

# A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice?

Arindam Dutta<sup>1,§</sup> and Anirban Pathak<sup>1,\*</sup>

<sup>1</sup>Jaypee Institute of Information Technology, A 10, Sector 62, Noida, UP-201309,  
India

<sup>§</sup>arindamsalt@gmail.com

<sup>\*</sup>anirban.pathak@gmail.com

## Abstract

Secure communication has achieved a new dimension with the advent of the schemes of quantum key distribution (QKD) as in contrast to classical cryptography, quantum cryptography can provide unconditional security. However, a successful implementation of a scheme of QKD requires identity authentication as a prerequisite. A security loophole in the identity authentication scheme may lead to the vulnerability of the entire secure communication scheme. Consequently, identity authentication is extremely important and in the last three decades several schemes for identity authentication, using quantum resources have been proposed. The chronological development of these protocols, which are now referred to as quantum identity authentication (QIA) protocols, are briefly reviewed here with specific attention to the causal connection involved in their development. The existing protocols are classified on the basis of the required quantum resources and their relative merits and demerits are analyzed. Further, in the process of the classification of the protocols for QIA, it's observed that the existing protocols can also be classified in a few groups based on the [inherent computational tasks used to design the protocols. Realization of these symmetries has led to the possibility of designing a set of new protocols for quantum identity authentication, which are based on the existing schemes of the secure computational and communication tasks. The security of such protocols is also critically analyzed.

## 1 Introduction

Authentication or identity authentication is a systematic procedure of validating the identity of the legitimate users and/or components/devices. This process helps us to circumvent various kinds of attacks on the schemes for secure computation and communication. The relevance of the schemes of identity authentication has been considerably increased in the recent past with the enhanced use of online banking, e-commerce, internet of things (IoT), online voting, etc. All these applications, and many others essentially require identity authentication. For example, IoT primarily requires authentication of the devices or components, whereas online voting requires authentication of the users (voters). From the perspective of cryptography, there is not much difference between a user and a component, and in what follows, we will treat them as equivalent.

In a two party scenario, authentication may be visualized as a procedure that allows a legitimate user (sender) Alice to transmit a message  $X$  (equivalently a key in case of key distribution schemes)

to a second user Bob (receiver) in such a way that Bob can be assured that the data was not corrupted during transmission through the channel [1]. In other words, it can be viewed as a procedure that certifies the identity of the creator of the message  $X$  and establishes the integrity of the message received by Bob. This is closely related to digital signature, which would allow a third party (Charlie) to verify at a later time that Bob has not modified the message  $X$  sent to him by Alice [1]. Authentication and digital signature are closely related but different tasks, and in the present review, we will restrict ourselves to the schemes for authentication only. More precisely, this review will be restricted to the schemes of authentication, which uses quantum resources, i.e., schemes for quantum identity authentication (QIA). To appreciate the relevance and importance of QIA schemes, we first need to briefly discuss the development of quantum cryptography which had historically transformed the notion of security.

The first ever protocol of quantum key distribution was proposed by Bennett and Brassard in 1984 [2] which is now known as BB84 protocol<sup>1</sup>. The claim that this protocol can provide unconditional security which is a desired facet not achievable by classical schemes of key distribution where security arises from the complexity of a mathematical task drew considerable attention of the cryptographic community. This led to a set of interesting protocols of quantum key distribution (QKD) including E91 [5] and B92 [6] protocols for QKD. The need for the identity authentication of the legitimate users were recognized in these works as we can see that even in the classic BB84 paper Bennett and Brassard wrote, “The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if the Alice and Bob have agreed beforehand on a small secret key, which they use to create Wegman-Carter authentication tags [7] for their messages over the public channel”. However, as no quantum identity authentication protocol was available prior to 1995, classical schemes for identity authentication, like Wegman-Carter scheme was intrinsically considered in the early schemes for QKD, although it was not always explicitly spelled out. In all such schemes and also the schemes for authentication developed later, “pre-shared small key” mentioned above plays a crucial and essential role<sup>2</sup>. This point will be further clarified in the later part of this paper. The use of Wegman-Carter scheme or a similar scheme in the early protocols of QKD was a natural consequence of the fact that no real channel can be strictly considered as faithful. Specifically, an eavesdropper (Eve) can replace a channel between the sender (Alice) and the receiver (Bob) by two channels, one from Alice to Eve and other from Eve to Bob. In such a scenario that can separate Alice and Bob, Eve will be able to create a key with Alice and another with Bob. The need to circumvent such a scenario makes it essential to use a protocol for identity authentication.

Now, as the security of the classical authentication schemes are also based on the complexity of the computational task(s) involved, authentication using classical resources cannot be done in an unconditionally secure manner, and consequently it may lead to a security loop-hole(s) into the so called unconditionally secure quantum key distribution schemes. Thus, to obtain a really unconditional secure scheme of quantum key distribution, one would require an unconditional security for the authentication scheme, too, and that in turn would need to use quantum resources. Such a scheme of identity authentication, which uses quantum resources is generally referred to as a quantum identity authentication (QIA) scheme. First such scheme was proposed by Crépeau et al. [8] in 1995, and it was followed by a large number of schemes. For example, before the flooding of schemes for QIA, in 1998, Zeng et al. proposed a QKD protocol [9] that allowed the simultaneous distribution of the key and the verification of the communicator’s identity and almost immediately after that in 1999, Dušek et al. [10] proposed two protocols for QIA. The protocols were hybrid (in the strict

---

<sup>1</sup>Of course, the origin of quantum cryptography owes a lot to the pioneering work of Wiesner [3]. For a beautiful description of the related history see [4].

<sup>2</sup>In fact, all the protocols of QKD can be viewed as key amplification protocols as every QKD protocol starts with a pre-shared small key used for authentication and creates a longer key in a particular session, and subsequently uses a small part of the longer key as the pre-shared small key in the next session.

