# Challenges and Future Directions in the Implementation of Quantum Authentication Protocols

Juliet McLeod[1], Ritajit Majumdar[2], and Sanchari Das[1]

[1] University of Denver, Denver CO 80208, USA
[2] Indian Statistical Institute, Kolkata WB 700108, India
julietlmcleod@gmail.com, majumdar.ritajit@gmail.com, and Sanchari.Das@du.edu

**Abstract.** Quantum computing is a powerful concept in the technological world that is critically valued in information security due to its enhanced computation powers. Researchers have developed algorithms that allow quantum computers to hack into information security concepts that were previously considered difficult, if not impossible, including asymmetric key cryptography and elliptic curve cryptography. Studies have been done to focus on improving security protocols through quantum computing to counter these vulnerabilities. One such focus is on the topic of quantum authentication (QA). However, while several QA protocols have been theorized, only a few have been implemented and further tested. Among the protocols, we selected and implemented five quantum authentication protocols to determine their feasibility in a real-world setting. In this late-breaking work, we discuss the difficulties and obstacles developers might face while implementing authentication protocols that use quantum computing.

**Keywords:** Quantum Computing · Authentication · User Studies · Quantum Authentication

## 1 Introduction

Authentication plays a critical role to protect user data and online user presence. Several researchers are focusing on improving these authentication technologies while adding advance computing strategies, one of which is *Quantum Computing* [20]. As we move into the realm of quantum computing, we must consider authentication in a quantum sphere as well. Researchers have postulated protocols to implement quantum authentication, with varying degrees of difficulty both in execution and in implementation [2]. However, there are no analyses of the difficulties in the actual implementation of these protocols from the developer perspective due to limited hardware capabilities. Additionally, there has been no reporting of any user studies to test the adaptability of these protocols from the user perspective in a real-world environment [16].

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14

In this late-breaking work, we report on our implementation of five quantum authentication protocols. This work contributes by detailing the technical difficulties in implementing and applying quantum authentication protocols with currently available infrastructure. We identified four primary obstacles in programming quantum authentication protocols. First, quantum computing is currently implemented for interaction only on a local computer. Second, there are no publicly available quantum communication channels. Third, quantum key distribution is difficult to realize or simulate. Fourth, classical computers are unable to read or store a quantum state. We plan to extend this study by presenting these protocols to users and determining how well users can understand and use these quantum authentication protocols.

## 2 Related Work

Due to the lack of noise-free, general-purpose, large-scale quantum computers, most QA protocols are proposed theoretically. However, a general lack in user-studies has been evident from the literature review done by Majumdar and Das [16]. Most of the general users of such quantum technology are not aware of quantum mechanics, and quantum computing and the technological feasibility is often questionable. For example, McCaskey et al. discusses how users are often not familiar with the technological implementation, codes, or device implemented in quantum computation [17]. One can argue that a fully working quantum computer is most likely decades away. However, we want to point out that working Quantum Random Number Generators (QNRG) [10] are already available, and many laboratories are trying to implement the Quantum Cryptography protocols [3].

## 3 Method

We began by identifying QA protocols for the implementation purposes. Here, we kept protocols that included QKD along with QA or protocols that verified user identity through a trusted third-party. While conducting this search, we identified 17 protocols that fit our criteria. These protocols included Barnum et al. [2], Curty & Santos [4], Dan et al. [5], Das et al. [6], Hong et al. [11], Hwang et al. [12], Kiktenko et al. [13], Lee et al. [14], Ljunggren et al. [15], Shi et al. [20], Wang et al. [21], Zawadzki [22], Zhang et al. [19], Zhang et al. [23], Zhao et al. [24], Zhu et al. [25], and Zuning & Sheng [26].

After the initial search, we considered the pre-shared key requirements of these protocols, which varied among the set of quantum entangled-state pairs, classical keys, classical sets of bits, and knowledge and registration with a trusted third-party. Thereafter, we focused on the number of transmissions between the two or three parties, since larger numbers of transmissions are more resource-intensive and more prone to errors. We also analyzed the type of quantum channel involved, which varied between maximally or non-maximally entangled-state

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14

pairs, squeezed state pairs, and GHZ states. Given the nature of communication through these channels, we evaluated whether the protocol involved more than two participants. Finally, we considered whether the protocol required any additional technical implementation, such as quantum encryption or a pseudo-random number generator.

