Quantum Authentication:
Current and Future Research Directions

Heather Crawford
Florida Institute of Technology
hcrawford@fit.edu

Steven Atkin
IBM
atkin@us.ibm.com

Abstract

Quantum computers have been seen as the arbiters of certain doom for classical computer security fundamentals such as cryptography. Much of this fear has been eased by the lack of real rather than theoretical or specialized quantum hardware. Since real quantum hardware is now available to the public and is rapidly maturing, it is essential that we focus on studying whether the doomsayers are correct: that traditional security techniques will be no match against quantum algorithms running on real quantum hardware. This paper examines research being undertaken in quantum identity authentication (QIA) protocols, dispels myths, and proposes directions for future research in this area. As such, our focus is on creating dialogue around quantum authentication in the authentication community to encourage further research and advancement in this field.

1 Introduction

A quantum computer makes use of the underlying principles of quantum mechanics to store and manipulate information held in the quantum states of subatomic particles. Long seen as a theoretical rather than real possibility, quantum computers have been touted as forcing the end of classical security fundamentals such as cryptography, although not all cryptography is susceptible and there are post-quantum public key cryptosystems [1]. This weakness is due to the ability of quantum computers to solve problems significantly faster than classical computers, thanks to the properties of quantum bits, or *qubits*. The reality, thankfully, is a bit different because speed only helps when breaking security protocols that are susceptible to brute-force attacks. Research in quantum computing to date has mainly focused on the fields of quantum cryptography [2], quantum key distribution [10, 13], quantum direct communication [20], and quantum secret sharing [5]. Since these primitives can be used to provide quantum authentication, research in these fields has also enabled research into quantum authentication.

Quantum authentication can be broken into two subtypes: 1) authentication of data or messages, which focuses on verifying that data was sent or is unchanged after being sent; 2) quantum identity authentication (QIA), which is verifying someone's identity as they claim or is supposed about them. This paper focuses on research being performed in the latter: using the non-classicality of quantum states and quantum mechanics to create authentication protocols that are stronger and less susceptible to attack than classical [2] authentication protocols. QIA does not refer to authenticating users who are using a quantum computer; instead, it implies that we can exploit the natural properties of quantum systems (e.g., superposition and entanglement) to authenticate users who are using *classical* computers. The distinction is important: real quantum computers exist, but they are not universally fault tolerant at scale beyond a small number of qubits. Currently, one of the largest production, generally available quantum computer is IBM Q System One (i.e., one that does not lose information, or *decohere*, so quickly as to be useless) is 20 qubits in size. This size of quantum computer, for example, is capable of solving the Traveling Salesman Problem for 5 nodes on the path, but no more. As such, current quantum computers have shown *quantum advantage* in that they can solve *some* problems faster than classical computers, yet it remains incapable of solving problems that are unsolvable by classical computers.

So why is quantum authentication a desired goal? In gen-

[1] For example, see NIST's Post Quantum Cryptography competition at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[2] Note that the term "classical" refers to non-quantum systems, i.e., traditional computing.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

eral, classical authentication protocols use an encrypted tunnel to ensure the privacy and secrecy of the authentication process, particularly if shared symmetric keys are part of the protocol (note: the encrypted tunnel can be replaced with a public key-based key exchange protocol such as the Diffie-Hellman Key Exchange Protocol). In quantum authentication, the fundamental nature of quantum mechanics is leveraged to construct a protocol that enables automatic detection of tampering or eavesdropping. This is possible due to the inability to simultaneously obtain all properties of a qubit through a single measurement. Specifically, once a qubit's state is measured, it collapses and loses its quantum properties. This means that an attacker cannot measure a quantum state in flight, because this will be easily detectable by the recipient. Furthermore, the no-cloning theorem of quantum computing [16] states that an attacker cannot clone or copy a quantum state reliably because of the Heisenberg Uncertainty Principle [3]. Therefore, an attacker cannot measure and subsequently copy a quantum state, thereby providing additional security and privacy assurances.

2 Current Research Directions

Generally, the current research in quantum identity authentication can be split into two major topics: authentication based on either entangled and non-entangled quantum states.

