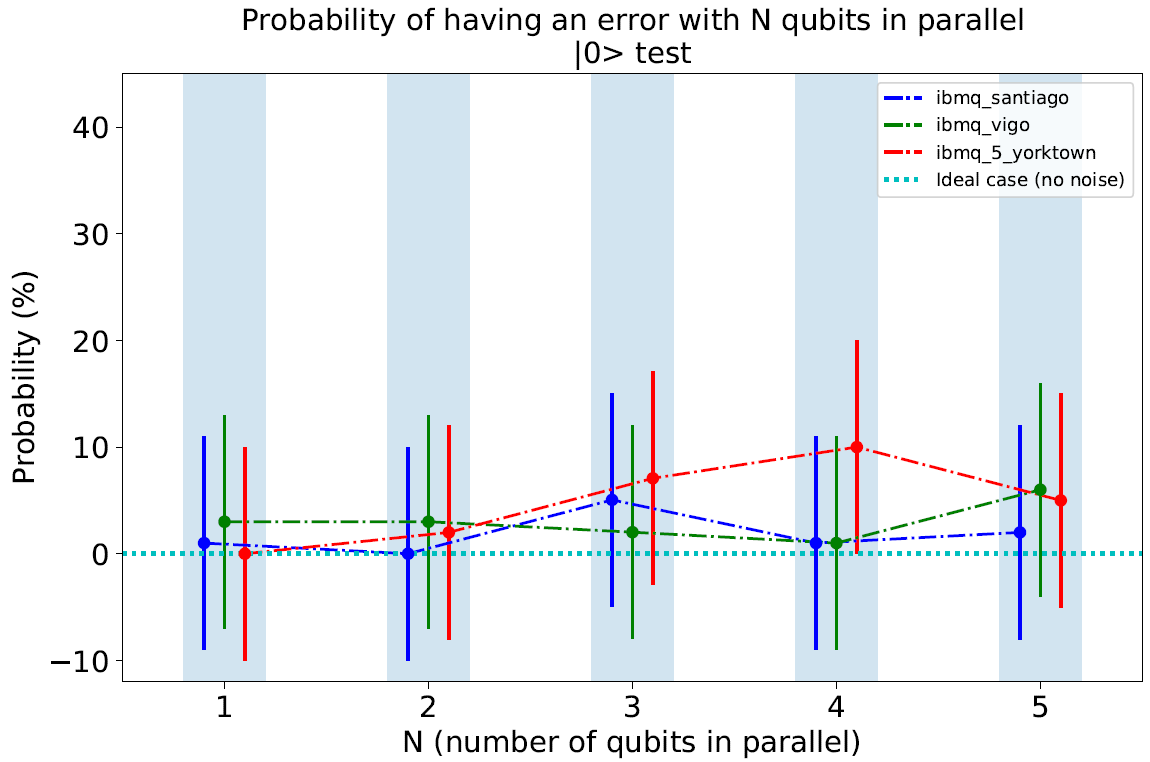
Risultati della simulazione:

Scenario	$P_{identici}$	σ	$P_{diversi}$	σ
Senza Eve	100%	0%	0%	0%
Con Eve	75.2%	$\pm$0.2%	24.8%	$\pm$0.2%

I risultati sono compatibili con i valori attesi.

Esperimento su computer quantistico – scelta dei dispositivi e rumore

- Presenza di rumore ⟶ errori nelle misure
- Caratteristiche dei diversi dispositivi (rate di errore, quantum volume)
- Configurazione dei circuiti quantistici ⟶ numero ottimale di qubit in parallelo ⟶ test preliminari



