SOK: An Evaluation of Quantum Authentication Through Systematic Literature Review

Ritajit Majumdar
Advanced Computing and Microelectronics Unit
Indian Statistical Institute
Email: majumdar.ritajit@gmail.com

Sanchari Das
University of Denver
Email: Sanchari.Das@du.edu

***Abstract*—Quantum computers are considered a blessing to the dynamic technological world that promises to solve complex problems much faster than their known classical counterparts. Such computational power imposes critical threats on modern cryptography where it has been proven that asymmetric key cryptosystem will be rendered useless in a quantum world. However, we can utilize such a powerful mechanism for improving computer security by implementing such technology to solve complex data security problems such as authentication, secrets management, and others. Mainly, Quantum Authentication (QA) is an emerging concept in computer security that creates robust authentication for organizations, systems, and individuals. To delve deeper into the concept, for this research, we have further investigated QA through a detailed systematic literature review done on a corpus of $N = 859$ papers. We briefly discuss the major protocols used by various papers to achieve QA, and also note the distribution of papers using those protocols. We analyzed the technological limitations mentioned by previous researchers and highlighted the lack of human-centered solutions for such modern inventions. We emphasize the importance of research in the user aspect of QA to make the users aware of its potential advantages and disadvantages as we move to the quantum age.**

***Keywords*—** Authentication, Quantum Authentication, Human Factors, Systematic Literature Review.

I. Introduction

The notion of introducing a new form of computing, different from the classical Turing Machine [1], came from the requirements which modern-day computers fail to meet [2]. Feynman pointed out a n-body system which comprises of 2^n parameters, and as n grows large, the problem becomes intractable in classical computers [3]. They first argued for a device that will work at the quantum level and will be able to overcome the drawbacks of classical computers. Such a device that explicitly uses quantum phenomena, such as superposition, entanglement, is called a *Quantum Computing*.

Other researchers also pointed out the differences based on energy usage in addition to the computational differences (speed, accuracy, and others) between quantum computing and classical devices. Landauer showed that every bit of information loss causes a dissipation of $kTln2$ amount of heat, where k is the Boltzmann Constant, and T is the temperature in absolute scale [4]. Bennett later showed that the heat loss could be avoided if the computation is reversible [5] and quantum computing complies with the reversible proposal. Furthermore, in recent times, as the size of the chips in a classical device are made smaller for optimal space and design architecture, quantum effects such as *Tunnelling* is coming into action, which hinders multiple functional and computational tasks [6]. Tunnelling refers to the non-zero probability that any quantum particle has of crossing a potential barrier [7]. Therefore, this hinders lowering the chips' size further, which is a constraint for classical computers compared to quantum computing.

The efficiency of quantum computers is dependent not only on the mechanics it is following but also on how scientists and technologists can utilize specific quantum phenomena such as *Superposition* [8] and *Entanglement* [9], [10], which are not observed in the classical computing realm [11], [12] (explained in detail in section II). Initial research, which showed speedup of quantum algorithms over classical algorithms [2], [13], [14], primarily focused on toy problems, and therefore did not attract much interest of researchers. However, two significant breakthroughs in the research of quantum speedup came when - (i) Shor designed a quantum algorithm to solve prime factorization and discrete logarithm in polynomial time [15], and (ii) Grover designed a quantum algorithm which provided quadratic speedup for NP-Complete problems [16]. While the second one is of theoretical interest, the algorithm by Shor immediately implied that public key encryption such as RSA or Elliptic Curve Cryptography (ECC) could be broken efficiently using a quantum computer. Therefore, we came across imminent online security threats with the emergence and digital evolution of quantum computing [17].

With technological evolution in the quantum computing realm, it became apparent that if the key sharing can be made secure, then private vital cryptosystems such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) will remain secure under quantum attack and can be used for the security purpose [18]. The inability of an eavesdropper to copy a quantum state [19], or even measure it without disturbing the information content [6] comes as a blessing for security in the quantum world. The pioneering research by Bennett was followed by several others that used quantum algorithms for the design of secure key distribution [20], [21] through Quantum Key Distribution (QKD), Quantum Secret Sharing (QSS), Blind Quantum Computation (BQC), and other concepts. A dual notion of security is the authentication of the sender in a communication.

In addition to the threat to modern-day cryptography, we see, on the user side, the digital presence of internet users has increased exponentially [22]. As a result, security attacks and threats have increased to a considerable amount, leading to 76% of global organizations reporting Phishing attacks in 2017 alone [23]. Additionally, with the advent of the COVID-19 pandemic and stay-at-home order, the phishing attacks in the last quarter of 2020 has been doubled since their prior years [24]. As a solution, authentication becomes the primary backbone for online applications and services to provide secure digital interactions for users [25], [26], [27]. Traditional single-factor authentication, such as Passwords, dominated the authentication system design for a long time [28]. However, under the increasing

Workshop on Usable Security and Privacy (USEC) 2021
7 May 2021, Auckland, New Zealand
ISBN 1-891562-73-8
https://dx.doi.org/10.14722/usec.2021.23003
www.ndss-symposium.org

complexity of threats on the internet, password, and pass-the-hash (password hash or authentication token) [29] is susceptible to several security vulnerabilities [30].

Thus, we cannot rely on a single-factor of authentication for mission-critical sectors such as finance, health care, government, and others [31]. Several solutions have been proposed to perform secure identity and access management (IAM), including graphical password, biometrics [32], hardware tokens [33], [34], visual tokens [35] etc. that are capable to replace traditional single-factor password authentication [36], [37], [38]. Researchers have even proposed to enhance password strength [39], [40] or enhance the usability of Multi-Factor Authentication (MFA) [41], [42], [43], [44]. However all such methods can be ineffective due to lack of human focused solutions [45], [46], [47], [48]. Lack of user focused research is constantly noticed in computer security [49], [50], [43]. Additionally, we see a new trend on studying, implementing, and expanded the authentication protocols through quantum computing [51], [52], however, it is important to note the relevance of such advancement both from technological and user side.

In that regards, in this paper we discuss about Quantum Authentication (QA) protocols and the use of Quantum Key Distribution (QKD), Quantum Secret Sharing (QSS), Blind Quantum Computing (BQC) and some other techniques for their implementation [53], [54], [55], [56], [57]. Prior to this, Crowford and Atkin studied the current and future research directions on QA [58]. However, discussing about quantum computing as a solution, though a fair amount of research is focusing on QA, our aim was to analyze if we are focusing on the user side of QA at all. To aid this we conducted a systematic literature survey on a corpus of $N = 859$ papers collected from ACM digital library, Google Scholar, Scopus, and IEEE Xplore. To our dismay, we found that none of the papers discusses the user side of QA or does any user study to evaluate the impact of the implementation of such authentication protocol. We acknowledge that we are still looking for technical feasibility for most of these solutions proposed, however forgoing the user side is extremely harmful as we see from prior research. Thus, we propose for further research on the human-centered component to enhance the effectiveness of such solutions.

Our paper presents a brief overview of related works in the quantum computing domain in Section II. Section III details the methodology followed in our systematic review, where we detail the data collection and screening procedure. This section is followed by the Findings in Section IV that details the quantum authentication, key distribution, entanglement, secret sharing, and other concepts introduced by the studied papers. After that, we discuss the importance of the user aspect towards QA (or lack thereof) in Section V. We conclude by providing the necessity of user aspect research in Section VI and summarize our work in the conclusion Section VII.

II. Background of Quantum Computing

To understand the fundamentals of *Quantum Computing*, in this section, we briefly describe the postulates and laws which govern the state, evolution, and measurement of a quantum system. We explain the technological component of *Quantum Computing* as noted and summarized in the book "Quantum Computation and Quantum Information " by Nielson et al. [6].

