Quantum Authentication Protocol for Secure Quantum Superdense Coding

Teo Kim
Department of Computer Science
University of North Carolina Greensboro
Greensboro, NC
tgkim@uncg.edu

Jinsuk Baek
Department of Computer Science
Winston-Salem State University
Winston-Salem, NC
baekj@wssu.edu

John T. Yi
Department of Chemistry
Winston-Salem State University
Winston-Salem, NC
yijt@wssu.edu

Abstract— **In quantum information theory, superdense coding allows two network entities to exchange two classical bits via a quantum channel using a single quantum bit (qubit) transmission, provided they have pre-shared an entangled qubit. An attacker intercepting the qubit during transmission cannot extract meaningful data without the other entangled qubit from the pair. However, an attacker can disrupt the communication by introducing its own qubit to the receiver. To enhance the security of superdense coding, we propose an authentication mechanism through a classical communication channel.**

Keywords— quantum computing, superdense coding, quantum authentication, entanglement

I. Introduction

Quantum computing, a revolutionary advancement in the field of information processing, leverages the principles of quantum mechanics to process vast amounts of information simultaneously. Within this realm, superdense coding [1] emerges as a unique protocol allowing the transmission of two classical bits using only a single quantum bit (qubit), providing a notable advantage in terms of communication efficiency. However, the very quantum nature that grants superdense coding its capabilities also exposes it to specific vulnerabilities. As quantum communication channels become more prevalent, ensuring the authenticity and integrity of the transmitted information becomes paramount. This paper delves into the necessity of integrating an authentication protocol within superdense coding to bolster its security and trustworthiness in the quantum communication landscape.

II. Superdense Coding

Superdense coding is a quantum communication protocol that enables the transmission of two classical bits using a single quantum bit (qubit). In essence, superdense coding stands in contrast to teleportation, which uses two classical bits to transmit a single qubit. For this mechanism to function, Sender *S* and Receiver *R* need to share an entangled qubit, commonly termed as a Bell state $|\Phi^+\rangle$ [2].

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_S \otimes |0\rangle_R + |1\rangle_S \otimes |1\rangle_R) = \frac{1}{\sqrt{2}}(|0_S 0_R\rangle + |1_S 1_R\rangle)$$

Sender *S* applies a corresponding quantum gate to only its own qubit, depending on the two classical bits which need to be transmitted to Receiver *R*. For the binary pairs "00", "01", "10, and "11", Sender *S* respectively applies the I, X, Z, and ZX gate to its qubit. Notably, the qubit of Receiver *R* remains unaffected since Sender *S* only adjusts its own qubit. After transmitting the qubit to Receiver *R* via the quantum channel, Receiver *R* can distinguish among four potential final states. Thereafter, Receiver *R* applies a CNOT gate to both qubits, using Sender *S*'s qubit as the control bit. This is followed by an H gate applied to Sender *S*'s qubit.

As an illustration, if Sender *S* wishes to transmit the classical bits "01", an X gate is applied to their qubit before sending it to Receiver *R*. By applying a CNOT gate on both qubits and an H gate on the first qubit, Receiver *R* will obtain the final state |01>. Upon measurement, this state will unveil the "01" message from Sender *S*. These processes are represented and illustrated with quantum circuits in Fig. 1 and Fig. 2, respectively.

Sender *S* side:

$$X_1 \otimes I_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \frac{1}{\sqrt{2}}(|0_S 0_R\rangle + |1_S 1_R\rangle)$$

$$= \frac{1}{\sqrt{2}}(|1_S 0_R\rangle + |0_S 1_R\rangle) = \frac{1}{\sqrt{2}}(|0_S 1_R\rangle + |1_S 0_R\rangle)$$

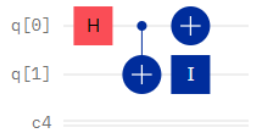

Fig. 1. Quantum circuit for sender *S* side

Receiver *R* side:

$$\text{CNOT}\ \frac{1}{\sqrt{2}}(|0_S 1_R\rangle + |1_S 0_R\rangle) = \frac{1}{\sqrt{2}}(|0_S 1_R\rangle + |1_S 1_R\rangle)$$

$$H_1\ \frac{1}{\sqrt{2}}(|0_S 1_R\rangle + |1_S 1_R\rangle)$$

$$= \frac{1}{\sqrt{2}}[(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1_R\rangle + (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1_R\rangle)$$

$$= \frac{1}{2}[|01\rangle + |11\rangle + |01\rangle - |11\rangle) = |01\rangle$$

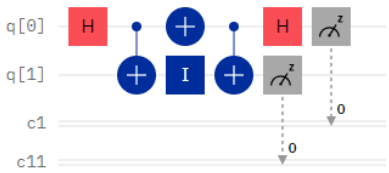

Fig. 2. Quantum circuit for receiver *R* side

SoutheastCon 2024 | 979-8-3503-1710-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/SOUTHEASTCON52093.2024.10500244

III. Authentication Protocol

Quantum authentication protocols, in the past few years, have seen significant advancements, drawing from the inherent properties of quantum mechanics to ensure secure communication. Various methodologies have been proposed, exploiting quantum entanglement [3], quantum states superposition [4], and even quantum error correction codes [5] for authentication. One popular technique involves the use of quantum digital signatures [6], ensuring both message authenticity and integrity. However, many of these protocols exhibit limitations when integrated with specific quantum communication techniques, such as superdense coding. Some might require extended quantum memory, while others might demand intricate operations on multi-qubit systems, making them unfeasible for practical implementations. In this paper, we introduce an authentication mechanism tailored for superdense coding. While superdense coding offers efficient quantum communication, it is still vulnerable to malicious interference. Attackers could alter qubits during transmission, compromising message integrity. To ensure both privacy and authenticity of messages, an authentication mechanism is required in quantum communication protocols.