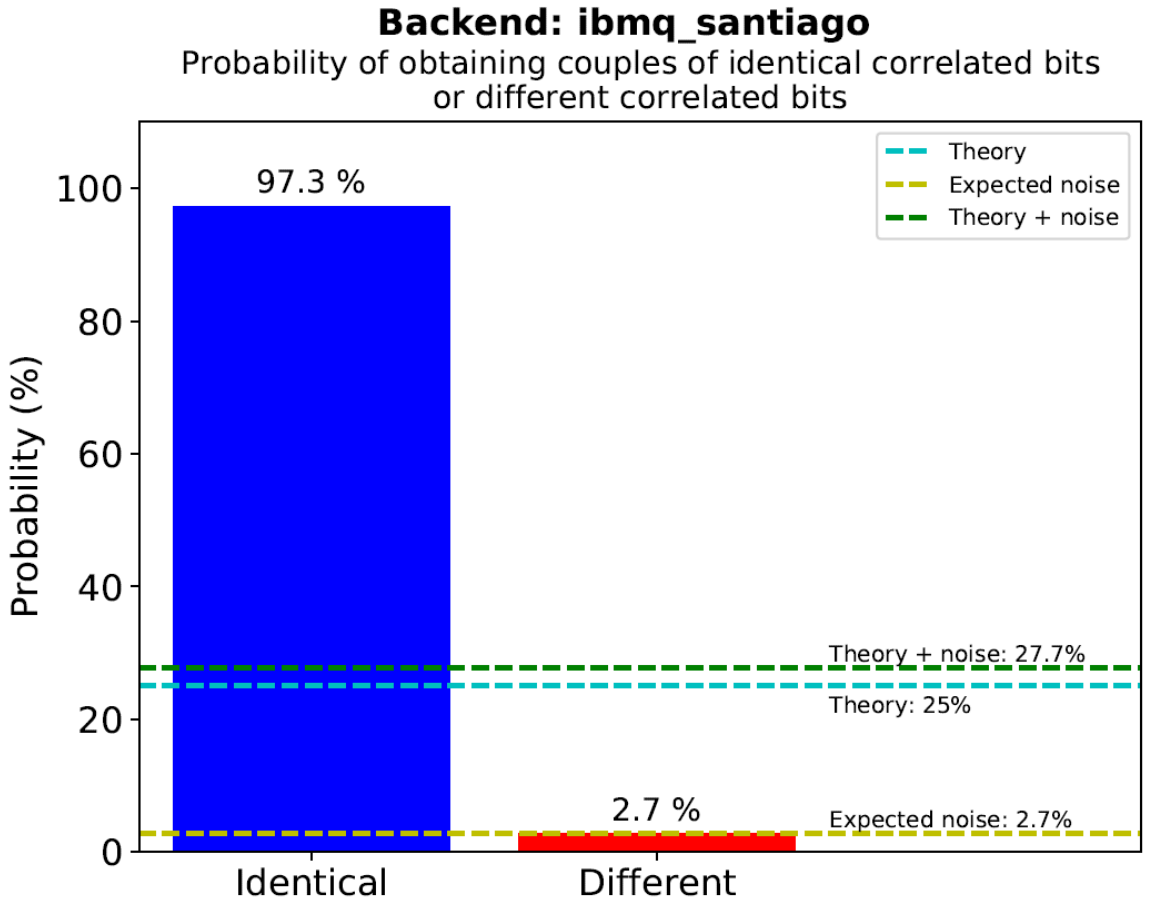
Dispositivi scelti: **ibmq_santiago** e **ibmq_vigo.**
Numero di qubit in parallelo: 5