1) *Quantum State*: The basic unit of information in a quantum computer, termed as qubit, is represented as a unit vector in Hilbert Space. A Hilbert Space can be loosely defined as a complex vector space with inner product. Unlike classical bits, a qubit can be in $|0\rangle$, $|1\rangle$ states or in a linear superposition of them [6]. A general qubit is represented as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. Therefore, a system of n qubits $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$ can reside in all 2^n possible configurations simultaneously.
2) *Evolution of qubit*: Evolution of a quantum system is governed by unitary operators. A unitary matrix (the mathematical representation of unitary operators) is always invertible. Thus, from the mathematical computation logic, a quantum computer governed by the unitary matrix is reversible by nature.
3) *Measurement principle*: Measurement of a quantum system is always associated with some basis. Any arbitrary quantum state can be written in multiple basis. For example,
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \tfrac{\alpha+\beta}{2}\,|+\rangle + \tfrac{\alpha-\beta}{2}\,|-\rangle$$
where $\{|0\rangle,|1\rangle\}$ is called the computational basis, and $\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ is called the Hadamard basis. There are infinitely many bases in which the same quantum state can be represented. Consider a quantum state $|\psi\rangle = \sum_i \alpha_i\,|b_i\rangle$, where $\{|b_i\rangle\}$ forms an orthonormal basis. Upon measurement in this basis, the state $|\psi\rangle$ collapses to one of the basis states $|b_i\rangle$ with probability $|\alpha_i|^2$. However, once the state has collapsed to $|b_i\rangle$, consequent measurements in the same basis yields the same outcome with certainty.
4) *No Cloning Theorem*: It was shown by Wootters et al. [19] that there exists no universal operator which can clone any arbitrary quantum state $|\psi\rangle$, i.e., it is not possible to design an operator U for all probable states $|\psi\rangle$, $U\,|\psi\rangle = |\psi\rangle \otimes |\psi\rangle$. This theorem immediately rules out the possibility of any eavesdropper in a quantum world to copy the information transmitted. Thus, the no cloning theorem helps in preserving the data confidentiality, in terms of the security triad- Confidentiality, Integrity, and Availability (CIA) components [59].

Additionally, measurement postulate as explained earlier and no cloning theorem rules out the possibility of an eavesdropper to copy or gain any information of the sent qubits without disrupting the process. This creates the possibility of identification of the malicious actor with attempted eavesdropping. However, these do not render an eavesdropper completely powerless over a quantum communication channel, which we will be discussing in the later sections. Additionally, we also discuss through the systematic literature review on the protocols which assures complete secrecy even in the presence of an eavesdropper.

III. Methodology

The first study of security in a quantum world dates back to as early as 1984 [60] and the first paper on quantum authentication was published in 1998 [61]. However, in this systematic literature review, we are primarily focusing on recent developments on quantum computing in the realm of digital authentication and security, thus we focus on papers published in between 2009–2019. We collected our data by starting with research publications on QA that are included in the ACM Digital Library, IEEE Xplore, Scopus, Google Scholar, and Web of Science. We performed the data extraction using ACMs export feature, IEEE Xplore repository, and Publish or Perish [1].

Thereafter, the researchers of this paper implemented a qualitative assessment protocol that utilized exclusion and inclusion criteria to generate a set of papers that were relevant for our analysis. The result yielded a total of 859 published papers on Quantum Computing in digital security, from which we eventually identified 118 papers that included Quantum Authentication. Two researchers applied thematic coding on the abstract and full text of each of these 118 papers to enable the systematic analysis of the reported research articles.

A. Data Collection and Screening

1) Title Screening: The initial process for our data collection began as a broad search for the term "Quantum Authentication" in the ACM Digital Library, IEEE Xplore, Scopus, Google Scholar, and Web of Science databases.

This generated 859 papers; 449 from Google Scholar, 200 from Scopus, 190 Web of Science, and 20 from ACM Digital Library. While scanning through these papers, we rejected papers where the

[1] www.harzing.com/resources/publish-or-perish

full-text were not available despite contacting the publisher or the authors of the paper. From this collected set of papers, we first removed any duplicate studies and found a total corpus of 478 papers. Our research is focused primarily on the current research of Quantum Authentication, thus we included those paper published in 2009 or later (111 papers were discarded).

To be included in our corpus, a paper needed to be primarily focused on the topic of QA. Papers were excluded if: (1) they were an extended abstract or a work-in progress, (2) the primary language in which they were written was not English, or (3) they were found not to be related to QA, even if they mentioned quantum computing somewhere in the paper. After applying the exclusion criteria on the collected sample of 367 papers, we were left with 118 papers. Two researchers trained in qualitative data coding and analysis independently completed the thematic analysis to find the different aspects of Quantum Authentication that was studied while applying the exclusion criteria in the collected corpus. Figure 1 shows the distribution of the corpuss studies focusing on Quantum Authentication over 10 years period from 2009 – 2019. Beginning in 2009 with seven papers published in this domain, we see a positive publication trend.

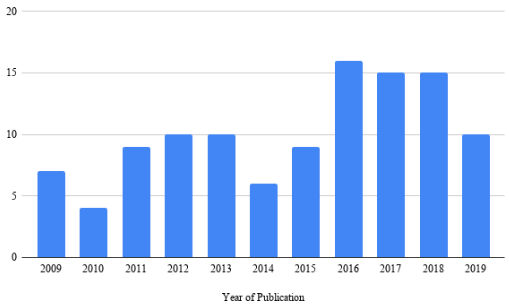

Fig. 1. Distribution of the Number of Publications in Our Data Set ($N = 118$) Grouped by the Year of Publication.

Abstract and Full Text Screening: After title screening, we performed abstract and full text screening to identify papers that satisfied our inclusion and exclusion criteria. Interestingly, out of 478 papers having "Quantum Authentication" in their title, 289 papers were published on or after 2009. A detailed study of these papers showed that many of these 289 papers focused on Post-quantum scenario (which are classical cryptosystem designed to be secure against quantum attacks). We removed these papers, since they were out of scope for this research and retained 239 papers. While we studied the abstracts of these papers, we found that many of them focused primarily on secure communication, and did not even mention authentication once in the abstract. We discarded these papers as well leading to a final repository of 118 papers. In the following section, we review the design technique and implementation of the authentication protocols which have been studied. The selected corpus was analyzed using thematic coding as well to find the over arching themes in the papers discussed by two researchers who were trained in qualitative coding. For thematic analysis, the researchers went through rigorous training and the inter-coder reliability was 96.7% after three interactions of the subset that was analyzed.

IV. Findings

As mentioned, we investigated the overarching concept of Quantum Computing while focusing on authentication strategies which included technical aspects of secret sharing as well. The first authentication protocol, proposed by Barnum et al. [61] used Quantum Error Correction technique for authentication which, unfortunately, requires a large number of qubits for its implementation. Therefore, the subsequent authentication protocols primarily take motivations from QKD, QSS, and BQC protocols, and some novel protocols different from these. Table I shows the overall distribution of the papers based on the themes developed by the researchers. In this section, we explain the technological concepts of QA and thereafter mention the papers which detailed them from our corpus.

TABLE I
Thematic distribution of QA papers

Protocols based on		# papers
QKD	Entanglement-assisted	30
	Without entanglement	15
QSS		8
BQP		3
Deniable authentication	Entanglement-assisted	5
	Without entanglement	3
	Real-world application based	13
Authentication of classical message in quantum scenario		9
Implementation oriented framework		6
Others		26
Total		118

A. Quantum Authentication (QA)

Authentication can be considered as an integral task of secure digital interactions. Going with Alice and Bob security examples with them being the two actors in the scenario, it may be possible that Alice and Bob share some information in a scenario where the data integrity, rather than the security of the message is of importance. This means Bob wants to be sure that the message they received is from Alice, and has not been tampered with some middle-person Eve. Classically, there are several techniques to achieve authentication, such as digital signature [62], universal hash function [63], etc.

From mathematical perspective, If Alice and Bob share a secret k, then they can produce a signature s for a particular message m, where $s = f_k(m)$. The entire message sent by Alice is then $(m, f_k(m))$. Upon receiving a possibly tampered message (m', s'), Bob can authenticate the sender if $s' = f_k(m')$. This technique of authentication is called digital signature. The first quantum authentication scheme used this technique for authentication of quantum messages. Authenticating quantum information impose some extra challenges. Two primary difficulties can be enlisted as follows:

1) In a classical message, Eve can at most flip one or more bits. For quantum information, any rotation operator $R(\theta)$, operated by Eve, is a tamper. Therefore, there are infinitely many possible tampering.
2) If the original qubit was $|\psi\rangle$, whereas the tampered message is $|\psi'\rangle$, there exists no operator which can distinguish the two states for any $|\psi\rangle, |\psi'\rangle$.