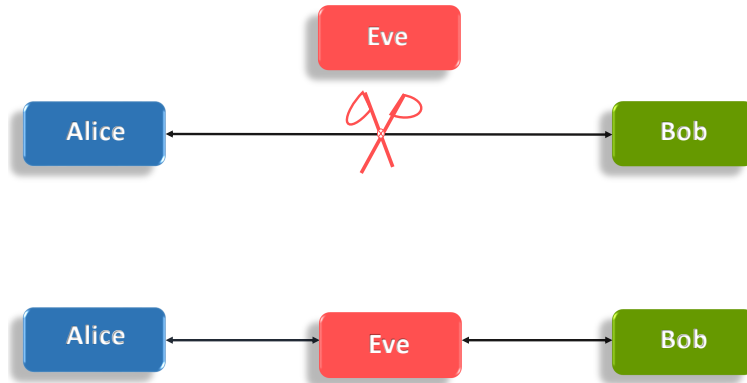


Figure 1: (Color online) Eve may try to impersonate Alice (Bob) in front of Bob (Alice), by replacing the channel between Alice and Bob with two channels- one from Alice to Eve and another from Eve to Bob.

sense, this is apparently the case with all the schemes proposed till date) in the sense that they were proposed using an amalgamation of classical authentication schemes and protocols for QKD with a specific stress on one time pad. The sequence continued and a large number of protocols having individual advantages and disadvantages appeared [11–18]. Considering the importance of secure quantum computation and communication protocols, and the crucial role of authentication in those protocols, here we aim to systematically review the protocols for QIA.

The rest of the paper is organized as follows. In Section 2, we have provided a short chronological history of the development of the schemes for QIA with specific attention to some schemes which are distinct in their characteristics. In Section 3.1 and Section 3.2, we have classified the existing schemes for QIA based on the resources and computational/communication tasks used to implement a scheme, respectively. Subsequently, a set of new protocols are proposed in Section 4; and in Section 4.1, the proposed protocols and the existing protocols are compared. The limitations of the particular classes of protocols are also highlighted. The security of the proposed protocols are analyzed in Section 5. Finally, the paper is concluded in Section 6.

## 2 A short chronological history of the protocols for quantum identity authentication

We have already mentioned in Section 1, that classical authentication scheme, like Wegman-Carter scheme, was used in the early protocols for QKD. Such message authentication schemes can lucidly be described as schemes composed of two phases. In the first phase, functions which produce identity authentication are cleverly utilized and in the second phase, the authenticity of a message is verified. Classically functions, like message encryption, message authentication code (MAC) and Hash functions are commonly used for authentication. Although, it's not our focus to discuss classical authentication schemes, we can briefly and lucidly mention some relevant ideas before we provide a chronological history of QIA. Such a short discussion on classical tricks is justified, as hybrid and completely classical schemes are still used in various schemes for secure quantum communication and computation. Further, some of the classical tricks of authentication can be easily extended to design the schemes for QIA. Let's first establish the point that classical tricks can be extended to designing of QIA through an example. Consider a pre-shared key  $x_1, x_2, \dots, x_n$  between Alice and Bob, where  $x_i \in \{0, 1\}$ , now Alice can use half of this as a message (say all the odd bits) and other half as key

(say all the even bits) and create a new sequence of length  $\lceil \frac{n}{2} \rceil$  such that  $i$ th bit of the new sequence is  $x_{2i-1} \oplus x_{2i}$ . This can be viewed as a Tag or equivalently a crypt. Alice can send it in a conventional manner and Bob can use the same key  $\{x_{2i}\}$  to decode it. Capability of communicating a message ensures the capability of communicating a Tag. So every scheme of quantum secure direct communication (QSDC) [19], quantum dialogue (QD) [20], deterministic secure quantum communication (DSQC) [21] can perform this task. In other words, the above classical trick can be extended easily to form simple minded schemes for QIA using different protocols for QSDC, DSQC and QD. Further, we may note that in the MAC technique, both parties share a common secret key  $K$ . When Alice wants to send a message to Bob, she calculates the MAC as a function of the message and the key, and sends the message and MAC to Bob. Subsequently, Bob calculates the MAC information in the same manner and compares that with the received MAC. If it matches, the receiver confirms the authenticity and also the integrity of the message. A hash function is a variation of MAC, which takes variable size of messages as input and produces a fixed-size of output referred to as hash code. Hash function has a one-way property and consequently, it's useful to produce a fingerprint of a message.

Now, it's important to note that no-cloning theorem which states that an unknown quantum state cannot be copied with unit fidelity and the collapse on measurement property of quantum states plays a crucial role in establishing advantages of the schemes for QIA over their classical counterparts. To visualize this let us consider a situation, where Eve trespasses into Alice's house in her absence and makes a copy of her authentication key without leaving any trace. In a classical scenario, this will allow Eve to pose as Alice and communicate with Bob without being detected. However, due to no-cloning theorem such a situation would not arise in the quantum world, if the authentication key is encoded and stored in a quantum state. Further, due to collapse on measurement principle, any eavesdropping efforts leave detectable traces in the schemes of quantum cryptography. This sets the motivation for designing protocols for QIA.

As mentioned in the previous section, first ever protocol for QIA was proposed by Crépeau et al. [8] in 1995, it was based on a scheme of oblivious transfer (OT) which is a cryptographic primitive. Interestingly, an extremely strong result by Lo and Chau [22] established the impossibility of an unconditionally secure two-party OT. The pioneering effort of Crépeau et al. [8] was followed by a set of early works [9, 10, 23] on QIA which are briefly mentioned in the previous section, but not much activity related to quantum or hybrid identity authentication happened in the previous century. This situation changed considerably in the present century. In the remaining part of this section, we will try to provide a chronological history of the development of different protocols. As the literature is vast, efforts will not be made to include all works<sup>3</sup>. However, the representative works mentioned here are expected to provide a clear picture of the evolution of the schemes of quantum and hybrid identity authentication. It's also expected to put light on the fact that the different type of QKD schemes and other protocols of cryptographic tasks, like continuous variable (CV) QKD (CV-QKD), discrete variable (DV) QKD (DV-QKD), counterfactual QKD, semi-QKD, etc., require different types of QIA schemes to ensure that the same resources/devices can be used for performing the communication task as well as the authentication task. Actually, applicability of earlier protocols of QIA were primarily restricted to conventional conjugate coding based on DV cryptographic schemes, but later the domain of applicability has been considerably enhanced.

