Communication over Continuous Quantum Secure Dialogue using Einstein-Podolsky-Rosen States

Shaokai Lin[1,*], Zichuan Wang[1,*], and Lior Horesh[2]
[1]Department of Computer Science, Columbia University, New York, NY, 10027, USA
[2]Mathematics of AI, IBM T J Watson Research Center, Yorktown Heights, NY, 10598, USA
[*]These authors contributed equally to this work.

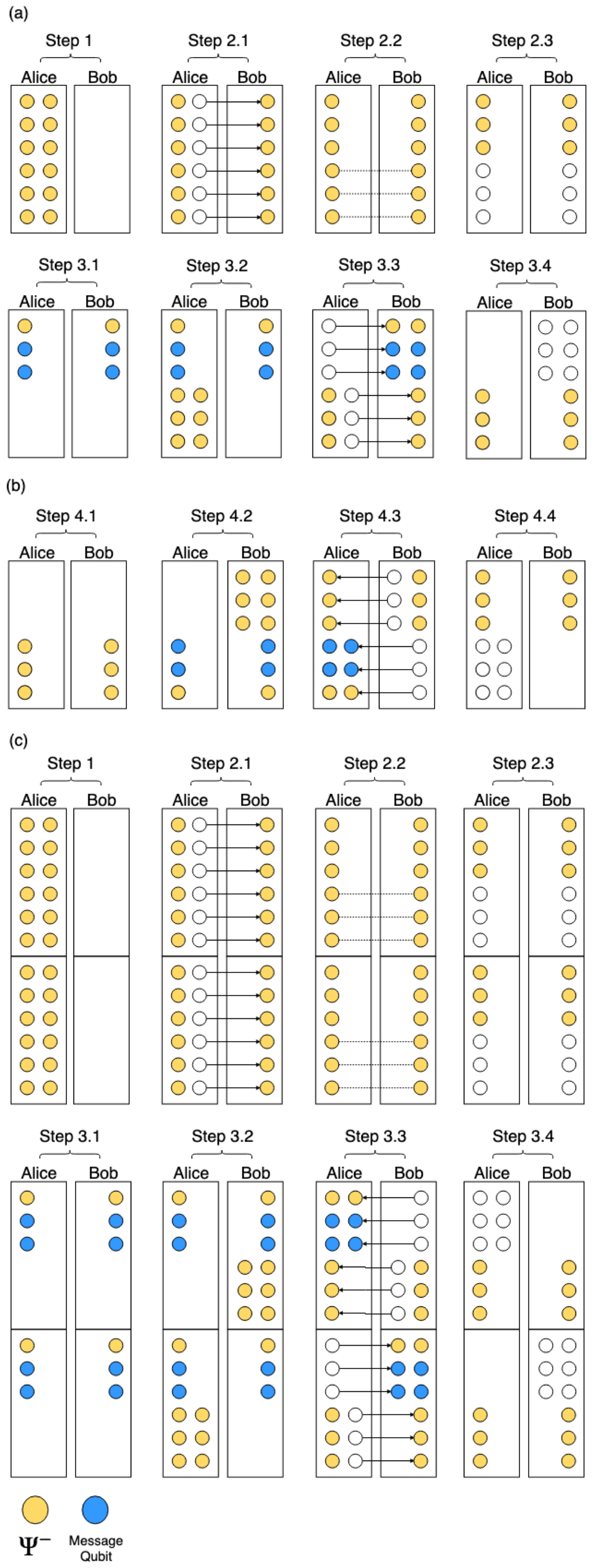
Background and Motivations

- Quantum computing makes traditionally secure encryption algorithms breakable [1]
- Many quantum-based communication protocols have been proposed
- One type of protocol (Quantum Secure Direct Dialogue, QSDD) focuses on bidirectional transmission of encrypted messages through the quantum channel [2]
- The efficiency of pre-existing communication protocols are undesirable