A technique to overcome these difficulties for authentication of quantum information was first studied by Barnum et al. [61], which uses error correction techniques. Consider g qubits of information $|\psi\rangle$ which can be encoded into $n > g$ qubits using some quantum error correction code (QECC) [64]. If $\mathcal{E}$ is the encoding algorithm, then Bob receives the state $\mathcal{E}(|\psi\rangle)$. If $\mathcal{D}$ is the decoding algorithm, then if the message was untampered, i.e., there is no error on the quantum state, then $\mathcal{D}(\mathcal{E}(|\psi\rangle))$ should produce syndrome 0. Any error correcting code $\mathcal{C}$, which has the capability of correcting m errors, can authenticate a message if Eve tampers at $l \leq m$ positions. However, there is a shortcoming to this process.

If the same QECC is used repeatedly, then Eve can identify the distance of the code and can fool the parties by introducing appropriate errors which cannot be detected by that QECC. In order to avoid this, the QECC can be drawn from a family of codes. The information of the QECC used for a particular message is encoded into a key k, and $|\psi\rangle \otimes |k\rangle$ is transmitted. A major drawback of this simple technique is that there is a significant increment in the required number of qubits. Furthermore, the encoding and decoding algorithms of many QECC can lead to a significant computation overhead as explained by Majumdar et al. [65], [66], [67]. Subsequent studies on QA, therefore, use other techniques for its implementation. In the following subsections we briefly define QKD, QSS, BQC and review their applications for various authentication protocols as studied by the researchers.

B. Quantum Key Distribution (QKD)

QKD protocols can be broadly divided into two themes - those which use entanglement, and those which do not. The first QKD protocol (Bennett et al. [60]) achieved secure key distribution without entanglement. Ekert [20] later came up with the first entanglement-assisted QKD protocol. Our review shows that 45 out of 118 papers on Quantum Authentication protocols have been inspired by QKD protocols (e.g. Gong et al. (2012) [68], Lin (2013) [69], Rass et al. (2015) [70], etc.) out of which 30 papers focus on the entanglement phenomena (e.g. Tan et al. (2014) [71], Kang (2015) [72], Alshowkan et al. (2016) [73], etc.).

1) BB84 Protocol: The first QKD protocol, called the BB84 protocol, was proposed by Bennett et al. [60], which does not use entanglement. In this protocol, the sender has n qubits, prepared randomly in state $|0\rangle$ or $|+\rangle$. The sender then measures each qubit randomly in the computational or the Hadamard basis, stores the measurement outcome, and sends the qubit to the receiver. The receiver also follows the same protocol. After both of their measurements, they publicly declare their choice of basis. Whenever, their choices do not match, the corresponding qubit is discarded. If they measure in the same basis, then by the Measurement Principle, their outcome should be the same. If their outcome is $|0\rangle$ or $|+\rangle$, then its corresponding classical bit is recorded as 0, otherwise 1. If there is some eavesdropper, Eve, who is trying to get hold of the secret key, the best they can do is to measure the qubit in some basis before the receiver receives it. However, the measurement principle asserts that if the choice of basis of Eve and the sender is not the same, then the measurement by Eve disturbs the qubit. It was proved by the authors that if the sender and the receiver declare the measurement outcome for half of their qubits (chosen randomly), then the disturbance created due to the measurement of Eve can be detected with very high probability.

Authentication protocols motivated by BB84: BB84 protocol has the advantage that it does not require any prior secret to be shared between the parties in the communication network. In the language of cryptography, this implies that sharing of prior secret is not necessary. This advantage has been used in various authentication protocols studied by X. Zhang (2009) [74], Y. Jing (2010) [75], H. Yuan (2014) [76], and other recent articles [77], [78], [79], [80], [81], [82], [73]. M. Oya proposed a QKD based authentication protocol which has better security measures than its predecessors, and was also shown to be implementable in Photonics technology [83]. Ghilen et al. suggested the incorporation of Quantum Cryptography and authentication protocols in the IEEE 802.11i Standards for enhancing its security. A disadvantage of most cryptographic systems is that the same key cannot be used multiple times [84]. However, in other studies, the authors came up with QKD based authentication protocols such that the same key can be recycled without the Eve being able to tamper with the message [85], [75], [86]. A disadvantage of BB84 is that in order to set up a key of size N, at least $2N$ qubits must be transmitted [60]. In the subsequent part, we discuss authentication protocols motivated by entanglement-assisted QKD. Ekert proposed first QKD which used entanglement for secure key distribution. For the sake of completeness, we first briefly discuss the concept of entanglement followed by the protocol of [20].

Entanglement: A quantum system $|\psi\rangle$, consisting of $n > 1$ qubits, is said to be entangled if it cannot be written as $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$, where $|\psi_i\rangle$ is the state of the i^{th} qubit. For example, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$ is an entangled state. If this state is shared between two parties A and B, then irrespective of the distance between them, measurement by any party disturbs the state of the other. If the measurement outcome of party A is $|0_A\rangle$ ($|1_A\rangle$), then the state of party B is also $|0_B\rangle$ ($|1_B\rangle$) with certainty, even though party B may not have made any operations on their qubit. An entangled state of the form of $|\phi^+\rangle$ is often called Maximally Entangled State, or Bell State [9]. There are four Bell states which form a basis for the two qubit vector space. Bell states are heavily used in protocols on security and communication [87], [88].

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle \pm |1_A1_B\rangle) \qquad |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0_A1_B\rangle \pm |1_A0_B\rangle)$$

2) Ekert91 Protocol [20]: This protocol makes use of quantum entanglement, and the principle of monogamy [6] which states that a maximally entangled state cannot be entangled with any other qubit. In this protocol, the sender Alice and the receiver Bob shares N Bell states between them. Alice and Bob both measure their qubits in the computational basis. Entanglement asserts that the outcome of Alice and Bob will be the same. If the outcome of the i^{th} pair is $|j\rangle$, $j \in \{0,1\}$, then the i^{th} bit of the key is j. This protocol immediately rules out the disadvantages of the BB84 protocol that the two parties may measure in different bases. However, a difficulty is that Alice and Bob may not have the resources to create N pairs of entanglement between them. Therefore, they are likely to rely on a third party Eve to deliver the entangled states to them. The natural question which arises is - *what happens if Eve herself is dishonest*?

The natural trickery of Eve will be not to prepare the requested Bell state, but to create some other state $|\zeta\rangle = \sum_{i,j} \alpha_{ij} |ij\rangle |e_{ij}\rangle$ where the first two qubits are sent to Alice and Bob respectively, and the third qubit $|e_{ij}\rangle$, which is entangled with the other two qubits is in possession of Eve. Upon measurement by Alice and Bob, if their qubits collapse on the state $|ij\rangle$, then the state of Eve will collapse on $|e_{ij}\rangle$, and hence Eve has perfect knowledge of the outcome. However, it was proved by the author that Eve is not detected if and only if the state they deliver is a maximally entangled state (as required for the original protocol). Moreover, monogamy rules out the possibility of Eve being able to entangle their own system with the maximally entangled pair. Therefore, even if Eve sends the entangled pairs to the two parties, they should either be honest, or their deceit will be detected.

Authentication protocols using entanglement-assisted QKD: Use of entanglement for authentication purpose has been ubiquitous in the literature. In several other studies the authors have used Bell states for identity authentication in quantum scenario [89], [90], [91], [69], [92], [69], [93], [94], [95]. Extensive security analysis of some of these protocols have been studied in [96], [97], [98]. Entanglement swapping is a process which allows the entanglement between two parties A and B to be generated perfectly between some other parties C and D using teleportation [88], [**?**]. Entanglement swapping has been successfully used as a method for quantum authentication [99], [100], [101], [72], [102]. Some of these protocols allow even authentication of multiple parties [103], [104], [71]. Communication over a network with more than two parties is necessary is realistic scenario. In such scenarios, every pair of parties may share Bell states (requiring a large number of such states), or multi-party entangled states can be used. Authentication protocols over networks, therefore, often use multi-party entangled states such as GHZ states [72], [105], [106], [107], [108] or W-states [109], [110].