Based on our filtering mechanism, we implemented five protocols. First, Shi et al. requires a pre-shared entangled-state key pair. It communicates solely over a quantum channel but requires multiple transmissions [20]. Second, Zawadzki uses a pre-shared entangled-state pair and a pre-shared classical key. It completes few transmissions over an unprotected classical channel [22]. Third, Dan et al. utilizes a pre-shared entangled-state pair and pre-shared classical user IDs. It uses a quantum channel and has many transmissions [5]. Fourth, Hong et al. requires a pre-shared classical key, but only needs single-photon messages for authentication. It uses a quantum channel and has multiple transmissions [11]. Finally, Das et al. uses pre-shared classical user IDs. It uses both a protected quantum and an unprotected classical channel. The quantum channel has few transmissions, but the classical channel has multiple [6]. We implemented the five above-mentioned quantum authentication protocols in Python. We used a popular Python quantum computing package called Qiskit to simulate quantum computing on a classical computer [1]. The characteristics of each of these protocols are summarized in Table 1.

| | Shi et al. | Zawadzki | Dan et al. | Hong et al. | Das et al. |
|---|---|---|---|---|---|
| Entangled-State Pair | X | X | X | | |
| Classical Key | | X | X | X | X |
| Quantum Channel | X | | X | X | X |
| Classical Channel | | X | | | X |

**Table 1.** Keys and channels used by each quantum authentication protocol.

## 4 Results: Challenges in Implementation

### 4.1 Challenges with the Implementation of Quantum Authentication Protocols

First, Qiskit is good at simulating local quantum devices. This is sufficient for quantum computations, but causes difficulty when attempting to execute quantum teleportation. In quantum teleportation, two subjects, Alice and Bob, are assumed to share one qubit each of the entangled pair while being separated spatially. It is not possible to simulate this spatial separation in Qiskit. The entire quantum circuit needs to be developed on a local quantum device, which somewhat defeats the purpose of teleportation.

Second, there are currently no publicly-available quantum channels. It is hard to conceptualize sending a qubit to another entity; it is even harder to implement. Qiskit addresses this problem by avoiding it, as there is no way to save a qubit

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14

directly since quantum memory (QRAM) is not available yet. A workaround that Qiskit provides is storing the statevector snapshot. Nevertheless, in reality it is not possible to obtain the statevector from a quantum circuit. This becomes a problem when combined with Qiskit's suggested means of teleportation, since both the entangled pair and the teleported qubit reside on the same quantum device. This limitation of Qiskit largely diminishes the protocols' integrity and security since now the relevant parties and the eavesdropper are on the same system. Therefore, while this allows simulation of the protocol, it is far from the ideal scenario.

Third, pre-shared key distribution is a problem. All of the QA protocols we identified require the two participants to possess a shared quantum pair, usually entangled. However, there are limitations in place that hinder this assumption from happening. There are a large number of theoretical quantum key distribution protocols. Many of these protocols currently achieve perfect security, but require a quantum communication channel.

Finally, a classical computer measures a qubit, and obtains a classical value, i.e., the state in which the qubit collapsed. Many QA protocols require distinguishing among the Bell states. Bell states are a set of four orthogonal states that correspond to different rotations of the qubit and represent a simple entangled state. This entanglement is sufficient to guarantee security in a variety of ways, but requires the ability to measure in Bell bases. Qiskit allows measurement in computational bases only, and therefore we needed to add relevant rotations to each qubit to compensate for this limitation.

### 4.2 Impact of Challenges with the Implementation

More than 80% of the protocols we initially surveyed required a pre-shared quantum key, including all five of the protocols we implemented. This is a prerequisite for each protocol. In order to start the protocol, the participants must already have a key shared. Unfortunately, based on current technology, there is no way to generate an entangled quantum key and distribute it to two or more participants. This is a result of a lack of quantum communication channels. It is possible to generate an entangled quantum key on a single computer, but it is currently impossible to transfer one of the qubits in that key to another computer. This inability causes any protocol that requires a prerequisite shared quantum key to function inadequately. The protocols we implemented that require a shared quantum key include Shi et al., Zawadzki, and Dan et al. [20, 22, 5].

Second, the lack of quantum storage creates interesting issues with quantum protocols. The inability to store quantum states requires the programmer to measure them before storing their values. This removes the uncertainty in their values. Measuring the values early creates a unique problem. When a participant measures a qubit, they must choose a basis to measure it in. If they choose the wrong basis, their results could be inaccurate. This concept is important to the security of quantum message channels, since an eavesdropper will not know the correct basis and will obtain inaccurate results with high probability if they try to measure intercepted qubits.