Esperimento su computer quantistico – ibmq_santiago

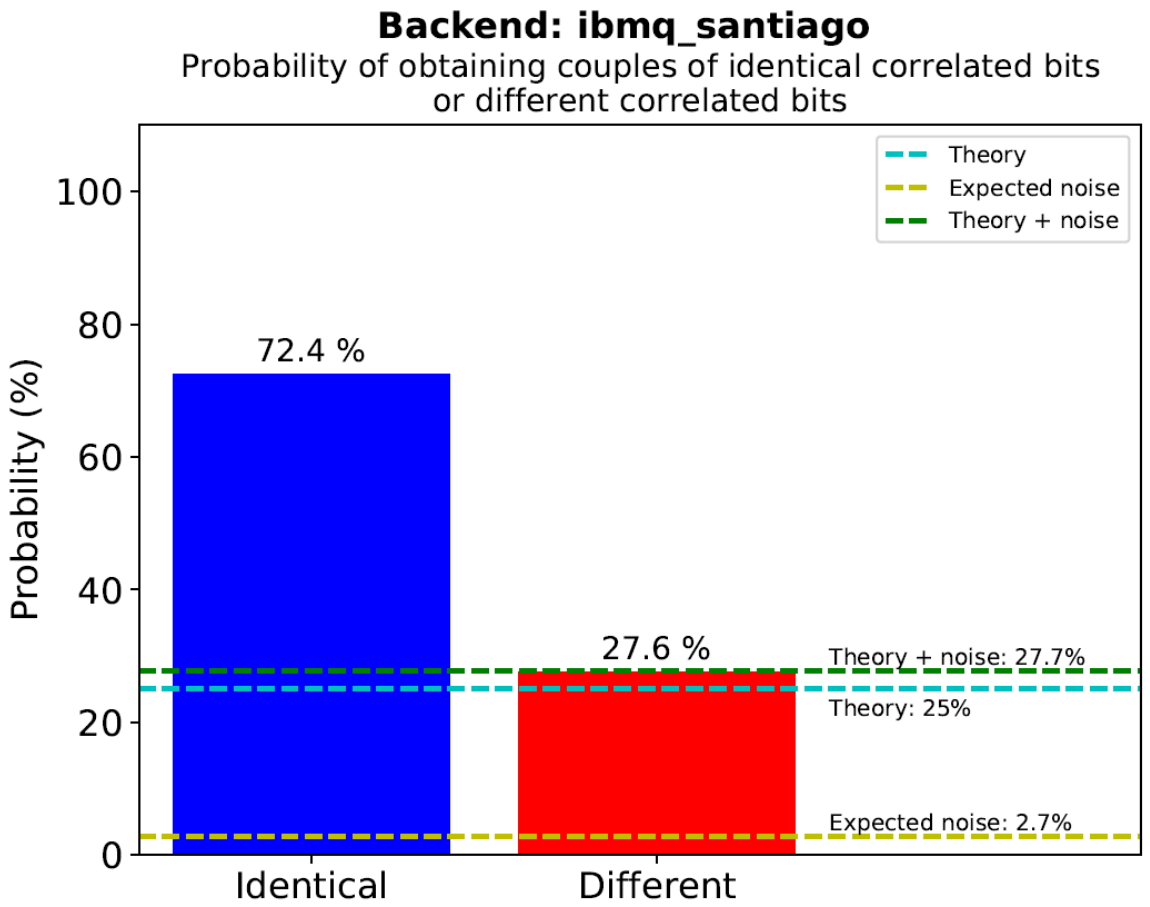
Soglia di rumore = $P_{diversi}$ in assenza dell'hacker = 2.7%

Obiettivo: verificare che, in presenza dell'hacker, $P_{diversi}$ sia superiore alla soglia di rumore.

Senza Eve:



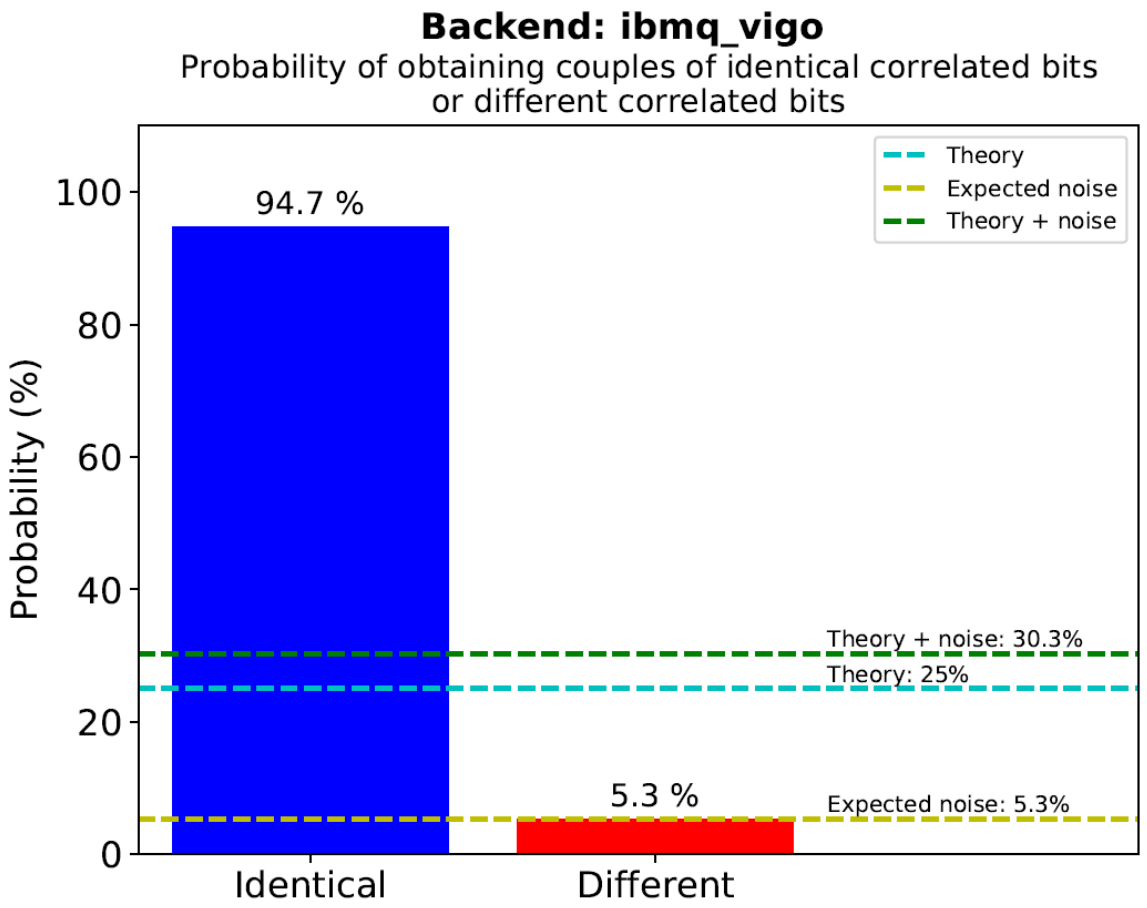
Con Eve:



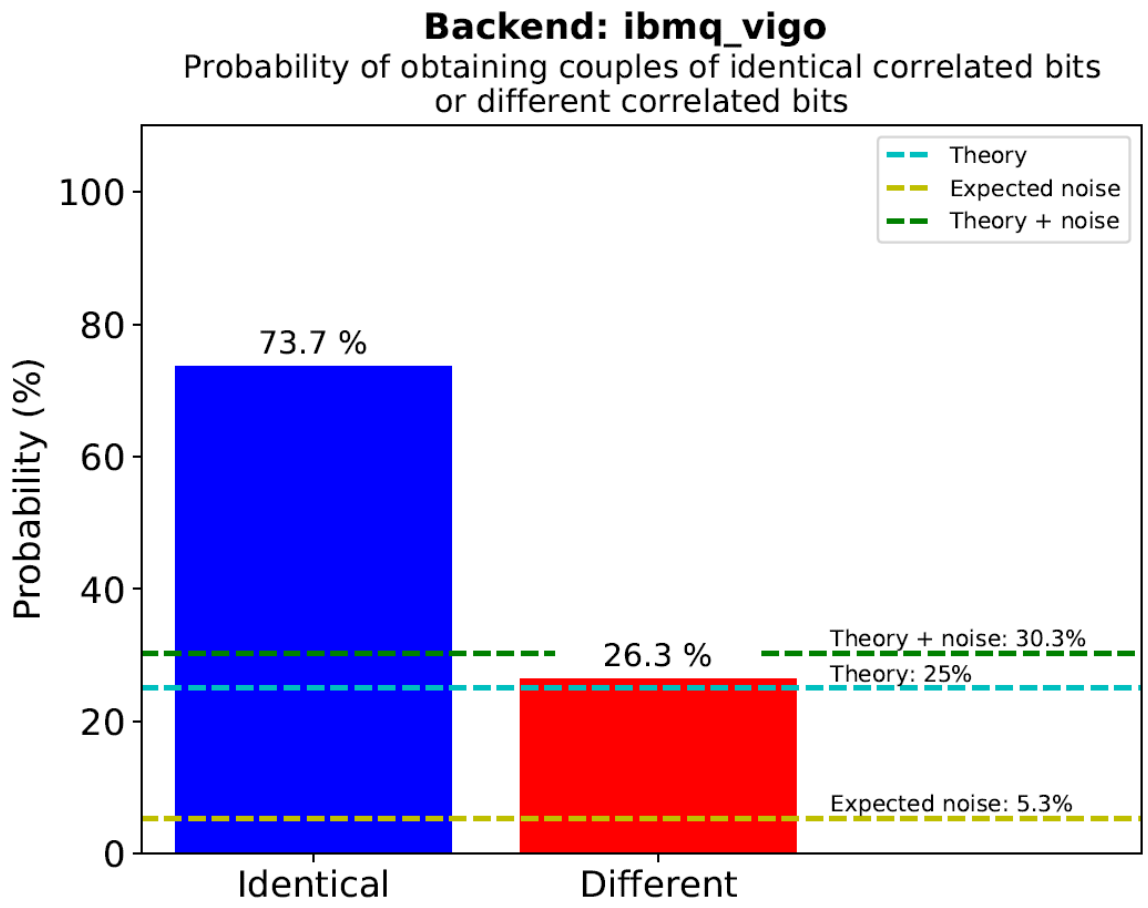
Esperimento su computer quantistico – ibmq_vigo