**2000:** It was a very active year, and many (at least 10) new protocols for QIA appeared. Most of them (all except 3 protocols of Ljunggren et al. [25]) were Bell state based. Specifically, Zeng et al. proposed a Bell-state based scheme for QIA [26] in early 2000. A few months later, Zhang et al. proposed another Bell state based protocol for QIA [13], where a pre-shared Bell state is used

---

<sup>3</sup>For a complete list of papers published in the domain of quantum authentication between 2009-2019, interested readers may see [24]. We came across this brief literature review work after completion of this review. Interestingly, classification of QIA schemes made in [24] is consistent with the classification made in this work.

as the pre-shared secret or equivalently as the authentication key. In between the introduction of these two Bell state based schemes, Jensen et al., [27] proposed a bi-partite entangled state based protocol for QIA<sup>4</sup> and claimed that their protocol is secure even when Eve possesses complete control over the classical and quantum channels. This work was a generalization of 1999 work of Barnum [23] and it was also interesting because it listed a set of open questions. Ljunggren et al. proposed a set of 5 protocols for authenticated QKD [25] between two parties Alice and Bob. In their protocols a third party, Trent was introduced as arbitrator. Three of the protocols were single-photon [24] based and the others were based on Bell states. Interestingly, one of the entangled-state based protocols was analogous to B92 protocol and the symmetry observed between schemes of QKD and QIA reflected in that protocol allows us to think of transforming other schemes of QKD into schemes for QIA or authenticated QKD. Further, here the role of Trent is analogous to the role of controller in cryptographic switch [28, 29], and following the result of [28, 29], one can easily generalize the three-party protocols of Ljunggren et al.

**2001:** In an interesting work, Curty et al., proposed an optimal scheme for quantum authentication of a classical message (CS01 protocol hereafter ) [30]. It was optimal in the sense that it allowed authenticated transmission of a two-bit classical message using a one qubit authentication key (which can be viewed as an optimal pre-shared secret). Interestingly, they classified the possible attacks on the authentication schemes as: (i) no-message attack and (ii) message attack. In CS01 scheme and many other schemes of message authentication, perfect deterministic decoding of the classical message happens. This implies that a protocol fails if and only if Bob accepts an unauthenticated message as authenticated one. Curty et al. argued that the same may happen in two different ways leading to two families of attacks. Specifically, in no-message attack, Eve prepares a quantum state prior to the transmission of a message from Alice and sends that to Bob aiming to pass the decoding algorithm of Bob with certain probability  $p_f$ . This is referred to as no-message attack, as it works in a situation where the legitimate user Alice has not yet send a message. In contrast, in a message attack, Eve intercepts the message sent by Alice and tries to obtain information from that. Subsequently, she prepares a fake message using the information obtained by interception and tries to pass the decoding algorithm of Bob. This classification of attacks helped security analysis of the subsequently developed schemes, but in the security analysis performed in [30] and in a large number of subsequent papers, a noiseless quantum channel has been considered which is an idealization and does not correspond to the practical situations.

**2002:** In CS01 protocol, a classical message was authenticated with the optimal amount of quantum resources. However, that naturally led to an interesting question like: How to authenticate a quantum message with a quantum key? Can a qubit (which can be viewed as a quantum message of minimum size) be authenticated using another qubit (which can be viewed as pre-shared quantum secret of minimum size)? These questions were addressed in Ref. [31], where Curty et al. established that a no-go theorem which can be stated as: A qubit cannot be authenticated with just another qubit.

T. Mihara proposed schemes for QIA and message authentication [18] using pre-shared entanglement. The QIA scheme proposed by them had a trusted third party, while the message authentication scheme was hybrid in nature as they used quantum resources along with Hash function. Here, it may be noted that the approach adopted by them in designing a message authentication scheme can be generalized easily and every known scheme of QSDC can be used

---

<sup>4</sup>It was not specifically mentioned that the particles are maximally entangled, but without affecting any result, we can consider this as a Bell state based scheme for QIA.

to design similar protocols. Interestingly, it was soon established that this scheme uses quantum correlations but doesn't exploit them and in principle the same task can be performed by classically correlated states [32]. Further, quantum part in the identity authentication scheme of Mihara [18] is vulnerable. To be precise, during entanglement distribution process (cf. Step 2-3, of Section entitled "Identifying Alice to Bob" in Ref. [18]) neither BB84 subroutine nor GV subroutine [33] is used and all the subsequent measurements are performed using computational basis, consequently it's vulnerable under man-in-the-middle attack. Of course, one can circumvent this possibility using decoy qubits implementing one of the above mentioned subroutines, as is routinely done in the schemes of QSDC (for example, one may see the description of ping-pong protocol in Ref. [34]).

**2004:** Li et al. proposed a scheme of QIA that uses Bell states [11]. Specifically, a Bell state is pre-shared by Alice and Bob as identification token. Subsequently, during the authentication process, Alice creates another auxiliary Bell state to interact with the "identification token" and sends the auxiliary information to Bob, who performs some operations before performing Bell measurement to complete the authentication procedure. As before, this Bell state based scheme too does not exploit the nonlocal properties of Bell states. Specifically, Bell inequality violation as a quantum resource is not used for designing schemes for QIA.

**2005:** Zhou et al. proposed a scheme of QIA using quantum teleportation and quantum entanglement swapping [35]. This scheme claimed to resolve the limitations of simple point-to-point QIA schemes as entanglement swapping can be used to extend the distance over which authentication can be done. This is a known trick and frequently used in QKD to circumvent the limitation on allowed distance that arise from the presence of noise and unavailability of quantum repeater. However, such an approach often leads to a new security concern as the device deployed in the middle to initiate entanglement swapping needs to be trusted.

A way to compute efficiency of a scheme of authentication is to compare how much pre-shared information it consumes during the authentication process. The less it consumes, the more efficient is the scheme. In view of this measure, an efficient QIA scheme was proposed by Peev et al. [36].

**2006:** Lee et al. proposed two quantum direct communication protocols with user authentication [37]. Here Alice can directly communicate a secret message to Bob without any pre-shared secret. The protocols are constructed in two parts: one part is dedicated for authentication and the other part is used for direct communication. They introduced a third party, Trent as more powerful than the other users and enabling him to authenticate the other users participating in the communication scheme by distributing tri-partite "Greenberger-Horne-Zeilinger" (GHZ) states.