2.1 Entanglement-Based

Quantum entanglement, or what Einstein called "spooky action at a distance", describes the effect that measuring one qubit has on a second qubit. These entangled qubits behave in a way that is individually random, but also strongly correlated to one another [1]. That is, by knowing the state of one entangled qubit (i.e., by measuring its state), you can predict will full certainty the state of the second entangled qubit without measuring it. This property is true irrespective of the distance between the two entangled qubits. In particular, entanglement has been proposed as a basis for identity authentication since two entities can each possess one qubit of an entangled pair, and know with certainty what measurement they should expect given the measurement taken by their counterpart.

Entanglement provides the ability to move information from one party to another through a process called *quantum teleportation*. One party who holds half of an entangled pair (one qubit) can measure it in the Bell basis [3] and discover its value before it was sent. Thus, one party can choose a random Bell state (an entangled pair of qubits), send one of the qubits to another party who can measure the qubit in the Bell basis to discover the original Bell state. Thus, information can be "teleported" or communicated, yet does not violate the no-cloning theorem. It is important to keep in mind that Quantum Teleportation does not enable faster than light communication as it still requires that the parties communicate their Bell measurements over a classical channel. In terms of authentication, if two authenticated parties share entangled qubits, they can also share information through entangled pairs.

There are several known variants of Bell states that have been used for entanglement-based authentication, including Einstein-Podolsky-Rosen (EPR) pairs and Greenberger-Horne-Zeilinger (GHZ) states. EPR pairs are simply realizations of entangled qubits encoded in Bell states - for the purposes of this paper, the terms "Bell state" and "EPR pair" are used synonymously. GHZ states extend Bell states to entangling three qubits instead of two qubits, allowing for more parties to be involved in entanglement-based authenticated communication without creating an entangled state for each pair of parties.

2.1.1 Bell States/EPR Pair Based

Penghao *et al.* [11] describe an authentication protocol based on entanglement that also used quantum teleportation to transmit information after authentication has succeeded. In their protocol, Alice and Bob each authenticate separately to a trusted third party, Trent, by sharing entangled qubits with Trent and performing measurements in the Bell basis to confirm that they are in possession of the correct matches to Trent's entangled qubits (the measurements are transmitted through classical communication channels). Once Trent has authenticated Alice and Bob, they prepare a number m of entangled qubits that serve as message bits. Trent allots one half of each entangled pair to Alice, and the other half to Bob. Alice and Bob then use these entangled pairs to transmit information to one another via quantum teleportation, as described previously. Trent cannot eavesdrop on this information since they no longer have either half of the entangled qubits alloted to Alice and Bob, respectively. Furthermore, since Alice and Bob never authenticate to each other, it is impossible for them to impersonate the other. Penghao *et al.* [11] also show that their protocol is resistant to both interception and replay attacks. One of the issues with this protocol is the trust placed in Trent, the trusted third party, which is the same as classical authentication schemes that depend on third parties.

Similarly, Shi *et al.* [13] propose a Quantum Key Distribution (QKD) protocol that also performs quantum authentication. The procedure used by Shi *et al.* is similar to that proposed by Penghao *et al.* [11] except that no trusted third party is required, nor is a classical communication channel necessary for transmitting the measurements of selected qubits [13]. The authors show that their protocol is secure against eavesdropping and replay attacks, as well as claim that it is more secure than other protocols because it does not require a classical channel, although they do not prove this assertion [13].

[3] The four Bell states are commonly used for entanglement.

2.2 GHZ Pairs-Based

In some situations, authenticating more than two parties is desirable. Doing so with the protocols discussed thus far requires the creation of multiple instances of the protocol until all n parties have authenticated, which is inefficient and time-consuming. A better approach is to allow multi-party authentication with one protocol instance; this can be made possible with GHZ pairs, which entangle three qubits instead of the traditional two qubit Bell pairs.

