Esecuzione e analisi del protocollo E91 per Quantum Key Distribution su computer quantistici

28 Febbraio 2023

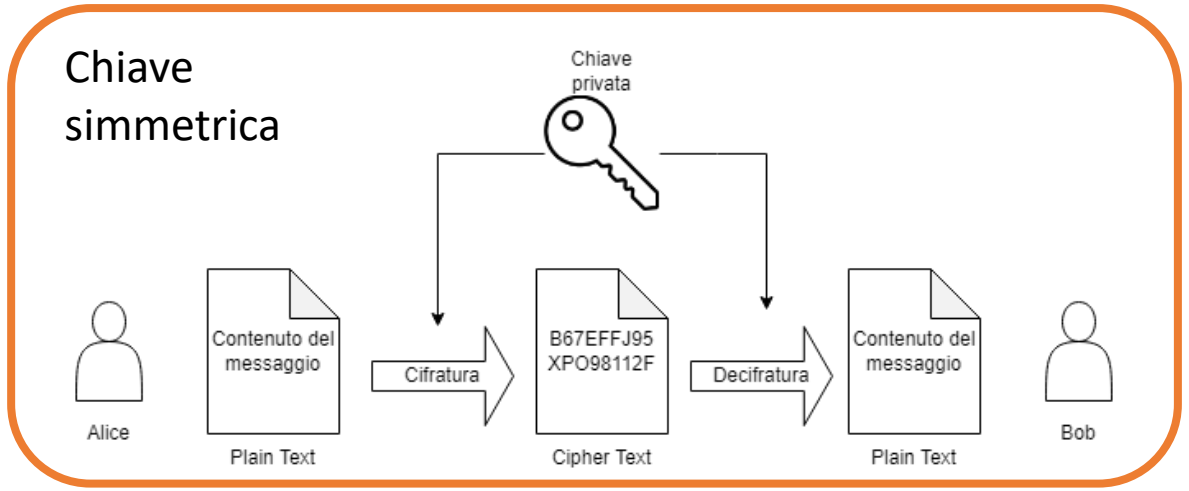
Loris Coppa
Matricola 826237

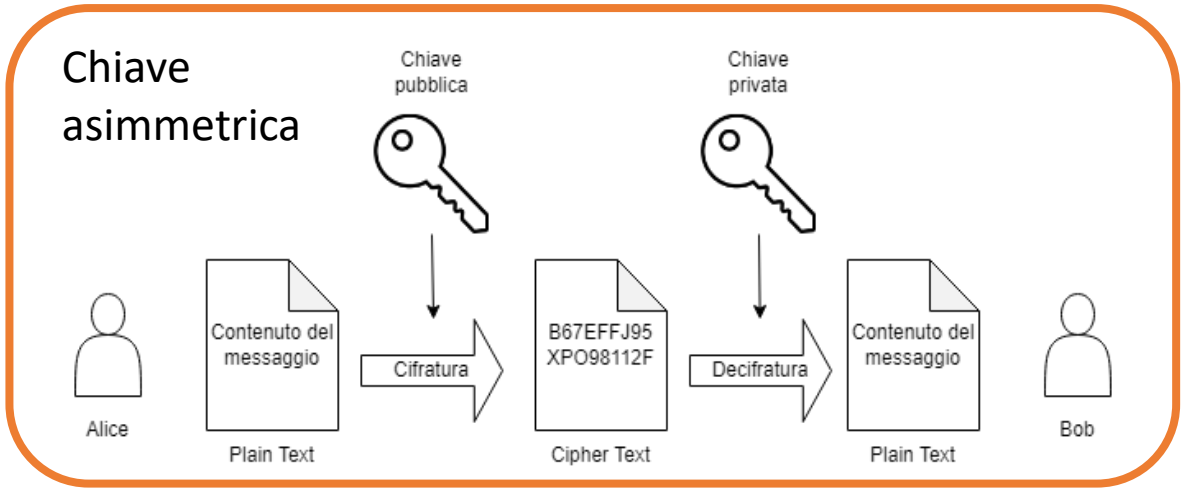
Relatore:
Dr. Andrea Giachero

Correlatore:
Dr. Danilo Labranca

Tipi di crittografia

- Nomenclatura: Alice è il mittente che vuole inviare un messaggio criptato a Bob, il destinatario. Un hacker, Eve, potrebbe cercare di scoprire il contenuto del messaggio;
- Crittografia simmetrica: la stessa chiave viene utilizzata sia per cifrare che per decifrare il messaggio;
- Crittografia asimmetrica: una chiave pubblica viene utilizzata per cifrare il messaggio; una diversa chiave privata può decifrare il messaggio.