Contributions

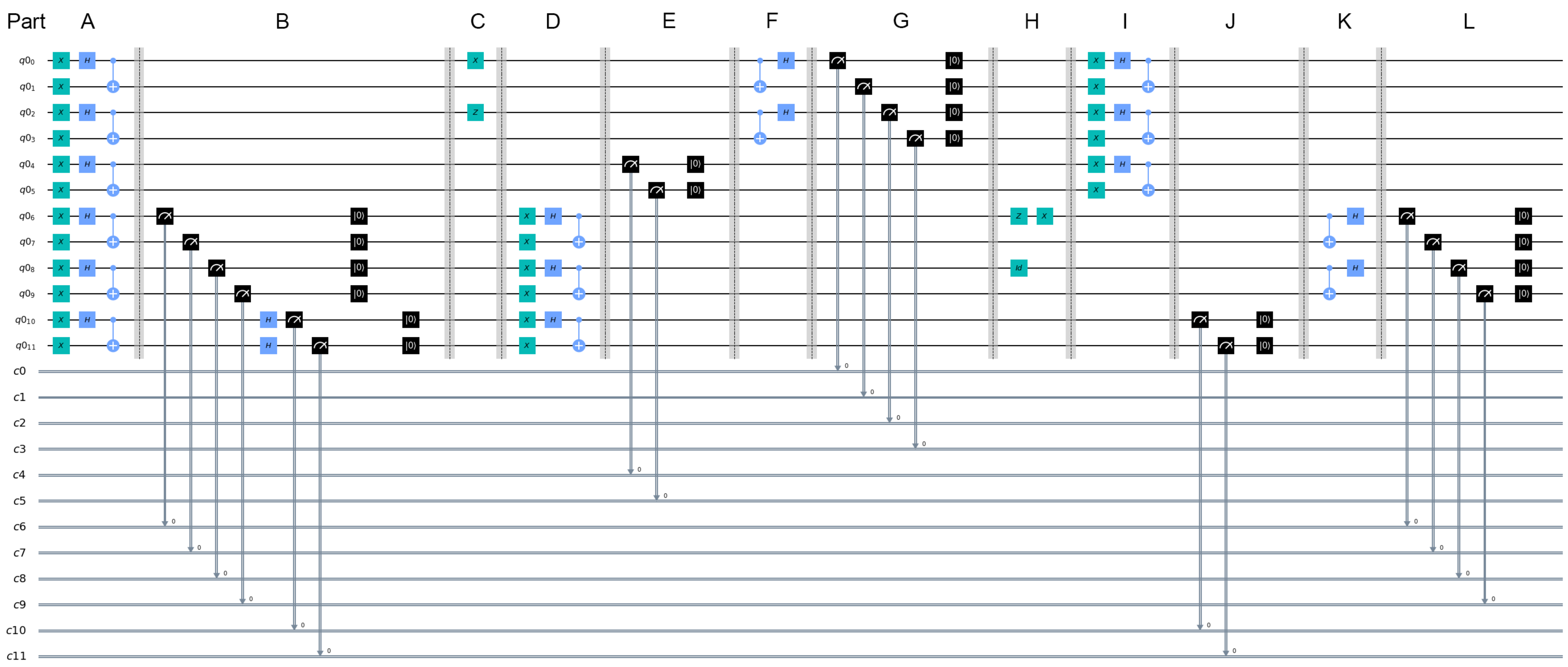
- Propose a novel quantum communication protocol that focuses on efficiency by enabling continuous dialogues while ensuring security
- Allow either party to speak during a conversation without being limited to a particular order
- Implement the protocol using the Qiskit framework and perform simulation of CQSD

CQSD Protocol



(a) Alice initiates the communication channel and sends information to Bob. (b) Bob sends information back to Alice. (c) Alice and Bob transmit information to each other simultaneously.

Protocol Simulation



Implementation

- CQSD protocol implemented in Qiskit using a 12-qubit circuit
- Alice and Bob each has a 6-qubit quantum computer
- The simulation is broken down into three sections:
  1. The initial eavesdropper check
  2. Alice speaks to Bob
  3. Bob speaks to Alice
- Assumes transmissions of qubits between users are seamless and perfect.

part A corresponds to step 1
part B corresponds to step 2.1 to 2.3
part C corresponds to step 3.1
part D corresponds to step 3.2
part E, F and G correspond to step 3.3 and 3.4
part H corresponds to step 4.1 and 4.2
part J, K and L correspond to step 4.3 and 4.4.

Results

- Many benefits of CQSD are observed in the simulation, such as continuous information exchange
- The eavesdropper checks at the beginning and during each transmission can effectively detect the presence of an eavesdropper and halt the transmission, preventing any leakage of information

Security Analysis

- Safe from the "intercept-and-resend" attack thanks to the initial eavesdropper check and the per-transmission eavesdropper check
- Can be made safe from the Trojan horse attack using the same techniques that protect QSDD from the attack [2]
- Can be made safe from the man-in-the-middle attack through the distribution of pre-shared secrets as shown in prior research [3]

Performance Analysis

- The communication over pre-existing QSDD has to halt after one cycle of information exchange due to the depletion of EPR pairs. In order to continue the exchange, a new handshake between two parties has to be performed to re-establish a secure communication channel
- In CQSD, every message sent not only transmits information, but also reserves capacity of the next message. Therefore, the two parties can exchange information without interruptions until one of the parties actively closes the channel
- Since CQSD eliminates the overhead of redundant initialization, it allows for a "continuous" dialogue

Future Work

- Testing CQSD protocol on real quantum machines
- Improving fault tolerance of the CQSD protocol
- Quantitatively compare CQSD's performance to other protocols

Conclusion

We propose the Continuous Quantum Secure Dialogue (CQSD) protocol, offer an implementation of the protocol, and analyze its security performance against common types of attack. CQSD demonstrates an improvement over existing protocols by offering continuous message flow while guaranteeing the privacy of communication.

Reference

1) Artur Ekert and Richard Jozsa. Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys., 68(3): 733–753, July 1996.
2) Chao Zheng and GuoFei Long. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. Sci. China Phys. Mech. Astron., 57(7):1238–1243, July 2014.
3) Zhan-junZhang. Improvingthesecurityofquantumdirect communication with authentication. Physical Review A, 75(2):026301, February 2007.
4) Long, G. L., and X. S. Liu. "Theoretically Efficient High-Capacity Quantum-Key-Distribution Scheme." *Physical Review A*, vol. 65, no. 3, Feb. 2002, p. 032302. *APS*, doi:10.1103/PhysRevA.65.032302.
5) Pirandola, S., et al. "Advances in Quantum Cryptography." *ArXiv:1906.01645 [Math-Ph, Physics:Physics, Physics:Quant-Ph]*, June 2019. *arXiv.org*, http://arxiv.org/abs/1906.01645.