C. Quantum Secret Sharing

Consider the scenario where the President of a bank wants to give access to a vault to three vice-presidents, whom they does not trust completely. If any one of them is compromised, then the security of the vault is compromised too. Therefore, it may be desirable to share the secret among them such that no one of them has the complete information of the security, but any two of them together can get the complete information. This process of distributing a secret S among multiple parties $S_1, S_2, \dots, S_n$, such that the knowledge of any k of them together is sufficient to determine S, but knowledge of $k-1$ or fewer pieces leaves the secret unknown, is called Secret Sharing. The first (k, n) Secret Sharing protocol was introduced by Shamir [111]. Many variants of this protocol, including scenarios where some of the parties are cheaters, have been studied henceforth. Hillery et al. studied $(2, 2)$ quantum secret sharing [112] in which Alice divides the secret between Bob and Charlie such that no one of them alone can decipher the secret. Consider the three parties sharing a single qubit of the GHZ state ($|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$), which is a three party entangled state. Each of the three parties randomly decide their basis of measurement as one of the following

$$|\pm x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \qquad |\pm y\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$$

TABLE II
Effect on Charlie's state due to measurement of Alice and Bob

Bob ↓	Alice →			
	+x	-x	+y	-y
+x	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle - i\,\|1\rangle$	$\|0\rangle + i\,\|1\rangle$
-x	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle + i\,\|1\rangle$	$\|0\rangle - i\,\|1\rangle$
+y	$\|0\rangle - i\,\|1\rangle$	$\|0\rangle + i\,\|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$
-y	$\|0\rangle + i\,\|1\rangle$	$\|0\rangle - i\,\|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$

The basis of measurement for each party is declared publicly, but not the outcome of the measurement. In a scenario, Alice and Bob measure in their declared basis the effect of their measurement on the state of Charlie is shown in Table II. Suppose that Alice and Bob both decided to measure in $|\pm x\rangle$ basis. This decision is also known to Charlie since it was declared publicly. However, if Charlie's state is $|0\rangle + |1\rangle$, they are not sure whether the outcome of Alice and Bob was both $+x$ or $-x$. Therefore, Charlie alone cannot determine the secret. Moreover, Bob alone, who knows the outcome of their measurement and the choice of basis by Alice, cannot determine the outcome of Alice. However, if Bob and Charlie come together, then armed with the knowledge that Bob received outcome $+x$ (say) and Charlie has the state $|0\rangle + |1\rangle$, they can uniquely determine the outcome of Alice's measurement. Several variants of this protocol has been studied henceforth [113], [114], [115], [116], [117]. These studies involve multiparty secret sharing, sharing secret in the presence of an eavesdropper and in the absence of entanglement. A concise theory of quantum secret sharing is available in [118].

Authentication protocols motivated by QSS: Quantum secret sharing techniques have been applied to develop authentication protocols. The primary theme in such protocols is that a trusted third party can authenticate one or multiple users, although a single party cannot alone authenticate other parties. In some of these protocols, as proposed by Wei et al. (2011) [119], W. Yie (2016) [120], and Abulkasim (2017) [121], QSS technique have been applied to authenticate a single party at a time, whereas in Bartkiewicz et al. (2014) [108] the trusted third party can simultaneously authenticate more than one parties involved in the communication. Certain QSS protocols [114] can share a secret when at least t out of n parties can assemble together. For an n party communication system, it is often more realistic to assume that all the parties will not be available at the same time. This technique of QSS proposed by Li et al. [114] has been the motivation for authentication protocols by B.B. Elliott (2008) [122] and Cao et al. (2012) [123] where only $t < n$ parties can participate for the authentication purpose at a time.

D. Blind Quantum Computation

Small scale quantum computers are already made available by companies such as IBM, DWAVE, and some companies such as Google, Microsoft are in the verge of having their own quantum computer. However, modern day quantum computers are expensive, and hence it does not seem likely that individuals can have their own personal quantum computer any time soon. The natural solution for this, which IBM has already implemented, is for companies to outsource their machines. Individuals can run their program on the quantum computer over cloud. IBM already has a 15 qubit quantum computer which anyone can access over cloud. This technique, however, raises the question of privacy in quantum world. Since every individual has to perform their task on a quantum server over cloud, the server can have complete information of each individual client, and their task. A technique to ensure masking the job of any client over the cloud is termed as Blind Quantum Computation (BQC). Ideally BQP protocols should involve a client with classical computer interacting with a single server with unlimited quantum power, and still maintain their secrecy. However, current BQP protocols tend to relax these assumptions to some extent. It was first shown that if the client has limited quantum capabilities, then they can encrypt their data such that the server operating on this encrypted data cannot gain knowledge of the original information of the client [124].

In the article titled "Universal blind quantum computation" , the authors could overcome the constraint of the client having quantum capabilities [125]. Instead, the authors showed that if the clients can prepare qubits, then they can divide their task into two quantum servers, and reconstruct their solution from the output of the two. This idea is similar to quantum secret sharing, where each server has only a part of the information, and cannot reconstruct the entire information of the client from the parts. Another technique, called Measurement Based Quantum Computing (MBQC) [126], considers n qubits in a quantum server is stored in a two-dimensional array structure. To perform a task, a unitary operator U^n is to be constructed which operate on all the n qubits, followed by a measurement on all of them to yield the output. However, the authors showed that it is possible for the client to design U^n such that

$$\exists\ U_1, \dots, U_k, k \le n,\ U^n = U_1 \otimes U_2 \otimes \dots \otimes U_k$$

where each U_i acts only on a subset of the qubits. With such a design, the client can then ask the server to operate each U_i on some of the qubits only. Moreover, instead of measuring all the n qubits together, the client can ask the server to measure a subset of the qubits at a time. Each U_i, and each measurement yields only a partial result to the server. However, the client, who knows U^n and its decomposition, can reconstruct the actual solution from these partial results. Further researches are being conducted to achieve the ultimate goal where a classical client can blindly interact with a single quantum server [127]. Nevertheless, the existing protocols show that it is possible for a client to retain their privacy even when interacting with a possibly malicious quantum server.

Authentication protocols for BQP: Our systematic literature review show that authentication for BQP is an area less studied. Li et al. provided a general framework for authentication in BQP protocols [128]. W. Zeng proposed an authentication protocol for BQP and proved it to be secure against Man-in-the-Middle and Denial-of-Service attacks [129]. Authentication for centralized cognitive radio network was studied by Q. Li [130]. BQP protocol and its authentication technique was applied for a framework for Online Banking system W. Zeng [129]. However, it is evident that this area of research has received lesser attention of the researchers as of yet.

E. New Schema

There are several studies where novel techniques, different from QKD, QSS and BQC, are used for authentication. A study which appears quite a few times in the literature is Quantum Deniable Authentication. In this process, if Bob received a message from Alice, then they can authenticate the message himself, but cannot authenticate it to some third party. Jin et al. [131], A. Ameriher [132], and some other articles [133], [134], [135] have studied entanglement-assisted deniable authentication protocol, whereas X. Li [136], Y.

Kanamori [78], Cao et al. [137] proposed deniable authentication protocols without the requirement of entanglement. Cederlf studied deniable authentication in the scenario where the third party is not trustworthy [138]. A theoretical framework for the application quantum authentication to online banking system (Liu et al. [139]) and the application of quantum deniable authentication to electronic voting system (Hughes et al. [140]) have also been studied in the literature. Quantum world do not render classical communication completely useless. Therefore even in a quantum communication system, it may become necessary to authenticate classical messages. Other researchers also studied the authentication of classical messages in a quantum network [141], [142], [143], [144], [145], [146].

A recent trend of study for the Noisy Intermediate Scale Quantum (NISQ) era [147] is to develop hybrid classical-quantum systems so as to reduce the requirement of quantum devices, which is costly. Researchers have also studied classical-quantum hybrid authentication protocols [148], [149]. However, studies on semi-quantum authentication, where some of the parties may not have quantum techniques seem limited [93]. Another natural question which arises is how to implement the authentication protocols in practice. From our literature analysis, it seems that photonics is the leading technology which the researchers have used for the implementation of certain protocols. Most of these studies are theoretical, which propose an experimental framework (Cederlf [138], Yang et al. [150], Hong [145]). In Rass et al.'s [120] and Buhari et al.'s [151] work, the authors have proposed quantum authentication protocols which require only a single photon for their implementation.