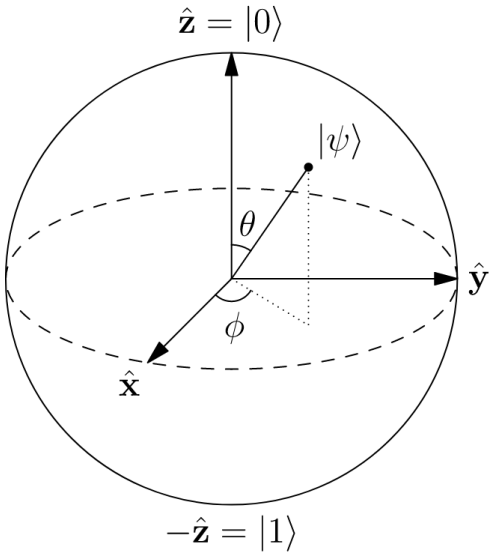




Necessità di una crittografia quantistica

- Lo standard attuale è la crittografia RSA basata su chiavi asimmetriche. Eve potrebbe ottenere la chiave privata a partire da quella pubblica se potesse calcolare la fattorizzazione in numeri primi della chiave pubblica;
- Questo è un compito molto difficile per i computer classici, ma non per i computer quantistici;
- Serve quindi un metodo che sia resistente anche ad attacchi di computer quantistici → QKD.