Wang et al. proposed an authentication protocol that allows a trusted third party to simultaneously authenticate multiple users with the help of entanglement swapping and GHZ states [12].

Zhang et al. [14] proposed a one-way QIA scheme by using the mechanism of the ping-pong protocol [38] of QSDC. This was a scheme of one-way QIA in the sense that in their work Alice was considered as a reliable *certification authority* (CA) and Bob was considered as the user whose identity needs to be verified when he would try to communicate with Alice. Technically, many of the schemes proposed so far are one-way in this sense. However, usually that's not explicitly mentioned as the capability of one-way authentication implies that two-way authentication can be done by using the same process two times. They showed that their scheme is secure against individual attacks like impersonated fraudulent attack (where Eve is unaware of the authentication key, but impersonates Bob by forging a new qubit) and substitution fraudu-

lent attack (where to impersonate Bob, Eve tries to obtain the authentication key using a new quantum channel and exploiting this channel and the qubits traveling from Bob to Alice). Here it may be noted that message attack and no-message attack are not always specified with these names, but most of the attacks discussed so far can be viewed as message attack or no-message attack.

**2007:** Zhang et al. [39] reported that Lee et al.'s protocol published in 2006 is vulnerable under two types of attack which can be performed by Trent. Zhang et al. also modified the protocol of Lee et al. and proposed an improved protocol, which is free from the limitations of the Lee et al.'s protocol. This type of cryptanalysis showing a vulnerability of a scheme and subsequent development of an improved scheme free from that vulnerability is very common in the field of cryptography, and this may be treated as a representative example, in the context of QIA.

**2009:** Using GHZ states Guang et al. proposed a scheme for simultaneous multiparty QIA [40]. The task performed by the scheme was similar to the task performed by the 2006 protocol of Wang et al. [12]. However, Guang et al.'s scheme was shown to be more efficient compared to the Wang et al.'s scheme in the sense that in comparison to Wang et al.'s scheme lesser quantum resources and lesser quantum operations are needed in Guang et al.'s scheme.

Rass et al. [41] introduced an interesting idea, where the authentication was performed at the end of the QKD scheme instead of the usual practice of performing it in the beginning. To design the scheme, they combined the ideas of QKD and quantum coin-flipping. They also found tight bounds on the amount of pre-shared secrets required for QIA.

**2010:** Dan et al. [42] introduced a simple protocol of QSDC with authentication. The protocol was based on Bell states and the qubits were described as the polarization encoded qubits. Though such specification is not always mentioned in the schemes of authentication, wherever transmission of qubits is involved, it's intrinsically assumed that the qubits used are photonic in nature as the transmon qubits used in superconductivity based quantum computing and other realization of qubits are not easily transferable from one place to the other. Dan et al. also established security of their scheme against a set of typical attacks, e.g., intercept and resend attack, Trojan horse attack and entanglement attack.

**2011:** Huang et al. [43] introduced a Gaussian-modulated squeezed state based CV-QIA protocol. This protocol and similar protocol allow CV-QKD schemes to use CV states for authentication, too. This is important as the use of DV quantum authentication in CV quantum protocols decreases efficiency and increases complexity in the sense that in such a case, devices/resources are required for performing operations and measurements on both CV and DV states.

**2012:** Gong et al. tried to utilize quantum one-way function to design a scheme of QIA involving a trusted third party which was referred to as a trusted server in their work [44].

A US patent (Patent number US 8,340,298 B2) was also given to MagiQ Technologies for a hybrid scheme of QIA in a quantum cryptographic network [45].

Skoric proposed a very interesting idea that combined quantum challenges with classical physical unclonable functions (PUFs). Specifically, the idea was that a classical PUF was challenged using a quantum state. Because of no-cloning theorem and collapse on measurement principle, any eavesdropping effort would lead to detectable trace and a verifier who sends the challenge via a quantum state would be sure about the identity of the prover if he receives the expected quantum state in response of the challenge. Here it may be noted that the idea of PUFs were introduced in the beginning of this century by Pappu et al., [46] as an entity embodied in a specific physical structure which can be easily evaluated but cannot be characterized easily. It

may also be viewed as an entity that cannot be feasibly duplicated because it's manufactured inherently with a large number of uncontrollable degrees of freedom [47]. Interestingly, FPGAs, RFIDs and many other devices can be used to implement PUFs and classical authentication schemes based on PUFs [48]. However, our interest is restricted to PUF based schemes for QIA. In what follows we will observe that interest on such schemes are progressively increasing.

**2013:** Yang et al. proposed two Bell state based schemes of authenticated direct secure quantum communication [49]. The protocols involved a third party, Trent and they were hybrid in nature as Hash functions were also used. The protocol allowed Alice and Bob to authenticate each other with the help of Trent using Bell states in accordance with the user's secret identity sequence and one-way Hash functions  $h_A$  and  $h_B$ .

**2014:** In controlled quantum teleportation, a controller Charlie controls when Alice can teleport a quantum state to Bob [34, 50]. To address the identification confirmation problem associated with controlled teleportation, Tan et al. proposed two identity authentication schemes [51] based on entanglement swapping. The scheme is not efficient as it requires two (three) entanglement swapping operations to confirm the identity of Charlie (Bob) by Alice.

Goorden et al. experimentally realized a scheme for quantum authentication of a physical unclonable key [47]. The key used here was essentially a PUF and classical in nature. It was authenticated by illuminating the PUF with a pulse of light having less number of photons compared to spatial degrees of freedom and a subsequent analysis of the spatial shape of the reflected light.

Shi et al. proposed a quantum deniable authentication protocol based on the property of unitary transformation and quantum one-way function using GHZ state [52]. Their protocol can provide the *completeness* of authentication and *deniability*. Here, completeness of an authentication protocol implies that the aimed receiver can always confirm the authentication of the source of the message if both receiver and sender follow the protocol. In turn, a slight deviation from the conditions of traditional authentication schemes, a deniable authentication scheme ensures that apart from the intended receiver, no one else can identify sources of a given message, and the receiver cannot prove the source of the message to a third party.