Noise in the system is a serious hindrance to the implementation of any quantum computing protocol. While the previous mentioned articles are theoretical frameworks, Oya et al. [152] have experimentally implemented quantum authentication for two parties using optics. Their efficient optical setup has allowed a low error probability of $\mathcal{O}(10^{-3})$. Application of quantum authentication in real-world scenario has attracted the interest of many researchers. H. Ma [80] and Devi et al. [153] have applied quantum authentication in IOT networks, and Murali et al. [154], Akila et al. [155], B. Lari [156] have applied it to wireless network communication. Some research works have also shown the application of QA to cloud computing networks [94], [157], [158], [159]. Kiktenko et al. [160] have recently proposed lightweight QKD and authentication protocols for use in small devices. Murali et al. have even proposed to enhance the security of IEEE 802.11i standard by incorporating quantum cryptography and authentication with it [161] .

Two areas which have been less studied are - (i) authentication in the presence of noise. Huang [162] studied the performance of authentication in the presence of Gaussian noise, and in [163], Li et al. studied authentication under amplitude damping and depolarizing noise channels. (ii) quantum authentication in biometric systems. Zhu et al. [164] studied quantum authentication using face recognition. One primary difficulty to these biometry based authentication is the efficient encoding of data in qubits, which is an ongoing field of research till today [165].

V. Discussion: User Aspect of QA

In this study, we have conducted a systematic literature review of quantum authentication protocols, and the various themes from which these protocols have been inspired. Our study show that majority of these protocols have been motivated from Quantum Key Distribution; in fact 38.13% of the papers on authentication are motivated from QKD protocols. 17.79% of the articles focus on deniable authentication, out of which 61.9% have designed framework for its application in real-world IOT, wireless network or cloud network architecture. On the other hand, only 7.6% and 5.08% of the papers focus on authentication of classical message in a quantum communication network and on their experimental implementation. Out of those papers on experimental implementation, only a single paper has actually implemented an authentication protocols, whereas the others have provided experimental frameworks.

Experimental realization require authentication protocols which are robust to the noise in the system. However, only two papers focus on the realization of these protocols in noisy environment. Therefore, it seems logical to infer that although there is a plethora of research on quantum authentication, both theoretical and technological research for its implementation is lagging behind. Another area which has not received lime light of the research is the user aspect of QA. BQC is an area of security which has been studied to maintain the secrecy of the user in a cloud based platform of quantum computing. However, only three papers have focused their study on authentication in a BQC based protocol. Furthermore, only three papers have studied biometric (fingerprint and face recognition) authentication in a quantum world. Amongst such analysis we find that most of the papers are theoretical contribution , and even if there are technical implementations, none of them conduct any user studies. While, discussing about authentication it is extremely critical to analyze the user aspect, given that the negative or misaligned perceptions of users [50] can often lead to failure in adaption [42].

User side is often the last concept to be added into any technological development, especially for authentication [166]. However, previous studies prove the usability while architecture and designing to not only gauge the technical feasibility but also the user side. From this systematic literature review, we can infer that quantum authentication has been rooted in a firm theoretical notion by now. However, its practical application in a noisy environment, and the user aspect is largely lacking and demand extra focus from the researchers in near future, which we are proposing to be established in design during the developmental stage through iterative mechanism.

VI. Future Work and Limitation

Our study provides with an overview of research done on Quantum Authentication, and through detailed research we indicate the dearth of user component in any of the studies. We understand that we limited our research to papers published between 2009-2019, which might have left the analysis of a few papers. However, with the current lack of focus on user side of quantum authentication, as a future direction we propose this proposition into analyzing the user perception and whether we users comprehend QA and can utilize the computational capability of the same. We will also include *Security by Design [167]* concept to be inbuilt which helps in evaluating the usability in an iterative manner instead of putting user experience as an evaluating factor at the end. Additionally, while utilizing this we want to developed user centered authentication architectural which will utilize the theoretical concepts developed in previous studies over the past 19 years of research in quantum authentication.

VII. Conclusion

In this systematic literature review, we have studied a corpus of $N = 859$ papers on quantum computing, and analyzed in depth a total of 118 papers on quantum authentication published between $2009 - 2019$. We have found that majority of these protocols are motivated from QKD and QSS, primarily introducing theoretical framework for the application of QA in modern IOT, wireless sensor, or even cloud computing network. Additionally, we noted that although photonics seem to be the most promising technology for implementation of quantum authentication protocols, most of these studies are theoretical, and there is only a single experimental implementation of QA. Nevertheless, the performance of QA in experimental noisy scenario, as well as its user aspect has been largely overlooked in the literature as of yet where even while applying QA for biometrics no user studies have been conducted to evaluate the efficacy or feasibility of Quantum Authentication. We propose security by design along with the computational component of QA where user evaluation is done iteratively in every stage along with the technological realization of QA into a tool.

References

[1] A. M. Turing, "On computable numbers, with an application to the entscheidungsproblem," *Proceedings of the London mathematical society*, vol. 2, no. 1, pp. 230–265, 1937.

[2] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[3] R. P. Feynman, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6, pp. 467–488, 1982.

[4] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM journal of research and development*, vol. 5, no. 3, pp. 183–191, 1961.

[5] C. H. Bennett, "Notes on landauer's principle, reversible computation, and maxwell's demon," *Studies In History and Philosophy of Science Part B: Studies In History and Philosophy of Modern Physics*, vol. 34, no. 3, pp. 501–510, 2003.

[6] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[7] D. J. Griffiths, *Introduction to quantum mechanics*. Prentice Hall, second edi, 2010.

[8] E. Schrödinger, "An undulatory theory of the mechanics of atoms and molecules," *Physical review*, vol. 28, no. 6, p. 1049, 1926.

[9] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[10] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, p. 777, 1935.

[11] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 339–354, 1998.

[12] J. Ding and B.-Y. Yang, "Multivariate public key cryptography," in *Post-quantum cryptography*. Springer, 2009, pp. 193–241.

[13] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.

[14] D. R. Simon, "On the power of quantum computation," *SIAM journal on computing*, vol. 26, no. 5, pp. 1474–1483, 1997.

[15] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," *arXiv preprint quant-ph/9605043*, 1996.

[17] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum cryptography," *Scientific American*, vol. 267, no. 4, pp. 50–57, 1992.

[18] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1984, pp. 475–480.

[19] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, p. 802, 1982.

[20] A. K. Ekert, "Quantum cryptography based on bells theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[21] K. Nagata, T. Nakamura, and A. Farouk, "Quantum cryptography based on the deutsch-jozsa algorithm," *International Journal of Theoretical Physics*, vol. 56, no. 9, pp. 2887–2897, 2017.

[22] M. Tan and T. S. Teo, "Factors influencing the adoption of the internet," *International Journal of Electronic Commerce*, vol. 2, no. 3, pp. 5–18, 1998.

[23] B. Team, "Must-know phishing statistics 2018," 2018. [Online]. Available: https://blog.barkly.com/phishing-statistics-2018

[24] Anti Phishing Working Group, "Phishing activity trends report: 4th quarter 2020," in *Activity October-December 2020*, 2021.

[25] D. Ferraiolo, J. Cugini, and D. R. Kuhn, "Role-based access control (rbac): Features and motivations," in *Proceedings of 11th annual computer security application conference*, 1995, pp. 241–48.

[26] R. Heiland, S. Koranda, S. Marru, M. Pierce, and V. Welch, "Authentication and authorization considerations for a multi-tenant service," in *Proceedings of the 1st Workshop on The Science of Cyberinfrastructure: Research, Experience, Applications and Models*. ACM, 2015, pp. 29–35.

[27] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[28] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[29] A. Oberle, P. Larbig, R. Marx, F. G. Weber, D. Scheuermann, D. Fages, and F. Thomas, "Preventing pass-the-hash and similar impersonation attacks in enterprise infrastructures," in *Advanced Information Networking and Applications (AINA), 2016 IEEE 30th International Conference on*. IEEE, 2016, pp. 800–807.

