Position-Based Quantum Cryptography for Multi-located Prover and Single Verifier

Sarah Noles[1] and Abhishek Parakh[2]
University of Nebraska, Omaha
[1]snoles@unomaha.edu, [2]aparakh@unomaha.edu

***Abstract*— This research proposes a new Position-Based Quantum Cryptography (PBQC) protocol using a single verifier and a single prover located in multiple physical locations rather than the traditional PBQC model (single prover and multiple verifiers). The protocol operates in two phases, identity verification and location verification, and relies on encryption to eliminate vulnerabilities to common PBQC attacks.**

I. INTRODUCTION

Traditionally, cryptographic systems require authentication using a set of credentials (something you know, have, or are). However, in certain forms of secure communication it is also necessary to authenticate the location of a party, *somewhere you are*. This mode of authentication is known as Position-Based Cryptography. Position-based cryptography has been examined in the classical context and shown to be insecure against colluding adversaries due to the adversary's ability to "run exactly the same copy of the Prover" allowing them to impersonate the prover [1]. However, the concept has shown promise in the quantum space due to the no-cloning theorem's capability to prevent an attacker from running an exact copy of the prover without the prover detecting the attacker's presence. Several Position Based Quantum Cryptographic (PBQC) protocols have been proposed. Each assumes a single prover, P, and multiple verifiers, $V_1, V_2, ..., V_n$ [2]–[6]. In general, each of these protocols involves sending information to the prover from multiple verifiers and correlating the time at which each verifier receives information back to verify the location of the prover. In this research we flip the scenario and propose a new protocol involving a single verifier and a single prover located in multiple physical locations (e.g. a cloud infrastructure located in multiple data centers). This protocol is potentially more practical to implement as it requires fewer resources for the verifier (end user) and relies on the existing resources shared between the prover's (cloud service provider's) locations. In addition, this protocol uses identity verification and encryption to eliminate vulnerabilities to common PBQC attacks.

II. PROTOCOL

The proposed protocol occurs in two parts: identity verification and location verification. The identity verification phase focuses on establishing identities between the verifier and each prover location using a zero-knowledge proof. The assumption that a zero-knowledge proof can occur is reasonable given the potential applications of this protocol (e.g. cloud services model). For example, the verifier likely already registered with the cloud provider via a username and password. Following this, the two parties are able to exchange encryption keys to be used during the location verification portion of the protocol where the location of each prover is verified. This is done using a triangulation scheme and requires the knowledge of two prover locations at a minimum. The verifier prepares quantum states and unitary operators sending one of each to each prover location. The prover performs the operation on the given state. The prover locations are grouped into pairs where one prover may participate in two pairs if an odd number of provers exists. After performing their operation, the pairs exchange states and perform their operation again on their new state. Then each encrypts the state using their previously established encryption key. Following this, they each return the state to the verifier. The verifier records the time at which the states were received and verifies that the expected state was returned. If both are true, the location is verified.

III. CONCLUSIONS

The proposed protocol is a novel application of position-based quantum cryptography that allows for the verification of a multi-located prover using only a single verifier. The success of the protocol is dependent on the use of a pre-established shared secret (username/password) used to establish identities and encryption keys and on timing verification. If the protocol is unsuccessful, it reveals the presence of an attacker. This model allows for stronger authentication between parties in real-world situations, such as cloud computing.

This work is partly supported by NSF Award #1623380.

REFERENCES

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position Based Cryptography," *Advances in Cryptology - CRYPTO 2009 Lecture Notes in Computer Science*, pp. 391-407, 2009.
[2] R. A. Malaney, "Location-dependent communicatiosn using quantum entanglement," *Physical Review A*, vol. 81, no. 4, 2010.
[3] F. Gao, B. Liu, and Q. Y. Wen, "Quantum position verification in bounded-attack-frequency model," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 59, no. 11, 2016.
[4] D. Unruh, "Quantum Position Verification in the Random Oracle Model," *Advances in Cryptology-CRYPTO 2014 Lecture Notes in Computer Science*, pp. 1-18, 2014.
[5] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, "The Garden-Hose Model," *Proceedings of the 4th conference on Innovations in Theoretical Computer Science - ITCS '13*, 2013.
[6] K. Chakraborty and A. Leverrier, "Practical position-based quantum cryptography," *Physical Review A*, vol. 92, no. 5, 2015.