Initial Setup:

- Shared Secret: Sender *S* and Receiver *R* need to establish a secret key using a Quantum Key Distribution (QKD) method, such as BB84 [7].
- Entanglement Generation: Sender *S* prepares several pairs of entangled qubits, commonly known as Bell pairs. From each pair, one qubit is sent to Receiver *R*, while the other is retained by Sender *S*. These qubits are pivotal for the superdense coding discussed in the previous section.

Protocol Steps:

- Quantum Authentication: Before initiating the superdense coding sequence, Sender *S* generates a quantum authentication tag by combining the shared secret key from the QKD and their intended message. This authentication tag is then relayed to Receiver *R*. Receiver *R* verifies the authenticity of the tag via the shared secret key. A failed authentication results in protocol termination.
- Superdense Coding: Sender *S* proceeds to encode a 2-bit classical message into its half of the pre-shared entangled qubit, which is subsequently transmitted to Receiver *R*.
- Decoding: Upon a successful authentication, Receiver *R* uses its half of the entangled pair to decode the received qubit and obtain the 2-bit message from Sender *S*.

A. Example of Authentication Tag Generation

To illustrate the quantum authentication process more clearly, let us consider a simple example based on the provided 4-bit shared secret key (1010) and the 4-bit authentication message (1101). We first map the 4-bit authentication message to a quantum state. Each bit of the message maps to a corresponding qubit. For 1101, the mapping would be |1> |1> |0> |1>. Secondly, we apply transformations based on the shared key 1010.

- 0 in the key corresponds to the application of the X gate
- 1 in the key corresponds to the application of the Z gate

Using the given mapping:

- Apply the Z gate on the first qubit (1 in the key): Z|1> = – |1>Intermediate state: – |1> |1> |0> |1>
- Apply the X gate on the second qubit (0 in the key): X|1> = |0> Intermediate state: – |1> |0> |0> |1>
- Apply the Z gate on the third qubit (1 in the key): Z|0> = |0> Intermediate state: – |1> |0> |0> |1>
- Apply the X gate on the fourth qubit (0 in the key): X|1> = |0> Intermediate state: – |1> |0> |0> |0>

Thus, the quantum authentication tag is derived from the 4-bit authentication message 1101 and the secret key 1010, is the quantum state – |1> |0> |0> |0>.

B. Example of Authentication Tag Verification

To verify the authenticity using the quantum authentication tag, Receiver *R* needs to reverse the transformations applied by Sender *S*. This is achieved by using the shared secret key.

- Apply the X gate on the fourth qubit (0 in the key): X|0> = |1> Intermediate state: – |1> |0> |0> |1>
- Apply the Z gate on the third qubit (1 in the key): Z|0> = |0> Intermediate state: – |1> |0> |0> |1>
- Apply the X gate on the second qubit (0 in the key): X|0> = |1> Intermediate state: – |1> |1> |0> |1>
- Apply the Z gate on the first qubit (1 in the key): Z(– |1>) = |1> Intermediate state: |1> |1> |0> |1>

From the quantum state |1> |1> |0> |1>, map back to the original 4-bit authentication message, which should be 1101. If the final derived message matches the original authentication message, Receiver *R* can be sure that no third-party interference has taken place during transmission.

IV. Conclusion

We have outlined a protocol, integrating authentication to ensure message integrity and security. Key facets to consider include the vital role of state preservation, and the necessity for efficient security measures. The practical implementation hinges on quantum infrastructure and security evaluations.

Acknowledgment

This work was supported by the Department of Energy (DE-SC0023595) and NSF (NSF-2329017).

References

[1] Nielsen, M. A. and Chuang, I. L, "Application: superdense coding," *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press. p. 97, Dec. 2010.

[2] Sych, D., "A Complete Basis of Generalized Bell States," *New Journal of Physics*. 11 (1): 013006, Jan. 2009.

[3] Penghao, N., et al., "Quantum Authentication Scheme Based on Entanglement Swapping," *Int J Theor Phys* 55, 302–312, Jan. 2016.

[4] Kanmori, Y., et al., "Atuthentication Protocol Using Quantum Superpostition States," *Int J. Net. Security*, 9 (2): 121–128, Jan. 2009.

[5] Dulek, Y., et al., "An Efficient Combination of Quatnum Error Correction and Authentication," *Quantum Physics*, Nov. 2022.

[6] Yin, H-L., et al., Experimental Quantum Secure Network with Digital Signatures and Encryption," *National Sci. Rev.*, 10 (4), Apr. 2023.

[7] Pereira, M. et al., "Modified BB84 Quantum Key Distribution Protocol Robust to Source Imperfections," *Phys. Rev. Res.*, 5. 02065, Apr. 2023.