Yuan et al. [53] proposed a feasible QIA scheme using a single particle based ping-pong protocol, which is analogous to LM05 [54] protocol of QSDC. This protocol requires a relatively lesser amount of quantum resources and simple-devices.

Fountain codes or rateless erasure codes are the codes having an interesting property that using a set of  $n$  source symbols one can generate a sequence of encoding symbols having  $m > n$  symbols and  $m$  can be as big as needed. Using this property in distributed scenario, i.e., using distributed fountain code, Lai et al. proposed a scheme for QIA [55] in the context of quantum secret sharing.

**2015:** Shi et al. [56] improved their previous work [52] by using a single photon source instead of a GHZ state. The new protocol was more efficient and clearly required lesser amount of quantum resources. It's easy to visualize as creation and maintenance of single photon states are much easier than the same for photonic GHZ states.

**2016:** Ma et al. proposed a teleportation-based CV-QIA protocol [57] using two-mode squeezed vacuum state and coherent state. Interestingly, CV-QKD protocols perform better compared to their discrete variable counterparts in relatively short distances [58]. Consequently, for a metropolitan network, CV-QKD equipped with CV-QIA is expected to provide an efficient solution.

Rass et al. proposed a QIA scheme in connection to BB84 protocol [59]. The novelty of the



scheme was derived from the introduction of a second public channel which was considered to be disjoint from the channel used for implementing the main BB84 scheme.

Security of the PUF based authentication schemes [47, 60] was questioned in Ref. [61] and it was shown that the earlier works (see [62] and references therein) on the security analysis of the PUF based QIA were incomplete in the sense that the earlier works established security against challenge-estimation attacks only, but challenge-estimation attacks can be outperformed by a cloning attack.

The composable security of a QIA scheme was established by Hayden et al. [63]. This was an important step for performing secure quantum communication tasks over a network. Here it will be apt to note that the composable security implies a real protocol implemented should remain  $\epsilon$ -indistinguishable from an ideal protocol for the same task. This allows us to obtain the information theoretic security of the composite scheme as  $\epsilon \leq \epsilon_p + \epsilon_a$ -secure if an  $\epsilon_p$ -secure cryptographic protocol is used with an  $\epsilon_a$ -secure application [64].

**2017:** Hong et al. presented a QIA protocol using single photon states [65]. Being single photon based scheme, the protocol was relatively less resource demanding and also more efficient as it allowed authentication of two bits of authentication key sequence using a single qubit.

Abulkasim et al. proposed an authenticated quantum secret sharing (QSS) protocol [66] based on Bell states. To obtain a higher level of security, here participants encrypt the pre-shared key before use. This trick is commonly used in quantum communication.

Nikolopoulos et al. introduced a CV authentication scheme [67] using coherent state of light and wavefront-shaping and homodyne measurement techniques.

Portmann proposed a quantum authentication scheme using recycling of the key [68] and showed the security against insecure noisy channels and shared secret key. They have also proved the number of recycled key bits is optimal for some authentication protocols.

**2018:** Kang et al. proposed a mutual authentication protocol [16] that allows Alice and Bob to authenticate each other even in the presence of an untrusted third party Trent. They used entanglement correlation checking (using GHZ-like states) to ensure that the state distributed by Trent is really entangled and random numbers to stop Trent from directly deducing the key. Similar strategies can be used into the other QIA protocols where a trusted third party is considered. Such a trivial effort can yield a set of new protocols for QIA.

A US patent (Patent number US 9,887,976 B2) was given for multi-factor authentication using quantum communication that involves two stages for enrollment and identification [69] with a computer system to implement a trusted authority.

**2019:** Semi-quantum protocols are a class of protocols that extends quantum security to some classical users. First semi-quantum protocol for QKD was proposed by Boyer et al. in 2007 [70]. Subsequently, semi-quantum schemes have been proposed for various tasks [71–74]. However, no semi-quantum authentication protocol was proposed until 2019, although that was a basic requirement of semi-quantum QKD and other semi-quantum cryptographic schemes. The gap was addressed by Wen et al. in 2019 when they introduced a semi-quantum authentication protocol [75] which is not required the quantum capability of all the users. Specifically, it allowed quantum Alice (Bob) to identify classical Bob (Alice).

Another facet of modern quantum cryptography also found its place in the authentication protocol in this year when Liu et al. introduced a QIA protocol [76] which can be used in the counterfactual QKD schemes.

Zheng et al. proposed a controlled QSDC (CQSDC) protocol with authentication [77] using five-qubit cluster state. Though the scheme was shown to be secure in the presence of noise, the five-qubit cluster state used in this protocol is extremely difficult to prepare and maintain.

It's straight forward to extend Bell state based schemes or GHZ state based schemes to the schemes that use  $n$ -partite entangled states such that  $n > 3$ . However, such an extension is not usually advantageous. Here it may be noted that this was not the first incident when a five qubit cluster state was used to design a scheme for QIA. In fact, in 2014, a QIA scheme using five qubit cluster state and one-time pad was proposed [17] and the same was cryptanalyzed in 2016 [78]. In addition, an entanglement swapping based scheme using six-qubit cluster state was proposed in 2012. Further, in 2015 an even larger entangled state (precisely six qubit state) was used in an effort to design a scheme of the authenticated QSDC scheme [79]. None of these schemes involving multi-partite entangled states are practically useful at the moment.

**2020:** Most of the protocols for QIA mentioned above have not considered the effect of noise which is unavoidable in practical situations. Addressing this issue directly, Qu et al. proposed a QIA protocol based on three-photon error avoidance code [80]. This scheme can effectively resist the interference of noise on information transmission through quantum channel.

Zhang et al. presented a Bell state based protocol of QIA that relies on entanglement swapping [15] and can provide security against the attacking strategies of a semi-honest third party. Here it may be noted that a semi-honest user strictly follows the protocol, but tries to cheat remaining within that. Consequently, attacks of a semi-honest third party are weaker compared to those of a dishonest third party and it's always preferable to consider a dishonest third party specially while dealing with schemes of quantum cryptography.