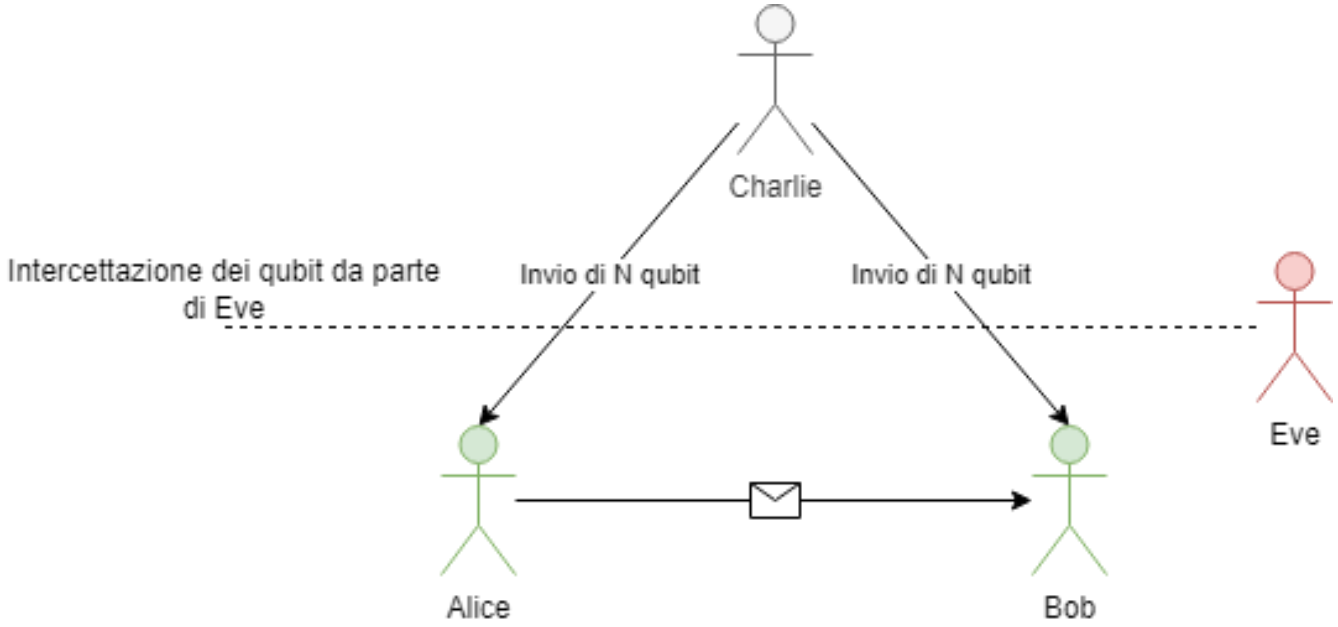
Qubit e gate



$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$$

- Il qubit (quantum bit) è l'unità d'informazione base dei computer quantistici;
- Mentre un bit classico può valere 0 o 1, un qubit è un sistema quantistico a due stati che può valere |0>, |1>, o una combinazione lineare dei due stati;
- I gate quantistici sono l'analogo dei gate classici (AND, OR, NOT, ecc.), possono modificare lo stato di un qubit e sono rappresentati da matrici unitarie.

Protocollo E91 (1)



- Un ente terzo, Charlie, invia N coppie di qubit ad Alice e Bob;
- Lo stato iniziale dei qubit è $|\psi\rangle = (|01\rangle - |10\rangle) / \sqrt{2}$;
- Alice e Bob misurano ogni qubit su una base scelta casualmente tra 3 opzioni;
- $A_1 = X; \quad A_2 = (Z + X)/\sqrt{2}; \quad A_3 = Z;$
- $B_1 = (Z + X)/\sqrt{2}; \quad B_2 = Z; \quad B_3 = (Z - X)/\sqrt{2};$

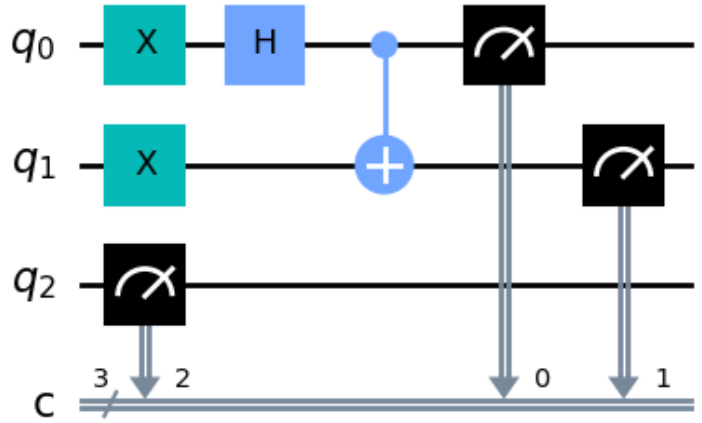
Protocollo E91 (2)

Disuguaglianza CHSH:

$|S| \leq 2$

$S = \langle A_1 B_1 \rangle - \langle A_1 B_3 \rangle + \langle A_3 B_1 \rangle + \langle A_3 B_3 \rangle$

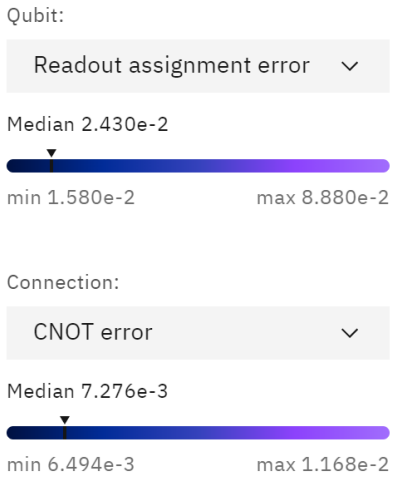
- Senza l'intervento di Eve, la disuguaglianza viene violata e si arriva al limite di Tsirelson $|S| = 2\sqrt{2}$.
- Se Eve interviene in qualche modo, la disuguaglianza è valida e $|S| \leq 2$;
- Per le combinazioni $A_2 B_1$ e $A_3 B_2$ la base è la stessa e i qubit vengono utilizzati come chiave;