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14

Third, the lack of quantum storage prohibits measuring quantum changes. One common practice in quantum authentication is measuring Bell states. As stated before, measurement in Bell basis is not supported in Qiskit or with current quantum devices. However, knowing which Bell state a qubit is in is important for security. The workaround to this is to incorporate additional rotations prior to measurement. This issue with Bell state measurement occurs in Shi et al., Dan et al., and Hong et al. [20, 5, 11].

## 5 Future Study Design: Vision

In our study design, the participants will first take a pre-screening survey to determine their technical ability regarding computers, authentication, and quantum topics. These technical questions are taken from the SEBIS questionnaire by Egelman et al. [9, 8] and the expert evaluation survey by Rajivan et al. [18]. We will select eligible participants to include a diverse set of technical experience, as technical expertise could be a critical factor in evaluating the effectiveness of the feasibility of QA for an in-lab study. Participants will use think-aloud while they execute the selected simulation of the protocols motivated by the study design of Das et al. [7]. We also plan to implement the QA for regular accounts which our users can implement in their daily life after the first phase of this experiment, then conduct a timeline analysis to see how the participants' continued usage is impacted. There are technical infeasibility issues for this extension which this study emphasizes but we plan to overcome those through this research and by starting with simulated accounts for the initial phase of the study. Along these lines, recent Quantum Networks [3] can be utilized instead of Qiskit to emulate real-world quantum communication.

## 6 Conclusion

Quantum computing and quantum authentication are becoming critical in the information security domain due to their computational power and secure identification capabilities. However, less is known about the implementation of the QA protocols, particularly from the feasibility perspective. In this paper, to explore and learn further on this, we report on our investigation of the challenges of implementing user authentication protocols that utilize quantum computing. First, we implemented five QA protocols in Python using the Qiskit library. While programming these protocols, we identified significant difficulties in implementing these or similar QA protocols. These difficulties include a lack of quantum teleportation channels, issues with pre-shared key distribution, and a lack of quantum storage. Additionally, we discuss why these difficulties exist and why they are problematic for accurately testing quantum authentication protocols. After the implementation, in this late-breaking work, we also report on our future direction plan to continue this research by conducting user studies through a think-aloud protocol to test the efficacy of the five protocols.

[3] https://www.quantum-network.com/

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14

## 7 Acknowledgement

We would like to acknowledge the Inclusive Security and Privacy-focused Innovative Research in Information Technology: InSPIRIT Research Lab at the University of Denver. We would also like to thank Nayana Das for their feedback on the Quantum Authentication protocols. Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the authors and do not necessarily reflect the views of the University of Denver or the Indian Statistical Institute.

## References

1. ANIS, M.S., Abraham, H., AduOffei, et al.: Qiskit: An open-source framework for quantum computing (2021). https://doi.org/10.5281/zenodo.2573505
2. Barnum, H., Crepeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. 43rd Annual IEEE Symposium on the Foundations of Computer Science pp. 449–458 (2002). https://doi.org/https://doi.org/10.1109/SFCS.2002.1181969
3. Bourennane, M., Gibson, F., Karlsson, A., Hening, A., Jonsson, P., Tsegaye, T., Ljunggren, D., Sundberg, E.: Experiments on long wavelength (1550nm)"plug and play" quantum cryptography systems. Optics Express **4**(10), 383–387 (1999)
4. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Physical Review A **64**, 062309 (2001). https://doi.org/https://doi.org/10.1103/PhysRevA.64.062309
5. Dan, L., Chang-Xing, P., Dong-Xiao, Q., Nan, Z.: A new quantum secure direct communication scheme with authentication. Chinese Physics Letters **27**(5) (2010). https://doi.org/https://doi.org/10.1088/0256-307X/27/5/050306
6. Das, N., Paul, G., Majumdar, R.: Quantum secure direct communication with mutual authentication using a single basis. International Journal of Theoretical Physics. (arXiv preprint arXiv:2101.03577) (2021). https://doi.org/https://doi.org/10.1007/s10773-021-04952-4
7. Das, S., Dingman, A., Camp, L.J.: Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In: International Conference on Financial Cryptography and Data Security. pp. 160–179. Springer (2018)
8. Egelman, S., Harbach, M., Peer, E.: Behavior ever follows intention? a validation of the security behavior intentions scale (sebis). In: Proceedings of the 2016 CHI conference on human factors in computing systems. pp. 5257–5261 (2016)
9. Egelman, S., Peer, E.: Scaling the security wall: Developing a security behavior intentions scale (sebis). In: Proceedings of the 33rd annual ACM conference on human factors in computing systems. pp. 2873–2882 (2015)
10. Herrero-Collantes, M., Garcia-Escartin, J.C.: Quantum random number generators. Reviews of Modern Physics **89**(1), 015004 (2017)
11. ho Hong, C., Heo, J., Jang, J.G., Kwon, D.: Quantum identity authentication with single photon. Quantum Information Processing **16**(236) (2017). https://doi.org/https://doi.org/10.1007/s11128-017-1681-0
12. Hwang, T., Luo, Y.P., Yang, C.W., Lin, T.H.: Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants. Quantum Information Processing **13**(925-933) (2014). https://doi.org/https://doi.org/10.1007/s11128-013-0702-x