[30] R. Joyce, "Disrupting nation state hackers," *USENIX Enigma. San Fransisco, CA*, 2016.

[31] M. A. Ward, "Information systems technologies: A public-private sector comparison," *Journal of Computer Information Systems*, vol. 46, no. 3, pp. 50–56, 2006.

[32] C. Adams and M. J. Wiener, "Multi-factor biometric authenticating device and method," 2002.

[33] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[34] E. R. Potter, "Multi-factor authentication using a one time password," Oct. 9 2008, uS Patent App. 11/697,881.

[35] A. P. Sabzevar and A. Stavrou, "Universal multi-factor authentication using graphical passwords," in *Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on*. IEEE, 2008, pp. 625–632.

[36] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 553–567.

[37] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568–581, 2014.

[38] J.-J. Kim and S.-P. Hong, "A method of risk assessment for multi-factor authentication," *Journal of Information Processing Systems*, vol. 7, no. 1, pp. 187–198, 2011.

[39] L. J. Camp, J. Abbott, and S. Chen, "Cpasswords: Leveraging episodic memory and human-centered design for better authentication," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 3656–3665.

[40] Y.-Y. Choong, M. Theofanos, and H.-K. Liu, *United States Federal Employees' Password Management Behaviors: A Department of Commerce Case Study*. US Department of Commerce, National Institute of Standards and Technology, 2014.

[41] A. Amin, I. ul Haq, and M. Nazir, "Two factor authentication," *International Journal of Computer Science and Mobile Computing*, vol. 6, pp. 5–8, 2017.

[42] S. Das, A. Dingman, and L. J. Camp, "Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key," in *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018.

[43] S. Das, B. Wang, Z. Tingle, and J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review," unpublished.

[44] D. M. Ting, O. Hussain, and G. LaRoche, "Systems and methods for multi-factor authentication," Aug. 25 2015, uS Patent 9,118,656.

[45] J. Abbott, D. Calarco, and L. J. Camp, "Factors influencing password reuse: A case study," in *Telecommunications Policy Research Conference on Communications, Information and Internet Policy (TPRC 46). DOI: http://dx. doi. org/10.2139/ssrn*, vol. 3142270, 2018.

[46] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[47] J. Lang, A. Czeskis, D. Balfanz, M. Schilder, and S. Srinivas, "Security keys: Practical cryptographic second factors for the modern web," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 422–440.

[48] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Advanced persistent threats: Behind the scenes," in *Information Science and Systems (CISS), 2016 Annual Conference on*. IEEE, 2016, pp. 181–186.

[49] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards implementing inclusive authentication technologies for older adults," *Who Are You*, 2019.

[50] S. Das, B. Wang, and L. J. Camp, "Mfa is a waste of time! understanding negative connotation towards mfa applications via user generated content," in *Proceedings of the Thriteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[51] B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo, "Quantum key distribution and quantum authentication based on entangled state," *Physics letters A*, vol. 281, no. 2-3, pp. 83–87, 2001.

[52] C. Portmann, "Quantum authentication with key recycling," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2017, pp. 339–368.

[53] L. Liao, X. Peng, J. Shi, and Y. Guo, "Graph state-based quantum authentication scheme," *International Journal of Modern Physics B*, vol. 31, no. 9, p. 1750067, 2017.

[54] D. Ljunggren, M. Bourennane, and A. Karlsson, "Authority-based user authentication and quantum key distribution," *Quantum Communication, Computing, And Measurement 3*, pp. 299–302, 2001, query date: 2019-09-11 21:27:02.

[55] F. Guo and Q. Wen, "Authentication in quantum key distribution," *Journal of Beijing University of Posts and Telecommunications*, vol. 26, pp. 54–56, 2003.

[56] B. Zhao, B. Liu, C. Wu, W. Yu, J. Su, I. You, and F. Palmieri, "A novel ntt-based authentication scheme for 10-ghz quantum key distribution systems," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 8, pp. 5101–5108, 2016.

[57] C. Zhou, W.-S. Bao, H.-W. Li, Y. Wang, and X.-Q. Fu, "Key-leakage evaluation of authentication in quantum key distribution with finite resources," *Quantum information processing*, vol. 13, no. 4, pp. 935–955, 2014.

[58] H. Crawford and S. Atkin, "Quantum authentication: Current and future research directions."

[59] H. M. Waseem and M. Khan, "Information confidentiality using quantum spinning, rotation and finite state machine," *International Journal of Theoretical Physics*, vol. 57, no. 11, pp. 3584–3594, 2018.

[60] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing." *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.

[61] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* IEEE, 2002, pp. 449–458.

[62] R. Gennaro and P. Rohatgi, "How to sign digital streams," in *Annual International Cryptology Conference*. Springer, 1997, pp. 180–197.

[63] M. Bellare, R. Canetti, and H. Krawczyk, "Message authentication using hash functions: The hmac construction," *RSA Laboratories CryptoBytes*, vol. 2, no. 1, pp. 12–15, 1996.

[64] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, p. 076001, 2013.

[65] R. Majumdar, S. Basu, P. Mukhopadhyay, and S. Sur-Kolay, "Error tracing in linear and concatenated quantum circuits," *arXiv preprint arXiv:1612.08044*, 2016.

[66] R. Majumdar, S. Basu, and S. Sur-Kolay, "A method to reduce resources for quantum error correction," in *International Conference on Reversible Computation*. Springer, 2017, pp. 151–161.

[67] R. Majumdar, S. Basu, S. Ghosh, and S. Sur-Kolay, "Quantum error-correcting code for ternary logic," *Physical Review A*, vol. 97, no. 5, p. 052302, 2018.

[68] C. Gong, H. Tang, and D. Zhang, "Ident-ity authentication and key distribution protocol based on quantum one-way function," *Computer Engineering*, vol. 38, no. 6, pp. 161–160, 2012.

[69] Y. Gorbenko, I. Svatovskiy, O. Shevtsov, and IEEE, "Post-quantum message authentication cryptography based on error-correcting codes," *2016 Third International Scientific-Practical Conference Problems Of Infocommunications Science And Technology (Pic S&T)*, pp. 51–54, 2016.

[70] S. Rass, S. König, S. Schauer, and O. Maurhart, "Implementation and evaluation of intrinsic authentication in quantum key distribution protocols," *International Journal on Advances in Security Volume 9, Number 1 & 2, 2016*, 2016.

[71] X. Tan and L. Jiang, "Identity authentication by entanglement swapping in controlled quantum teleportation," *International Journal of Embedded Systems 4*, vol. 6, no. 1, pp. 3–13, 2014.

[72] H. Lai, J. Xiao, M. A. Orgun, L. Xue, and J. Pieprzyk, "Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes," *Quantum information processing*, vol. 13, no. 4, pp. 895–907, 2014.

[73] M. Sobota, A. Kapczyński, and A. Banasik, "Application of quantum cryptography protocols in authentication process," in *Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, vol. 2. IEEE, 2011, pp. 799–802.

[74] R. Gelfond and A. Berzanskis, "Key management and user authentication for quantum cryptography networks," Dec. 25 2012, uS Patent 8,340,298.

[75] L. Min and Y. Li, "Public-key encryption and authentication of quantum information," *Science China-Physics Mechanics & Astronomy*, vol. 55, no. 9, pp. 1618–1629, 2012.

[76] M. Peev, M. Nölle, O. Maurhardt, T. Lorünser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, and A. Zeilinger, "A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography," *International Journal of Quantum Information*, vol. 3, no. 01, pp. 225–231, 2005.

[77] A. Abidin and J. Larsson, "Security of authentication with a fixed key in quantum key distribution," *arXiv preprint arXiv:1109.5168*, 2011.

[78] W. Jian, Z. Quan, and T. Chao-Jing, "Multiparty simultaneous quantum identity authentication based on entanglement swapping," *Chinese Physics Letters*, vol. 23, no. 9, p. 2360, 2006.

[79] N. Li, J. Li, L.-L. Li, Z. Wang, and T. Wang, "Deterministic secure quantum communication and authentication protocol based on extended ghz-w state and quantum one-time pad," *International Journal Of Theoretical Physics*, vol. 55, no. 8, pp. 3579–3587, 2016.