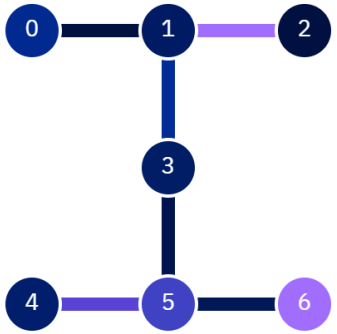


Implementazione con IBM Quantum

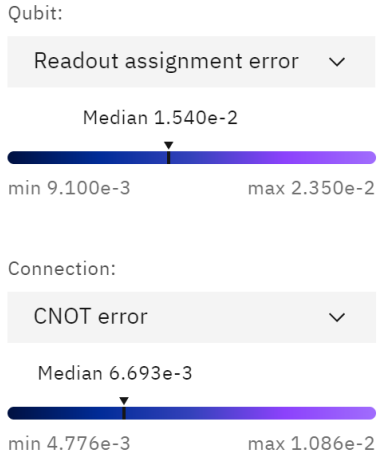
- Il protocollo è stato implementato utilizzando Qiskit, un pacchetto di librerie Python open-source;
- I circuiti quantistici creati con Qiskit possono essere eseguiti su un simulatore o su computer reali online di IBM;
- Il programma che simula il protocollo è stato eseguito sul simulatore e poi su due computer reali. Sono stati scelti i computer ibm_lagos e ibmq_jakarta per le loro differenze di prestazioni.