**2021:** Either existing protocols are cryptanalyzed or modified to propose a newer version of QIA scheme in connection with a specific application. Specifically, in [81] and in [82], QIA schemes are discussed in the context of quantum private query and QSDC, respectively. Further, an earlier proposed hybrid scheme of authentication [83] (which was an improved version of a single photon based scheme proposed in 2017 [65]) was systematically cryptanalyzed in Ref. [84]. In Ref. [84], two attacks are designed and it's shown that not only the protocols proposed in Refs. [65,83], a set of other existing protocols for QIA are also vulnerable under these attacks. In addition, an intense interest is observed in PUF based quantum authentication schemes [85,86] and closely related applications [87].

Before we close this section, it would be apt to note that there are a few variants of the authentication protocols. For example, we may note that deniable authentication is a particular variant of authentication protocol, which does not allow a receiver to prove the source of the message to a third party. For example, a protocol for quantum deniable authentication was proposed in [52]. Further, we must note that most of the QIA protocols are discussed in the two-party scenario involving sender Alice and receiver Bob, but there is a set of schemes where a third party Trent (referred to as an authenticator) is added. For example, using GHZ states [37], a set of two three-party schemes for QIA were proposed by Lee et al., but later it was reported in Ref. [39] that Trent can eavesdrop in both the protocols. Interestingly, in [39], a solution to circumvent the proposed attacks was also proposed. Further, in [25], a three party scenario where authentication was done by an arbitrator Trent.

### 3 Classification of the protocols for quantum identity authentication

Classification of anything depends on the criterion selected. Here, we will classify the existing schemes for QIA based on two criteria: (i) quantum resources used to design the schemes and (ii) computational or communication task inherently used to design the schemes. The classification performed

here is neither unique nor complete. One can, of course select a different criterion to classify the schemes. The reason behind classifying the schemes based on the above two criteria is to explore the inherent symmetry among the existing protocols for QIA and thus to create a framework for designing new protocols.

### 3.1 Classification based on the quantum resources used

Based on quantum resources used, we can classify the existing schemes of QIA simply into two classes: (a) schemes that use entangled states [11–18] and (b) schemes which don't use entangled states [10, 53, 56, 65, 83, 88].

#### 3.1.1 Entangled state based schemes of QIA

Bell states are the simplest entangled states, and they are easy to prepare and maintain. Naturally, a large number of Bell state-based schemes for QIA have been designed. Specifically, protocols are described in Refs. [11, 13–15, 18, 25, 26, 30, 31, 35, 42, 49, 66] using Bell states only. These protocols are different from each other in many different aspects: some of them use Bell states to perform entanglement swapping [12, 51], some others use it to design schemes for authentication in analogy to ping-pong protocol for QSDC [38]. However, the beauty of Bell states (more precisely, the advantages of nonlocality) is not yet explored in its fullest. Specifically, one can also exploit the inherent symmetry explored in this review to design device independent and semi-device independent schemes for QIA. Further, simple QIA schemes based on the violation of Bell inequality can also be devised. Of course implementation of such schemes will be more demanding compared to the existing schemes, but will have their own advantages. Further, there are existing schemes of authentication, which uses multipartite entangled states. For example, authentication schemes using three-qubit GHZ states are reported in [12, 37, 40, 51, 52] and three-qubit GHZ-like states (which are also GHZ states) are used to design QIA schemes in Refs. [16, 75]. Also, in Ref. [17], five-qubit cluster states are used for identity authentication. Creation and maintenance of such multi-partite entangled states are still challenging. In addition, most of these entangled states based schemes of QIA require quantum memory which is not available at the moment.

#### 3.1.2 Schemes of QIA which don't use entanglement

There are many schemes of QIA which uses separable states or more precisely single photon states. For example, we may mention [10, 53, 56, 65, 83, 88] and similar schemes. The advantage of these schemes over the entangled state based schemes arises from the relative ease of the preparation of single qubit states and the fact that most of the entangled state based schemes need to store home qubits that requires quantum memory which is not available, but the single qubit based schemes generally does not require quantum memory. Consequently, these protocols appear to be more feasible from the perspective of practical implementation. These protocols primarily use BB84 kind of encoding, where travel qubits are prepared in  $Z = \{|0\rangle, |1\rangle\}$  basis or  $X = \{|+\rangle, |-\rangle\}$  basis based on the pre-shared authentication key and a predecided rule that connects bit value of authentication key to the basis in which a travel qubit is to be prepared. A particular scheme of this type is Zawadzki's [83] scheme for QIA. Recently, Guillou et al. [84] have shown that Zawadzki's scheme is insecure in general and the claimed logarithmic security of Zawadzki's scheme loses its advantage under a key space reduction attack which is explicitly described by Guillou et al.

These kind of schemes often uses Hash function to ensure the security of the authentication procedure. However, the use of Hash function takes us outside the domain of quantum security, but at present confidence of the cryptographers on a set of Hash functions is high. In what follows, we

propose a set of three new protocols for QIA in Section 4, out of which two protocols are single qubit based, but not vulnerable under key space reduction attack and other known strategies.

## 3.2 Classification of the protocols based on the computational or communication tasks used to design the schemes

In the section we will classify the existing protocols for QIA based on the computational or communication tasks involved in the realization of the scheme for QIA. To begin with, let us briefly describe the schemes for QIA which are based on specific quantum communication tasks.

### 3.2.1 Protocols based on the schemes for QKD

There exist many protocols of authentication, which are essentially based on the existing schemes of QKD. In fact, all schemes for QKD can in principle be reduced to schemes of QIA, provided there exists a pre-shared secret key. Of course, one may need to slightly modify the original protocol of QKD to reduce it to a scheme for QIA. For example, such an effort was made in [89] where a scheme of QIA was obtained by slightly modifying BB84 protocol of QKD. Lately, a counterfactual QKD scheme was modified to propose a scheme for QIA in [76]. Further, in the early work of Duijck et al. a classical-quantum hybrid scheme of authentication was used where the quantum part was based on QKD. To be precise, they utilized the fact that QKD schemes are essentially schemes for key amplification, and thus if Alice and Bob start with a pre-shared sequence for identity authentication and use that sequence only once to authenticate each other and thus to generate a secure key using a scheme of QKD then for a later run of identity authentication part they will be able to use a part of the key generated by the scheme of QKD. Here, only the refueling of the identity authentication sequence happens via QKD, so this early effort does not really qualify as a scheme of QIA, but it was definitely based on QKD. Similar use of QKD in the authentication process is now common.