Soglia di rumore = 5.3%

Senza Eve:



Con Eve:



Esperimento su computer quantistico – risultati

Numero di qubit utilizzati in totale da ogni dispositivo: N = 5000

Errore: $\sigma = \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{5000}} \approx 1.4\%$

Device	Theory + noise	Experimental
ibmq_santiago	$27.7\% \pm 1.4\%$	$27.6\% \pm 1.4\%$
ibmq_vigo	$30.3\% \pm 1.4\%$	$26.3\% \pm 1.4\%$

Soglia di rumore in ibmq_santiago: 2.7% ± 1.4% → Risultato sperimentale: **27.6% ± 1.4% ≫ 2.7% ± 1.4%**

Soglia di rumore in ibmq_vigo: 5.3% ± 1.4% → Risultato sperimentale: **26.3% ± 1.4% ≫ 5.3% ± 1.4%**

La soglia fissata è stata ampiamente superata: l'hacker è stato individuato.

Conclusioni

Il protocollo BB84:

- rende sicura la condivisione di una chiave crittografica privata;
- permette l'individuazione di qualsiasi tipo di intromissione da parte di un hacker;
- non è basato sulla complessità della codifica, ma sulle proprietà di particolari fenomeni quantistici.

L'esperimento sui computer quantistici ha mostrato che, in caso di attacco hacker, la percentuale di bit diversi supera abbondantemente la soglia di rumore.

L'hacker viene quindi sempre individuato, ed il protocollo BB84 risulta essere completamente sicuro.

Applicazioni:

- Protezione di dati sensibili
- Sicurezza in ambito informatico
- Tecnologia sviluppabile su larga scala

Grazie per l'attenzione!

Rumore in un computer quantistico

Il **rumore** dei dispositivi è dovuto a diversi fattori:

- errori nelle misure
- porte quantistiche non ideali
- rumore ambientale, che interferisce con il sistema