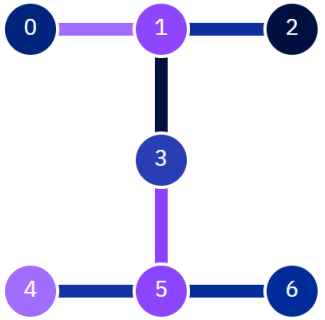
ibmq_jakarta



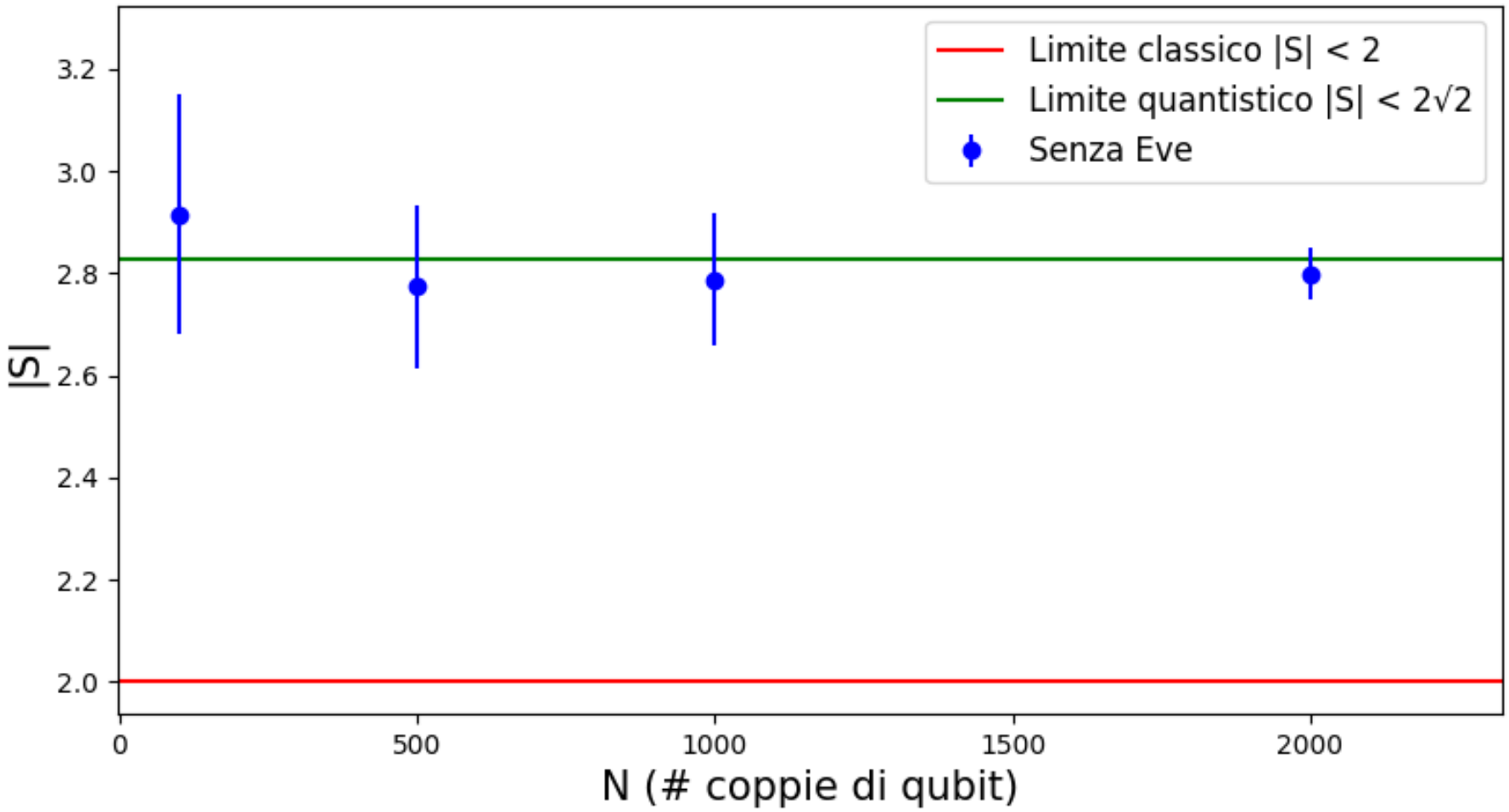


ibm_lagos





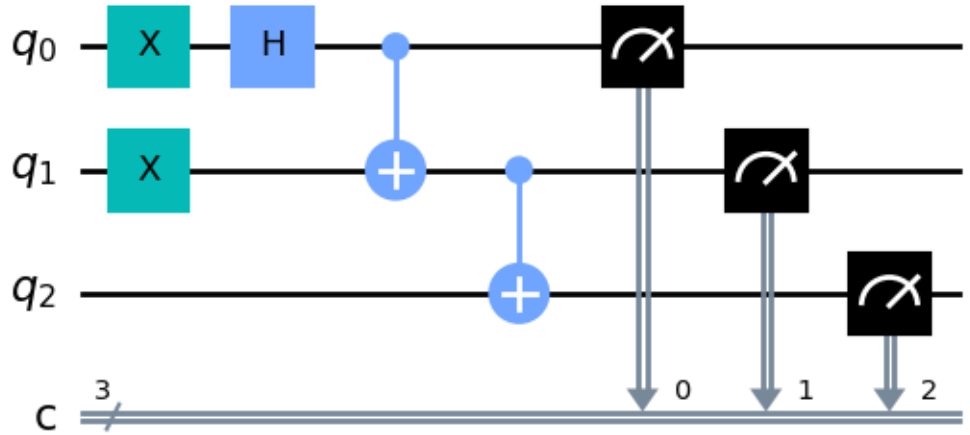
Risultati sul simulatore senza Eve



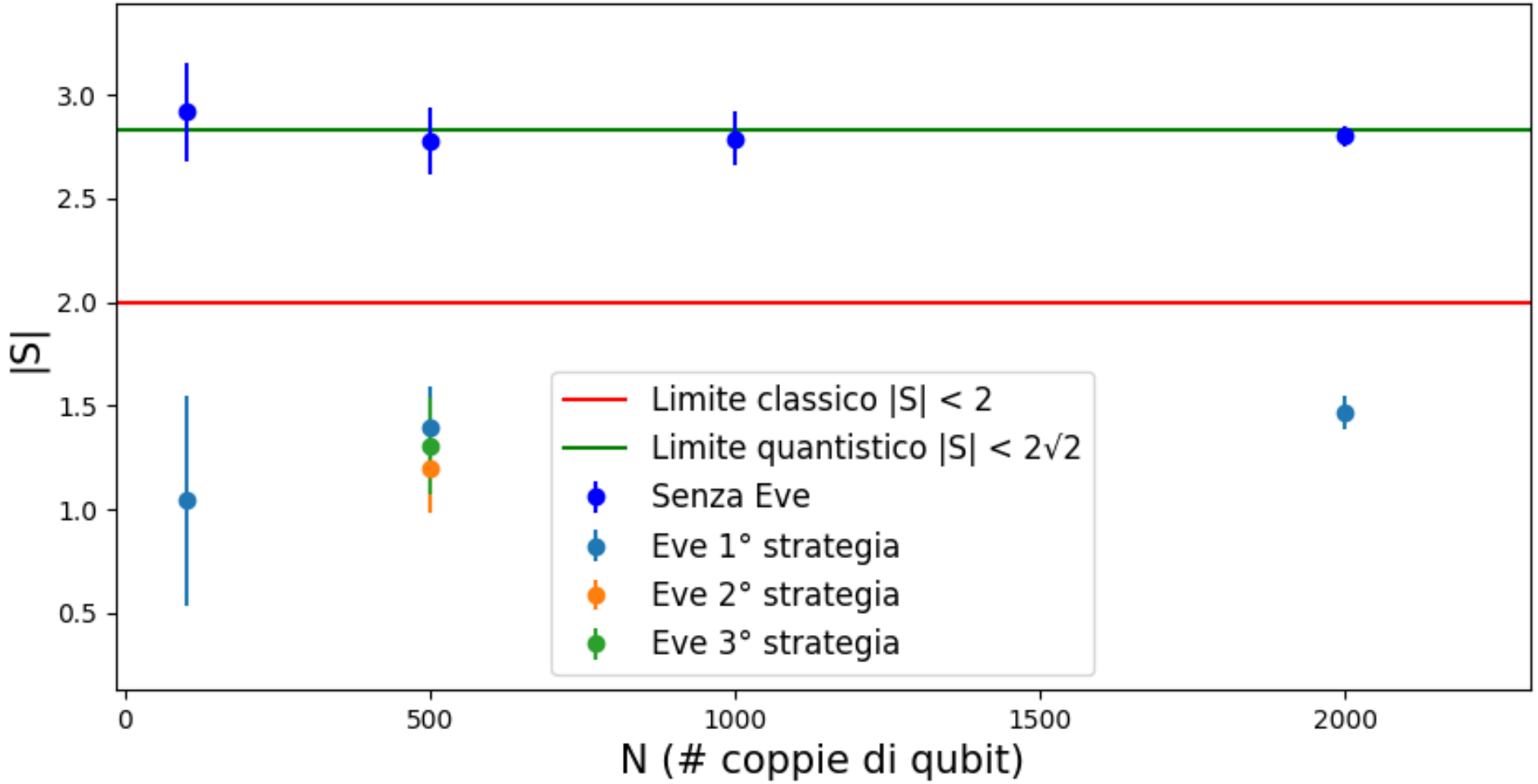
Senza l'intervento di Eve, il valore medio di |S| è sempre compatibile con $2\sqrt{2}$

Strategie di Eve

- Eve può intervenire durante lo scambio dei qubit. Sono state testate 3 strategie:
  - 1) Eve misura tutti i qubit di Bob;
  - 2) Eve applica dei gate scelti tra quelli che può applicare Bob, ai qubit di Bob;
  - 3) Eve utilizza un suo qubit e lo mette in entanglement con il qubit di Bob per ottenere uno stato: $|\psi\rangle = \frac{|011\rangle - |100\rangle}{\sqrt{2}}$
- In ogni caso, l'intervento di Eve porta il valore di |S| sotto al limite classico di 2;
- Eve non potrà mai ottenere l'intera chiave in nessun caso, siccome non può indovinare il 100% delle volte la base scelta da Alice e Bob;