In [17], Yang *et al.* propose an entanglement-based QIA protocol that makes use of GHZ pairs. The main benefit of this protocol is that it can authenticate t parties out of a set of n possible users rather than authenticating only two parties. The threshold $t \leq n$, is based on Shamir's Secret Sharing [12], a classical method of sharing a secret amongst n parties in which only $t \leq n$ parties must be present for the secret to be known. This means that not all parties need to participate for authentication to take place, a known weakness of other QIA protocols, both entanglement-based [11, 15, 18] and single-photon based [6, 19]. Similarly to other protocols, Yang *et al.*'s [17] depends on a trusted third party that enables the authentication, and to whom all other parties authenticate. Yang *et al.* claim that their protocol is resistant to eavesdropping through the use of decoy particles that are interspersed at known positions with message particles when their measurements are transmitted on the quantum communication link. The decoy particles, which are chosen at random from $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ can detect eavesdropping by ensuring that they appear in the correct locations in the sequence both from the trusted third party and the users' points of view [17]. However, it is unclear from Yang *et al.*'s description of how to check for eavesdroppers whether the decoy particles protect against a passive eavesdropper who does not change the photons as they traverse the quantum communication link.

Kang *et al.* [7] first proposed a QIA protocol based on GHZ-like states that required a trusted third party; each of the three entangled GHZ-like qubits were given to Alice, Bob, and the third party respectively. This protocol used the trusted third party, via their entangled qubit, to control the quantum network and to prepare the GHZ-based qubit sequences used in authenticating Alice and Bob, the two communicating parties. Therefore, it was shown by Gao and Wang [4] that the trusted third party was able to both deduce Alice and Bob's authentication keys via eavesdropping on the quantum network, and also introduce abnormalities to the quantum channel that can allow the third party to eavesdrop on the quantum channel without Alice or Bob's knowledge. This led Kang *et al.* in [8] to subsequently add to their original QIA protocol the use of decoy qubits to detect eavesdropping and entanglement correlation to detect quantum channel abnormalities. Their improved protocol therefore can be considered resistant to trusted third party attacks, thus making it useful for situations in which the third party is by definition untrusted, such as in cloud computing environments. Their new protocol also allows many other entities such as financial institutions and independent parties to act as the third party, which makes their protocol more widely useful.

2.3 Non-Entanglement Based

One of the major issues with authentication based on entangled states is the challenge of controlling the entangled states for long periods of time. This is commonly known as *decoherence*. To be able to produce, manipulate, and create entanglement between qubits inside a quantum computer, especially those based upon superconducting circuits, requires that the superconducting circuits be held at temperatures colder than outer space. IBM Q System One, for example, operates at 15 milliKelvin. As quantum states age, they both decohere and begin to lose their quantum properties. Thus, entangled qubits cannot exist for long outside of these controlled environments. This means that alternatives may be necessary, such as single-photon states that do not rely on entanglement.

In [6], the authors present a quantum identity authentication protocol in which two parties (Alice and Bob) agree upon a two classical-bit sequence that is then related to set quantum states. For example, Alice and Bob could agree on the following mapping, which serves as their secret key: $00 \mapsto |0\rangle, 01 \mapsto |1\rangle, 10 \mapsto |+\rangle, 11 \mapsto |-\rangle$. Authentication takes place when Alice selects a key $A_{ki} \in \{00, 01, 10, 11\}$ and sends to Bob the corresponding quantum state $Q_{ai} \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Bob then measures Q_{ai} in either the Z-basis (by applying the Hadamard gate to Q_{ai}) or the X-basis (by applying the Pauli X gate to Q_{ai}) depending on the value of Q_{ai}. Bob's measurement, which results in a two classical bit sequence, acts as the authentication check, similar to comparing a user-entered hashed password to the relevant entry in a server: if Bob and Alice's classical bit sequences match, then Alice is authenticated. This protocol also allows for checking the state of the communication channel using decoy states [6]. The authors show that their protocol is resistant to impersonation and replay attacks, with only a small probability that an attack will go unnoticed ($< 0.1\%$ in most cases), and a small amount of leaked information per protocol run (about 1 classical bit per run) [6]. However, this protocol depends on an idealized quantum system (i.e., that the photon source is perfect and that the detectors always detect sent photons), which is not plausible in real quantum systems. The authors modify their approach for realistic quantum systems, but with an additional requirement of quantum error correction [6]. While the authors state that their protocol is experimentally feasible on real quantum equipment, they did not perform this experiment.