### 3.2.2 Protocols based on the schemes for QSDC and DSQC

There are two types of schemes of secure quantum direct communication, namely QSDC and DSQC. There exist many schemes of QSDC and DSQC (cf. [19, 21, 71, 90, 91] and references therein) and each of them provides a way to directly transfer a message from sender Alice to receiver Bob in an unconditionally secure manner. Now, if we assume that Alice and Bob have a pre-shared secret then Alice can send a part or full of that secret to Bob by using a QSDC or DSQC protocol and Bob can decipher the text and compare with his secret to verify Alice's identity. Thus, in principle, every QSDC and DSQC protocol can be converted to protocols for QIA. A specific example of early QSDC protocol is ping-pong protocol, the same was used to design a scheme for QIA by Zhang et al. in 2006 [14] as an example of this class of QIA schemes. Here, we may note that schemes for secure direct quantum communication that cannot be used for long distance quantum communication due to noise can also be used for QIA. Specifically, in the context of CV secure direct quantum communication, this particular advantage of the schemes of secure direct quantum communication was noted in Ref. [92]. The beauty of CV-QIA schemes (independent of whether it's designed using a scheme of CV-QSDC or CV-DSQC) like the one hinted in [92] underlies in the fact that the existing infrastructure can be used for the implementation of these schemes.

LM05 [54] is a single photon based protocol for QSDC, which is analogous to ping-pong protocol of QSDC. Using LM05 protocol, another scheme of QIA was proposed by Yuan et al. in 2014 [53] they described it as a ping-pong scheme without entanglement, but it was actually a modified LM05 scheme. Interestingly, neither Zhang et al. nor Yuan et al. and the subsequent authors have

recognized the essential symmetry mentioned above which allows to transform all the existing schemes for QSDC and DSQC to the schemes for QIA.

Reduction of schemes of QSDC or DSQC into the schemes for QIA often involves some modifications which take the final scheme outside the domain of QSDC or DSQC and in reality we obtain QSDC or DSQC inspired schemes for QIA. For example, structure of Zhang et al.'s scheme [13] is analogous to the original ping-pong protocol, but it's different in the sense that the travel qubit sent by Bob to Alice is not returned by Alice further. Specifically, in Zhang et al. scheme, a Bell state  $\psi_{AB}^+ (= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$  is pre-shared by Alice and Bob, where the subscript  $A(B)$  refers to the qubit in possession of Alice (Bob). In the original ping-pong protocol, Bob prepares the Bell state and sends a qubit (travel qubit) to Alice, but this step may be considered as equivalent. Here Bob prepares an arbitrary single qubit pure state  $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$  and sends it to Alice, who performs a CNOT using her share of the Bell state as control qubit and  $|\psi_1\rangle$  as the target qubit. Subsequently, Alice returns the qubit indexed with subscript 1 (here we get the analogy with ping-pong) and after receiving that Bob performs a CNOT operation using his share of Bell state (qubit  $B$ ) as control qubit and qubit 1 as the target qubit. After that, Bob measures qubit 1 in a basis in which  $|\psi_1\rangle$  is a basis element, if he obtains  $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$  then the authentication succeeds. There are two specific reasons behind additional attention being given to this type of QSDC based protocols. Firstly, in what follows, we will propose new QSDC/DSQC based protocols and secondly several QSDC/DSQC based protocols for QIA have recently been proposed and those protocols may be viewed as protocols belonging to the ping-pong family. For example, Li et al. proposed a QIA protocol [11] in a manner similar to Zhang et al.'s scheme with a difference that in their protocol instead of single qubit state  $|\psi_1\rangle$  prepared and shared by Bob, Alice prepares an auxiliary Bell state and performs a CNOT operation in which the first qubit of auxiliary Bell state is used as the control qubit and her qubit of the pre-shared Bell state (qubit  $A$ ) as target. Then she sends the auxiliary Bell pair to Bob who performs the CNOT operation with the second qubit of the auxiliary pair as control qubit and qubit  $B$  as target qubit. If a subsequent Bell measurement performed by Bob on the auxiliary Bell state finds it in the same state in which it was prepared by Alice then authentication is considered to be successful. The above two protocols require quantum memory, but quantum memory devices are not yet available commercially. Even the lab-level quantum memory devices available today require much development before those can be used in real applications.

Later, Zhang et al. introduced a one-way QIA protocol [14] which is also similar to the protocol [13]. This protocol was followed by another protocol by Li et al. [93] which can be viewed as a modified version of their earlier protocol [11] as the auxiliary state is now prepared by Alice and Bob separately in a single qubit state instead of Bell state. As it appears from the brief description of the protocols, all the protocols described in this section belongs to ping-pong family of protocols for QIA. This family of protocols contains several other protocols, including the single qubit based protocol of Yuan et al. [53].

### 3.2.3 Protocols based on teleportation

It's known that teleportation can be used for secure communication provided we have an ideal (noise free) quantum channel [94]. This is a known issue and will be discussed in some more details in Section 3.2.7. Despite this issue and associated issues involving entanglement concentration and/or purification, several authors have proposed schemes for QIA based on teleportation. For example, we may mention the schemes reported in [35, 51, 57] and the references therein. Interestingly, even for CV-QIA a teleportation based scheme has been proposed [57]. However, applicability of all these schemes are limited by the requirement that in a noisy situation shared entanglement will get corrupted and to obtain the desired entangled state from that one would require to implement an entanglement purification or concentration scheme which would require interaction between Alice

and Bob even before the authentication. Here it may be noted that the above mentioned concern is also applicable to a large number of entangled states based protocols for QIA (e.g., [13] and similar schemes) which do not explicitly use teleportation, but use shared entanglement. This undesired interaction is a weakness of the QIA schemes which are directly based on teleportation or shared entanglement. However, clever tricks like one used in Barnum et al. [95] (cf. Section 3.2.7 for a short discussion) can help us to circumvent this limitation of the teleportation based schemes for QIA.