[80] S. Rass, S. Konig, and S. Schauer, "Bb84 quantum key distribution with intrinsic authentication," *ICQNM*, 2015.

[81] S. Rass, P. Schartner, and M. Greiler, "Quantum coin-flipping-based authentication," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.

[82] B. Skoric, *Quantum readout of physical unclonable functions: Remote authentication without trusted readers and authenticated quantum key exchange without initial shared secrets*. IACR, 2009.

[83] A. Amerimehr and M. H. Dehkordi, "Impersonation attack on a quantum secure direct communication and authentication protocol with improvement," *Applied Physics B*, vol. 124, no. 3, p. 44, 2018.

[84] A. Neish, T. Walter, and P. Enge, "Quantum-resistant authentication algorithms for satellite-based augmentation systems," *Navigation-Journal Of The Institute Of Navigation*, vol. 66, no. 1, pp. 199–209, 2019.

[85] P. Hayden, D. W. Leung, and D. Mayers, "The universal composable security of quantum message authentication with key recyling," *arXiv preprint arXiv:1610.09434*, 2016.

[86] M. Naseri, M. A. Raji, M. R. Hantehzadeh, A. Farouk, A. Boochani, and S. Solaymani, "A scheme for secure quantum communication network with authentication using ghz-like states and cluster states controlled teleportation," *Quantum Information Processing*, vol. 14, no. 11, pp. 4279–4295, 2015.

[87] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states," *Physical review letters*, vol. 69, no. 20, p. 2881, 1992.

[88] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[89] Y. CHEN and X. YUN, "Quantum identity authentication with zero knowledge," *lk.hfcas.ac.cn*, 2014.

[90] D. Shen, W. Ma, X. Yin, and X. Li, "Quantum dialogue with authentication based on bell states," *International Journal Of Theoretical Physics*, vol. 52, no. 6, pp. 1825–1835, 2013.

[91] A. Yamamura and H. Ishizuka, "Error detection and authentication in quantum key distribution," *Conference on Information Security and Privacy*, 2001.

[92] T. H. Lin and T. Hwang, "Man-in-the-middle attack on quantum secure communications with authentication," *Quantum Information Processing*, vol. 13, no. 4, pp. 917–923, 2014.

[93] A. Kapczynski and M. Sobota, "Distributed authentication systems enhanced by quantum protocols," in *Fifth International Conference on Information Technology: New Generations (itng 2008)*. IEEE, 2008, pp. 928–931.

[94] A. Ghilen, M. Azizi, R. Bouallegue, and H. Belmabrouk, "Quantum authentication based on entangled states," in *Proc. of World Cong. on Multimedia and Computer Science*. Citeseer, 2013, pp. 75–78.

[95] X. Xin, X. Hua, J. Song, and F. Li, "Quantum authentication protocol for classical messages based on bell states and hash function," *International Journal Of Security And Its Applications*, vol. 9, no. 7, pp. 285–291, 2015.

[96] Y. Chang, S. Zhang, L. Yan, and J. Li, "Deterministic secure quantum communication and authentication protocol based on three-particle w state and quantum one-time pad," *Chinese science bulletin*, vol. 59, no. 23, pp. 2835–2840, 2014.

[97] E. Guedes and F. de Assis, "An approach to evaluate quantum authentication protocols," *elloaguedes.com*, 2011.

[98] T.-S. Wei, C.-W. Tsai, and T. Hwang, "Comment on "quantum key distribution and quantum authentication based on entangled state"," *International Journal Of Theoretical Physics*, vol. 50, no. 9, pp. 2703–2707, 2011.

[99] A. Farouk, J. Batle, M. Elhoseny, M. Naseri, M. Lone, A. Fedorov, M. Alkhambashi, S. H. Ahmed, and M. Abdel-Aty, "Robust general n user authentication scheme in a centralized quantum communication network via generalized ghz states," *Frontiers Of Physics*, vol. 13, no. 2, 2018.

[100] G. Alagic and C. Majenz, "Quantum non-malleability and authentication," *Annual International Cryptology Conference*, 2017.

[101] C.-H. Chien, T.-S. Lin, T.-H. Chang, S.-Y. Yuan, and S.-Y. Kuo, "Quantum authentication protocol using entanglement swapping," in *2011 11th IEEE International Conference on Nanotechnology*. IEEE, 2011, pp. 1533–1537.

[102] P. PAN and H. LUO, "Quantum key swapping scheme and authentication based on teleportation," *Journal of Guizhou University (Natural Sciences)*, 2012.

[103] M. Alshowkan and K. Elleithy, "Quantum mutual authentication scheme based on bell state measurement," in *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2016, pp. 1–6.

[104] V. Padmavathi, M. Madhavi, and N. Nagalakshmi, "An approach to secure authentication protocol with group signature based quantum cryptography," *Int. J. Innov. Technol. Explor. Eng*, vol. 2, no. 2, pp. 105–107, 2013.

[105] Y. Yu-Guang and W. Qiao-Yan, "Economical multiparty simultaneous quantum identity authentication based on greenberger–horne–zeilinger states," *Chinese Physics B*, vol. 18, no. 8, p. 3233, 2009.

[106] M. Bae, J.-S. Kang, and Y. Yeom, "A study on the one-to-many authentication scheme for cryptosystem based on quantum key distribution," in *2017 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 2017, pp. 1–4.

[107] K. A. Al-Khateeb, M. M. Saeb, M. M. A. Majeed, and M. R. Wahiddin, "A secure protocol using 6dp for quantum authentication and hash functions for key distribution (kdp-6dp)," in *International Conference on Computer and Communication Engineering (ICCCE'10)*. IEEE, 2010, pp. 1–4.

[108] S. Fehr and L. Salvail, "Quantum authentication and encryption with key recycling," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2017, pp. 311–338.

[109] Y. Yu-Guang, " key laboratory for modern communication, chengdu 610041, china); a theoretical scheme for multi-user quantum authentication and key distribution in ," *Acta Physica Sinica*, 2005.

[110] M. Elboukhari, A. Azizi, and M. Azizi, "Integration of quantum key distribution in eap-tls protocol used for wireless lan authentication," in *2010 5th International Symposium On I/V Communications and Mobile Network*. IEEE, 2010, pp. 1–4.

[111] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[112] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[113] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, no. 3, p. 648, 1999.

[114] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Physical Review A*, vol. 69, no. 5, p. 052307, 2004.

[115] Z.-j. Zhang, Y. Li, and Z.-x. Man, "Multiparty quantum secret sharing," *Physical Review A*, vol. 71, no. 4, p. 044301, 2005.

[116] G.-P. Guo and G.-C. Guo, "Quantum secret sharing without entanglement," *Physics Letters A*, vol. 310, no. 4, pp. 247–251, 2003.

[117] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A*, vol. 59, no. 1, p. 162, 1999.

[118] D. Gottesman, "Theory of quantum secret sharing," *Physical Review A*, vol. 61, no. 4, p. 042311, 2000.

[119] T. Wei, T. Hwang, and C. Tsai, "Quantum secret authentication code," *arXiv preprint arXiv:1108.3500*, 2011.

[120] A. Buhari, Z. A. Zukarnain, S. K. Subramaniam, H. Zainuddin, and S. Saharudin, "A quantum based challenge-response user authentication scheme over noiseless channel," *International Journal of Network Security & Its Applications*, vol. 4, no. 6, p. 67, 2012.

[121] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-to-Peer Networking and applications*, 2018. [Online]. Available: https://link.springer.com/article/10.1007/s12083-016-0528-2

[122] B. B. Elliott, "Authentication in a quantum cryptographic system," Apr. 15 2008, uS Patent 7,359,512.

[123] D. CAO and Y.-l. SONG, "Quantum fuzzy commitment and biometric authentication scheme based on entanglement-assisted quantum error-correcting codes," *Acta Electronica Sinica*, no. 7, p. 34, 2012.

[124] A. M. Childs, "Secure assisted quantum computation," *arXiv preprint quant-ph/0111046*, 2001.

[125] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, 2009, pp. 517–526.

[126] R. Jozsa, "An introduction to measurement based quantum computation," *NATO Science Series, III: Computer and Systems Sciences. Quantum Information Processing-From Theory to Experiment*, vol. 199, pp. 137–158, 2006.