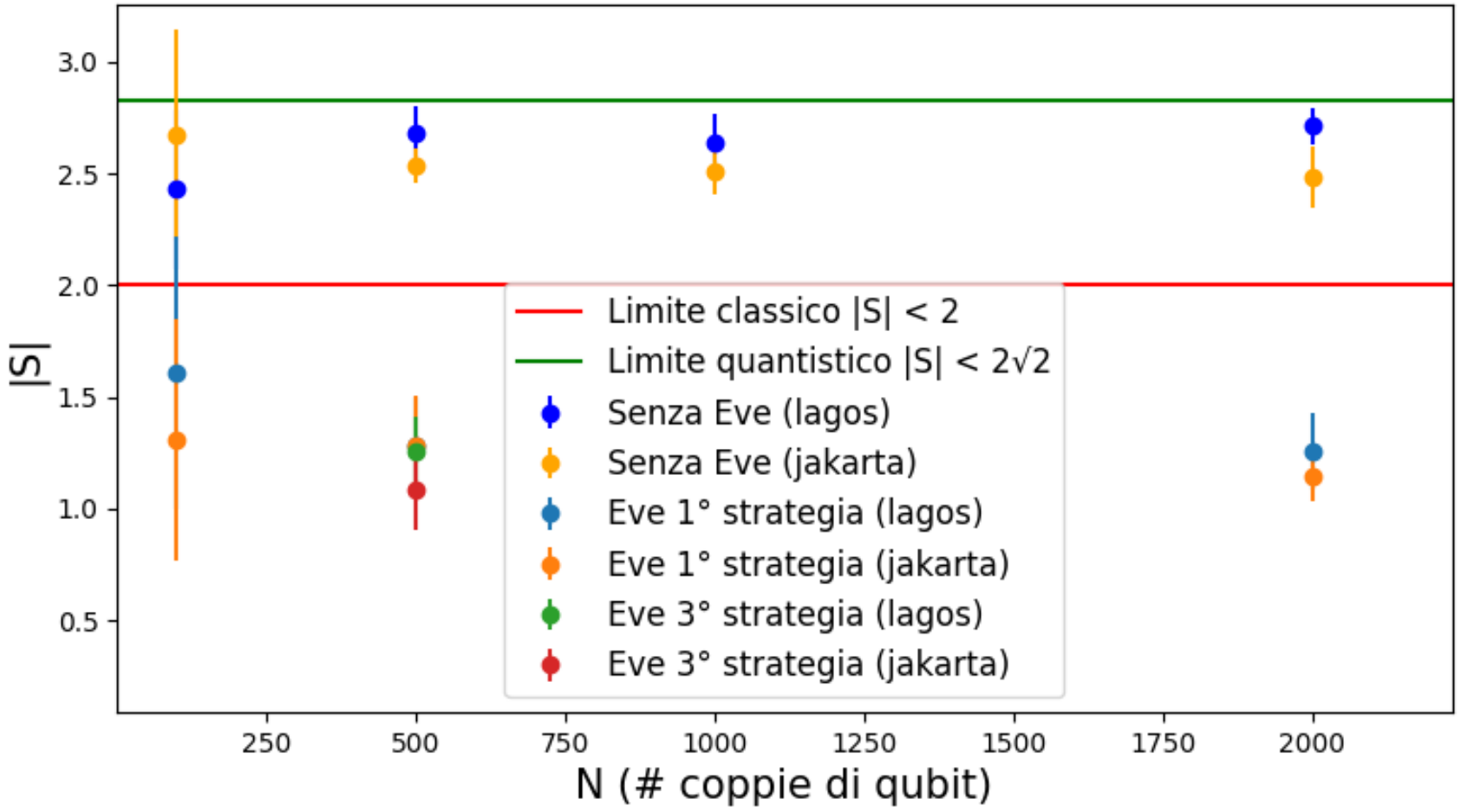


Risultati sul simulatore con Eve



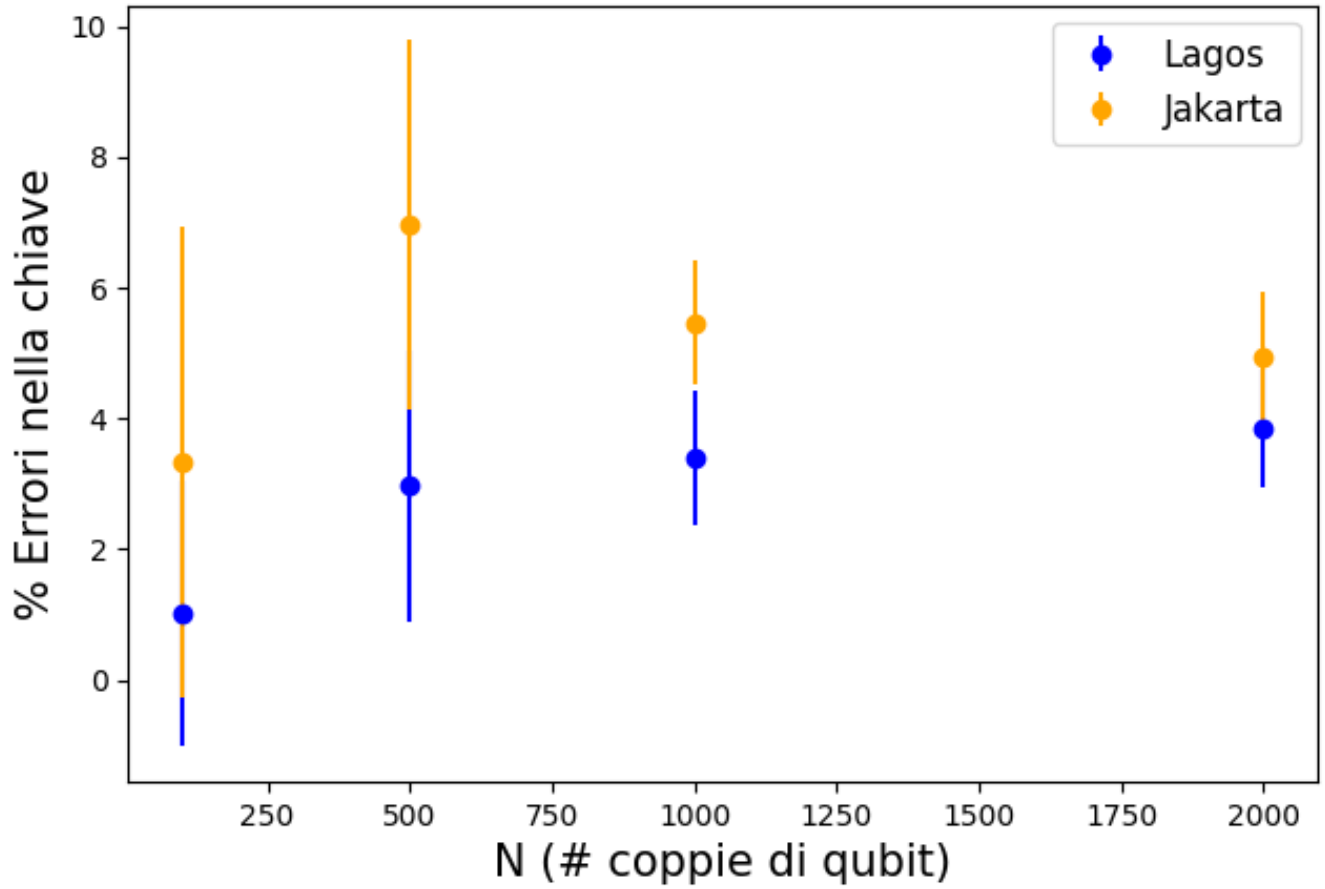
Con l'intervento di Eve, il valore medio di |S| torna a essere inferiore di 2

Risultati sui computer reali – Calcolo di S



Con N = 100 non è possibile distinguere con certezza la presenza di Eve dalla sua assenza.
Con N ≥ 500 i valori di |S| permettono di distinguere sempre i due casi, su entrambi i computer.

Risultati sui computer reali – Errore nelle chiavi



Sui computer reali esiste una probabilità di ottenere un risultato errato dalla misura di un qubit. Così, la chiave condivisa tra Alice e Bob presenterà sempre una certa percentuale di bit incongruenti.

Conclusioni

- Il problema principale è la precisione nella misura dei qubit;
- Possedendo una chiave diversa, Bob non potrà ottenere il messaggio originale di Alice quando lo decifrerà;
- Esistono tecniche di correzione degli errori, ma queste occupano altre risorse (qubit e gate) che non erano disponibili sui due computer utilizzati;
- È necessaria inoltre una ”rete quantistica” che permetta lo scambio di qubit;
- Superati questi due ostacoli, si possono implementare protocolli di QKD come l’E91 che permettono una trasmissione di dati completamente sicura.

Grazie dell’attenzione