Zawadzki addressed the information loss to eavesdroppers in [19], stating that even a small loss of information to an attacker is an issue in authentication systems, since the complete authentication information can be gathered in a series of successive protocol runs. Zawadzki proposes improvements [19] to Hong *et al.*'s protocol [6] that address information loss and make it less useful in breaking subsequent authentication attempts. Zawadzki's modifications include adding a classical channel for communication before the quantum channel is used [19]; an approach that is also used in other quantum algorithms such as Shor's factorization [14]. Thus, Alice and Bob must agree not only on a set of bits and related quantum bases (Hong *et al.*'s key), but also a hash algorithm H, which allows them to communicate on classical channels that otherwise are unprotected. Once the hashed shared secret is sent via classical communication channels, Alice encodes her message one qubit at a time with constant speed that must also be known by Bob. Once Bob has received all expected qubits, he checks for missing qubits and rejects the authentication if either the bit error rate or the number of lost qubits is too high [19]. There is no indication in the paper of what is considered "too high" a qubit loss or error rate. Zawadzki then shows that this modified protocol is resistant to the bit leakage and observation attacks known to affect Hong *et al.*'s approach, but there is no discussion of how known attacks on hash algorithms (e.g., collisions) affects the security of the improved scheme, nor an indication of whether the hash function H must be cryptographically strong [19].

3 Future Research Directions

Most of the protocols surveyed in this paper are highly theoretical. Importantly, they assume a perfect quantum system with no information loss or errors in the quantum channel, and idealized qubit generating and detecting implements. Real quantum computers do not exhibit such properties: they are prone to loss of data, inefficient qubit generation, and error-prone qubit detection without information on whether the qubit was lost or simply not detected. Therefore, one avenue of future research is to implement these protocols on currently available quantum hardware in the presence of noise to determine their usefulness, susceptibility to information loss and error, and general usability. To the best of our knowledge, there is also no indication in the literature of how these protocols are to be implemented in real computer systems with real users. Thus, creating an interface between the quantum authentication schemes and classical computing systems is essential. Since this is most likely the part of a QIA system that will be used by real users, they should be tested for usability before being released.

Another rich area for future research is in revokable QIA in which a user can choose to no longer be authenticated in the system. This is similar to revoking a public key that is known to be false, or to be matched with a compromised private key in classical asymmetric cryptography. At present, none of the surveyed research has allowed for revocation, which means that these methods can only be used for short-term authentication sessions. Creating such revokable authentication methods allows for a quantum "ID card" that can be used to prove identity even to those not involved in the one-way or mutual authentication protocols described in this paper. Furthermore, the protocols describe depend heavily on third parties, some on trusted and others on untrusted, but this level of centralization still remains, which provides a single point of failure for these protocols. Removing such a dependence would allow for easier, less time consuming authentication.

Classical authentication may also be undertaken using multifactor authentication, but currently there is no parallel in quantum computing. Given that many of the protocols surveyed herein depend on quantum cryptography, it is unclear where the subsequent factors can be used since crypto-based authentication depends on shared secrets (e.g., keys), which places them in the "something you know" factor. It is possible that the "something you are" factor could be added using traditional biometrics such as fingerprints [9]. However, it is unclear whether the quantum versions of these biometric algorithms fall to the same replay and impersonation attacks as do classical biometric algorithms. The "something you have" factor assumes that the user is in possession of a quantum device, which given the cost, complexity, size, and cooling requirements of current quantum computers is unlikely to exist in the near future. It is possible, however, that physical devices such as smartphones can be modified to communicate with quantum computers, and thus can act as a token much like devices such as the RSA SecurID token (or the smartphone app) [4] provides multifactor classical authentication

There is also a need for QIA algorithms that work to authenticate users of quantum computers, rather than using quantum computers to authenticate users on classical systems. However, this need is not urgent since reliable, powerful quantum computers that use more than 20 qubits are not yet widely available for public use. While research is expanding the usefulness of quantum computers, their use is still somewhat limited as many software practitioners have yet to be trained on how to develop quantum algorithms.