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14

13. Kintenko, E., Malyshev, A., Gavreev, M., Bozhedarov, A., Pozhar, N., Anufriev, M., Federov, A.: Lightweight authentication for quantum key distribution. IEEE Transactions on Information Theory **66**(10), 6354–6368 (2020). https://doi.org/https://doi.org/10.1109/TIT.2020.2989459
14. Lee, H., Lim, J., Yang, H.: Quantum direct communication with authentication. Physical Review A **73**(4), 042305 (2006). https://doi.org/https://doi.org/10.1103/PhysRevA.73.042305
15. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Physical Review A **62**(2), 022305 (2000). https://doi.org/https://doi.org/10.1103/PhysRevA.62.022305
16. Majumdar, R., Das, S.: Sok: An evaluation of quantum authentication through systematic literature review. In: Proceedings of the Workshop on Usable Security and Privacy (USEC) (2021)
17. McCaskey, A., Dumitrescu, E., Liakh, D., Humble, T.: Hybrid programming for near-term quantum computing systems. In: 2018 IEEE International Conference on Rebooting Computing (ICRC). pp. 1–12. IEEE (2018)
18. Rajivan, P., Moriano, P., Kelley, T., Camp, L.J.: Factors in an end user security expertise instrument. Information & Computer Security (2017)
19. Sheng, Z., Jian, W., Chao-Jing, T., Quan, Z.: A composed protocol of quantum identity authentication plus quantum key distribution based on squeezed states. Communications in Theoretical Physics **56**(2), 268–272 (2011). https://doi.org/https://doi.org/10.1088/0253-6102/56/2/13
20. Shi, B.S., Li, J., Liu, J.M., Fan, X.F., Guo, G.C.: Quantum key distribution and quantum authentication based on entangled state. Physics Letters A **281**(2-3), 83–87 (2001). https://doi.org/https://doi.org/10.1016/S0375-9601(01)00129-3
21. Wang, J., Zhang, Q., jing Tang, C.: Multiparty simultaneous quantum identity authentication based on entanglement swapping. Chinese Physics Letters **23**(9), 2360–2363 (2006). https://doi.org/https://doi.org/10.1088/0256-307X/23/9/004
22. Zawadzki, P.: Quantum identity authentication without entanglement. Quantum Information Processing **18**(7) (2018). https://doi.org/https://doi.org/10.1007/s11128-018-2124-2
23. Zhang, S., Chen, Z.K., Shi, R.H., Liang, F.Y.: A novel quantum identity authentication based on bell states. International Journal of Theoretical Physics **59**(236-249) (2019). https://doi.org/https://doi.org/10.1007/s10773-019-04319-w
24. Zhao, B., Liu, B., Wu, C., Yu, W., Su, J., You, I., Palmieri, F.: A novel ntt-based authentication scheme for 10-ghz quantum key distribution systems. IEEE Transactions on Industrial Electronics **63**(8), 5101–5108 (2016). https://doi.org/https://doi.org/10.1109/TIE.2016.2552152
25. Zhu, H., Wang, L., Zhang, Y.: An efficient quantum identity authentication key agreement protocol without entanglement. Quantum Information Processing **19**(381) (2020). https://doi.org/https://doi.org/10.1007/s11128-020-02887-z
26. Zuning, C., Zheng, Q.: A "ping-pong" protocol with authentication. 5th IEEE Conference on Industrial Electronics and Applications pp. 1805–1810 (2010). https://doi.org/https://doi.org/10.1109/ICIEA.2010.5515357

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_14