[127] J. F. Fitzsimons, "Private quantum computation: an introduction to blind quantum computing and related protocols," *npj Quantum Information*, vol. 3, no. 1, p. 23, 2017.

[128] Q. Li, Z. Li, W. H. Chan, S. Zhang, and C. Liu, "Blind quantum computation with identity authentication," *Physics Letters A*, vol. 382, no. 14, pp. 938–941, 2018.

[129] G. Alagic, C. Majenz, A. Russell, and F. Song, "Quantum-secure message authentication via blind-unforgeability," *arXiv preprint arXiv:1803.03761*, 2018.

[130] C. Yan, Z. Shi-Bin, Y. Li-Li, and H. Gui-Hua, "Robust quantum secure direct communication and authentication protocol against decoherence noise based on six-qubit df state," *Chinese Physics B*, vol. 24, no. 5, 2015.

[131] C.-h. JIN, Z.-y. LI, and S.-h. LIAO, "A simple deniable authentication protocol based on quantum key distribution," in *International Conference on Computer Networks and Communication Technology (CNCT 2016)*. Atlantis Press, 2016.

[132] N. Li, X. Zha, and Q. Lan, "Secure quantum report with authentication based on six-particle cluster state and entanglement swapping," *Science China Information Sciences*, 2012.

[133] S. Garg, H. Yuen, and M. Zhandry, "New security notions and feasibility results for authentication of quantum data," in *Annual International Cryptology Conference*. Springer, 2017, pp. 342–371.

[134] Y.-G. Yang, Q.-Y. Wen, and F.-C. Zhu, "A theoretical scheme for multi-user quantum authentication and key distribution in a network," *Acta Physica Sinica*, vol. 54, no. 9, pp. 3995–3999, 2005.

[135] H. Zhu, "A simple and secure non-interactive deniable authentication scheme with privacy protection using quantum bits," *Ł*, vol. 29, no. 3, pp. 83–93, 2018.

[136] S. Bakhtiari Chehelcheshmeh and M. Hosseinzadeh, "Quantum-resistance authentication in centralized cognitive radio networks," *Security and Communication Networks*, vol. 9, no. 10, pp. 1158–1172, 2016.

[137] H. Cao and W. Ma, "Comment on a novel quantum deniable authentication protocol without entanglement," *Quantum Information Processing*, vol. 17, no. 11, p. 289, 2018.

[138] S. JI, Z. TAN, X.-p. SUN, and J. LUO, "A quantum identity authentication protocol based on polarization rotation," *Chinese Jourany of Quantum Electronics*, vol. 27, no. 1, pp. 40–45, 2010.

[139] A. Sharma and S. Lenka, "Authentication in online banking systems through quantum cryptography," *Int. J. Engineering and Technology*, 2013.

[140] R. J. Hughes, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, R. T. Newell, K. P. McCabe, N. Dallmann *et al.*, "Streaming authentication and multi-level security for communications networks using quantum cryptography," Aug. 25 2016.

[141] P. Basuchowdhuri, "Classical authentication aided three-stage quantum protocol," *arXiv preprint cs/0605083*, 2006.

[142] Y. Dong, S. Xiao, H. Ma, and L. Chen, "Research on quantum authentication methods for the secure access control among three elements of cloud computing," *International Journal of Theoretical Physics*, 2016.

[143] L. Gyongyosi and S. Imre, "Novel quantum information solution to copy-protection and secured authentication," *International Journal of Internet Technology and Secured Transactions*, vol. 3, no. 1, pp. 40–62, 2011.

[144] ——, "A quantum copy-protection scheme with authentication," *arXiv preprint arXiv:1207.4462*, 2012.

[145] B. C. Jacobs, "Embedded authentication protocol for quantum key distribution systems," Apr. 8 2014, uS Patent 8,693,691.

[146] X. Xin and F. Li, "Quantum authentication of classical messages without entangled state as authentication key," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 8, pp. 199–206, 2015.

[147] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[148] M. S. Azevedo, R. A. Medeiros, R. C. Freire, and F. M. de Assis, "Comments on the security of a hybrid quantum-classical authentication protocol." *researchgate.net*, 2006.

[149] T. Thangavel, *Hash based quantum key two server password authentication for internet system*. Chennai, 2014, query date: 2019-09-11 21:14:19.

[150] G. Fei, Q. Su-Juan, G. Fen-Zhuo, and W. Qiao-Yan, "Cryptanalysis of quantum secure direct communication and authentication scheme via bell states," *Chinese Physics Letters*, vol. 28, no. 2, 2011.

[151] A. Buhari, Z. A. Zukarnain, S. K. Subramaniam, H. Zainuddin, and S. Saharudin, "A single photon quantum user bi-directional authentication scheme over noiseless channel," in *2012 IEEE Symposium on Industrial Electronics and Applications*. IEEE, 2012, pp. 1–6.

[152] M. Oya, N. Namekata, J. Nishikawa, and S. Inoue, "Quantum secure authentication system experiment using adaptive optics," in *Conference on Lasers and Electro-Optics/Pacific Rim*. Optical Society of America, 2017, p. s1938.

[153] R. Devi, R. Balaguru, R. Amirtharajan, and ..., "A novel quantum encryption and authentication framework integrated with iot," *Security, Privacy and* , 2019.

[154] G. Murali, R. S. Prasad, and K. B. Rao, "Effective user authentication using quantum key distribution for wireless mesh network," *International Journal of Computer Applications*, vol. 42, no. 4, pp. 7–12, 2012.

[155] T. Akila and P. UmaMaheswari, *MPQC: Secure Authentication for Message Passing Via Quantum Cryptography*. pdfs.semanticscholar.org, 2016.

[156] B. Lari, "Quantum authentication protocols for gsm," *arXiv preprint arXiv:1812.02081*, 2018.

[157] L. Zhi-Hao, C. Han-Wu, and L. Wen-Jie, "Information leakage problem in high-capacity quantum secure communication with authentication using einsteinpodolskyrosen pairs," *Chinese Physics Letters*, 2016.

[158] G. Yang, M. Nie, and W. Yang, "Quantum authentication and key agreement scheme for sip protocol," *Journal of Sichuan University (Natural Science Edition)*, 2016.

[159] R. Khalid, Z. A. Zukarnain, Z. M. Hanapi, and M. A. Mohamed, "Authentication mechanism for cloud network and its fitness with quantum key distribution protocol: A survey." *Journal of Theoretical & Applied Information Technology*, vol. 81, no. 1, 2015.

[160] E. Kiktenko, A. Malyshev, M. Gavreev, A. Bozhedarov, N. Pozhar, M. Anufriev, and A. Fedorov, "Lightweight authentication for quantum key distribution," *arXiv preprint arXiv:1903.10237*, 2019.

[161] G. Murali, R. Prasad, and V. Madhavi, "Effective key authentication for ieee 802.11 networks using quantum cryptography," *International Journal of Computer* , 2012.

[162] G. Guo, C. Li, and G. Guo, "Quantum non-demolition measurement of nonlocal variables and its application in quantum authentication," *Physics Letters A*, vol. 286, no. 6, pp. 401–404, 2001, query date: 2019-09-11 21:27:02.

[163] D. fen Li, R. jin Wang, Y. ming Yang, and J. lian Chen, "Authentication of quantum secure communication under noise," *International Journal Of Theoretical Physics*, vol. 58, no. 4, pp. 1079–1087, 2019.

[164] D. Zhu, X. Li, X. Li, R. Wei, J. Wu, and L. Song, "A quantum identity authentication protocol based on optical transmission & face recognition." *International Journal of Online Engineering*, vol. 14, no. 4, 2018.

[165] M. Schuld, R. Sweke, and J. J. Meyer, "Effect of data encoding on the expressive power of variational quantum-machine-learning models," *Physical Review A*, vol. 103, no. 3, p. 032430, 2021.

[166] G. S. Oreku and J. Li, "End user authentication (eua) model and password for security," *Journal of Organizational and End User Computing (JOEUC)*, vol. 21, no. 2, pp. 28–43, 2009.

[167] S. Chiasson, A. Forget, R. Biddle, and P. C. Van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, no. 6, p. 387, 2009.