4 Conclusion

This paper has surveyed quantum identity authentication (QIA) protocols based on both entangled and single-photon quantum states. Such QIA protocols can be used to authenticate users on a classical communication network by using the natural properties of quantum computing states to provide security and resistance to attacks such as man-in-the-middle, eavesdropping, replay, and malicious insiders (e.g., untrustworthy trusted third parties). This is a rich area for future research since it is currently unknown if the available protocols can operate on a noisy, intermediate-scale quantum computer while still providing reliable authentication decisions.

[4] https://www.rsa.com/en-us/products/rsa-securid-suite

References

[1] IBM Q Experience, `https://quantumexperience.ng.bluemix.net/qx/community`, Last Checked: May 28, 2019.

[2] Charles H. Bennett and Gilles Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of International Conference on Computers, Systems and Signal Processing*, pages 175 – 179, 1984.

[3] Paul Busch, TeikoHeinonen, and Pekka Lahti. Heisenberg's Uncertainty Principle. *Physics Reports*, 452(6):155 – 176, 2007.

[4] G. Gao and Y. Wang. Cryptanalysis of Controlled Mutual Entity Authentication Using Entanglement Swapping. *Communications of Theoretical Physics*, 67(1):33 – 36, 2017.

[5] Mark Hillery, Vladimir Buzek, and Andre Berthiaume. Quantum Secret Sharing. *Physical Review A*, 59(3), March 1999.

[6] Chang ho Hong, Jino Heo, Jin Gak, and Daesung Kwon. Quantum Identity Authentication With Single Photon. *Quantum Information Processing*, 16(236), 2017.

[7] Chang-Ho Kang, S.J. Hong, Jong-In Lim, and Hyung-Jin Yang. Controlled Mutual Quantum Entity Authentication Using Entanglement Swapping. *Chinese Physics B*, 24(9):116 – 124, 2015.

[8] Min-Sung Kang, Jino Heo, Chang-Ho Hong, Hyung-Jin Yang, Sang-Wook Han, and Sung Moon. Controlled Mutual Quantum Entity Authentication with an Untrusted Third Party. *Quantum Information Processing*, 17(159), July 2018.

[9] Jiawei Li and Ying Guo. Fingerprint-Based Quantum Authentication Scheme Using Encoded Graph States. *International Journal of Theoretical Physics*, 57(10):3271 – 3283, October 2018.

[10] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure Quantum Key Distribution. *Nature Photonics*, 8(8):595 – 604, 2014.

[11] Niu Penghao, Chen Yuan, and Li Chong. Quantum Authentication Scheme Based on Entanglement Swapping. *International Journal of Theoretical Physics*, 55(1):302 – 312, January 2016.

[12] Adi Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612 – 613, November 1979.

[13] Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, and Guang-Can Guo. Quantum Key Distribution and Quantum Authentication Based on Entangled State. *Physics Letters A*, 281(2-3):83 – 87, 2001.

[14] P.W. Shor. Algorithms for Quantum Computation: Discrete Log and Factoring. In *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124 – 134, 1994.

[15] Jian Wang, Quan Zhang, and Chao-Jing Tang. Multiparty Simultaneous Quantum Identity Authentication Based on Entanglement Swapping. *Chinese Physics Letters*, 23(9), 2006.

[16] W.K. Wootters and W. H. Zurek. A Single Quantum Cannot Be Cloned. *Nature*, 299:802 – 803, 1982.

[17] Yu-Guang Yang, Hong-Yang Wang, Xin Jia, and Hua Zhang. A Quantum Protocol for *(t,n)*-Threshold Identity Authentication Based on Greenberger-Horne-Zeilinger States. *International Journal of Theoretical Physics*, 52(2):524 – 530, February 2013.

[18] Yu-Guang Yang and Qiao-Yan Wen. Economical Multiparty Simultaneous Quantum identity Authentication Based on Greenberger-Horne-Zeilinger States. *Chinese Physics B*, 18(8), 2009.

[19] Piotr Zawadzki. Quantum Identity Authentication without Entanglement. *Quantum Information Processing*, 18(7), January 2019.

[20] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. Quantum Secure Direct Communication with Quantum Memory. *Physical Review Letters*, 118, 2017.