→ è molto difficile da stimare

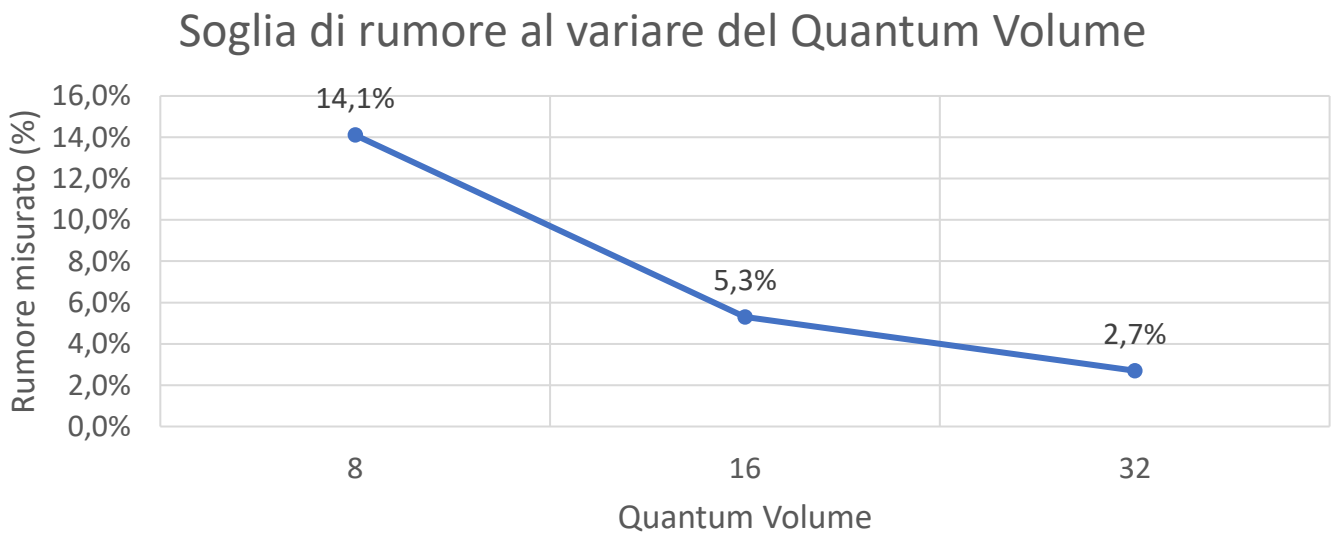
Quantum Volume

Quantum Volume: parametro che descrive la capacità e il rate di errore di un computer quantistico.

Diverse definizioni; la più semplice è (Moll et al.):

$$V_Q = \min[N, d(N)]^2$$

N = numero di qubit del dispositivo, d = profondità del circuito (numero di step)



Principio di sovrapposizione

Un qubit può trovarsi in uno stato che è combinazione lineare dei due stati $|0\rangle$ e $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Risultati possibili di una misura di Z:

- 0 con probabilità $|\alpha|^2$
- 1 con probabilità $|\beta|^2$

Collasso della funzione d'onda

- Misura di Z su $|0\rangle$ oppure $|1\rangle$ ⟶ stato imperturbato
- Misura di X su $|+\rangle$ oppure $|-\rangle$ ⟶ stato imperturbato

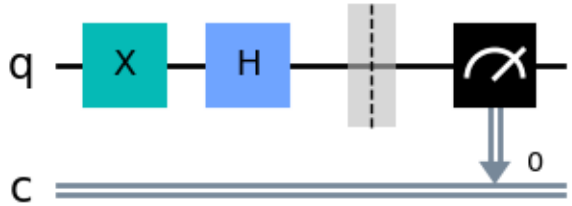
- **Misura di Z su $|+\rangle$ oppure $|-\rangle$** ⟶ lo stato collassa in uno dei due stati $|0\rangle$ e $|1\rangle$
- **Misura di X su $|0\rangle$ oppure $|1\rangle$** ⟶ lo stato collassa in uno dei due stati $|+\rangle$ e $|-\rangle$

Teorema di no - cloning

Non esiste alcuna trasformazione unitaria U che permetta di produrre una copia di un arbitrario qubit ignoto.

- Si possono creare copie soltanto di stati che appartengono alla **stessa base ortonormale.**
- Nel protocollo entrano in gioco **due basi diverse.**
- Eve non può sapere a priori a quale base appartenga lo stato di un qubit, se non **facendo una misura**.

Circuiti quantistici



$$X|0\rangle \equiv |1\rangle \qquad X|1\rangle \equiv |0\rangle$$
$$Y|0\rangle \equiv -i|1\rangle \qquad Y|1\rangle \equiv i|0\rangle$$
$$Z|0\rangle \equiv -|0\rangle \qquad Z|1\rangle \equiv |1\rangle$$

$$H|0\rangle \equiv |+\rangle \qquad H|1\rangle \equiv |-\rangle$$
$$H|+\rangle \equiv |0\rangle \qquad H|-\rangle \equiv |1\rangle$$

Tecnologia

Sistemi superconduttivi

- Trasmon qubit
- Giunzioni Josephson