### 3.2.4 Protocols based on quantum secret sharing

Quantum secret sharing (QSS) schemes are also modified to design schemes for QIA enabling authentication of the legitimate users individually or simultaneously by a set of other users or trusted third party [96]. In addition, a set of schemes for QSS with the feature of identity authentication for better security have been proposed [66, 97–99]. A large variety of quantum resources and operations (e.g., Bell state, phase-shift operation, GHZ state) have been used in these schemes. In an interesting development, an effort was made in Ref. [97] to simultaneously use the concept of QSS and QD [20, 100] to design protocols for mutual QIA. In multiparty version of the scheme proposed by Abulkasim et al. Alice was considered to be the boss and Bob and Charlie as her agents. In a later work [101], a vulnerability of the Abulkasim et al.’s scheme was reported and it was shown that if the agents (Bob and Charlie) collude then the Abulkasim et al.’s scheme becomes insecure. Responding to this criticism, Abulkasim et al. proposed a modified version of their earlier scheme in [102] which was a QSS based scheme free from the collusion attacks of the agents.

Protocols reviewed and classified in this section till now are all derived from the protocols for different quantum communication tasks, e.g., teleportation, QKD, QSDC and DSQC. In what follows, we will show that a similar reduction is possible from the protocols for different quantum computing tasks, too.

## Protocols based on quantum computation tasks

As mentioned above, existing protocols for different quantum computing tasks can be modified to obtain schemes for QIA and the same has been done since the early days of QIA schemes. In fact, the pioneering effort for designing QIA by Crépeau et al. [8] involved OT. To begin with we will mention that, and will continue to discuss the schemes designed (or can be designed) using the schemes of other computing tasks, like blind quantum computing and quantum private comparison.

### 3.2.5 Protocols based on oblivious transfer

As mentioned in Section 1, first protocol for QIA was proposed by Crépeau et al. [8] in 1995 using OT. The scheme was aimed to check the identities of the legitimate participants having a pre-shared common information by comparing their mutual knowledge of this common information. This pioneering effort to design a scheme of identity authentication whose security is obtained from the attributes of quantum mechanics has been followed by many others. In fact, security of all the protocols for QIA mentioned in this review are obtained from the quantum features. However, OT is hardly used as a resource to design schemes for QIA.

### 3.2.6 Protocols based on blind quantum computing

Blind quantum computing (BQC) was first proposed by Childs [103], his demand was that a user (client) with limited amount of quantum resources may delegate a task to another user or quantum server having full quantum capability or more quantum power, with the condition that input and

output of the client and the computational task performed are kept in private, i.e., the server or the user with higher quantum power remains blind about these information. Several schemes of BQC with identity authentication have been proposed [104–106], but the capability for BQC in designing schemes of QIA is not yet fully utilized. However, in Ref. [107], a scheme for blind quantum signature—a task closely related to QIA has been proposed using BQC. This may be mapped to a scheme of QIA and generalizing the idea, efforts may be made to explore the possibility of designing schemes for QIA using the existing and new schemes for BQC. This is a strong possibility that needs to be explored properly.

### 3.2.7 Protocols based on quantum error detection or correction code

A simple idea for performing authentication may be to start with a shared entangled state(s) and a private quantum key which is to be teleported by Alice to Bob using the shared entangled state for the verification of her identity by Bob. Interestingly, the shared entanglement can get corrupted due to noise and Alice and Bob may require to execute a purity-testing protocol, which would check whether the shared entangled state is in the desired state or not, but it would not try to correct it as is done in the schemes of entanglement concentration and purification. Barnum et al. [95] realized that such a protocol for purity testing is expected to be interactive, but this interactive nature is not desired in the schemes for QIA and quantum message authentication specially when one-way authentication is desired. Here comes the beauty of Barnum et al.’s [95] idea, they first established that purity-testing schemes can be designed using a family of quantum error-correcting codes (QECCs) having a specific property that any Pauli error is detected by most of the codes in the family. Subsequently, they showed that a scheme for secure non-interactive quantum authentication can be derived from any scheme of purity-testing which can be obtained from a QECC. This is an interesting work where QECCs were used for quantum authentication. Much later, Qu et al. proposed a QIA protocol based on three-photon error avoidance code [80, 108].

### 3.2.8 Protocols based on quantum private comparison

In 2017, Hong et al. proposed an efficient single qubit based protocol for QIA [65] where decoy qubits were used for establishing the security against eavesdropping. The protocol was efficient in the sense that verification of two bits of authentication information was performed using a single qubit. Later this protocol was cryptanalyzed and improved by Zawadzki [83]. Zawadzki’s main criticism was that each run of Hong et al.’s protocol causes some information leakage and an eavesdropper can continue collecting such information in successive protocol runs. Zawadzki proposed an improved version of Hong et al.’s protocol where Hash function was also used. Interestingly, Guillou et al. has recently shown that Zawadzki’s protocol is vulnerable against key space reduction attack [84]. Without going into a detailed discussion on that aspect, we would like to note that in Zawadzki’s protocol and many other protocols for QIA the main task is actually to perform quantum private comparison or to compute a function  $f(A, B) : f(A, B) = 0$  if  $A \neq B$  and  $f(A, B) = 1$  if  $A = B$ , using quantum resources without really disclosing the value of  $A$  and  $B$  to a party who computes this function (of course, some information will be logically obtained from the value of  $f(A, B)$ ). This is a standard problem of secure multiparty computation [90, 109, 110] and the task is closely related to the socialist millionaire problem [20]. To visualize this let us look back on Zawadzki’s protocol in little more detail. In Zawadzki’s protocol (and in many other protocols) Alice and Bob share secret authentication key  $k$ . Alice generates a random number  $r_A$  and computes session secret ( $s_A = H(k, r_A)$ ) using secret key ( $k$ ) and Hash function ( $H$ ). Alice subsequently sends the random number  $r_A$  to Bob, who may receive a different number  $r_B$  and uses that to generate his own copy of session secret ( $s_B = H(k, r_B)$ ). The rest of the task is simply to use quantum resources to compare whether  $s_A = s_B$  or not or

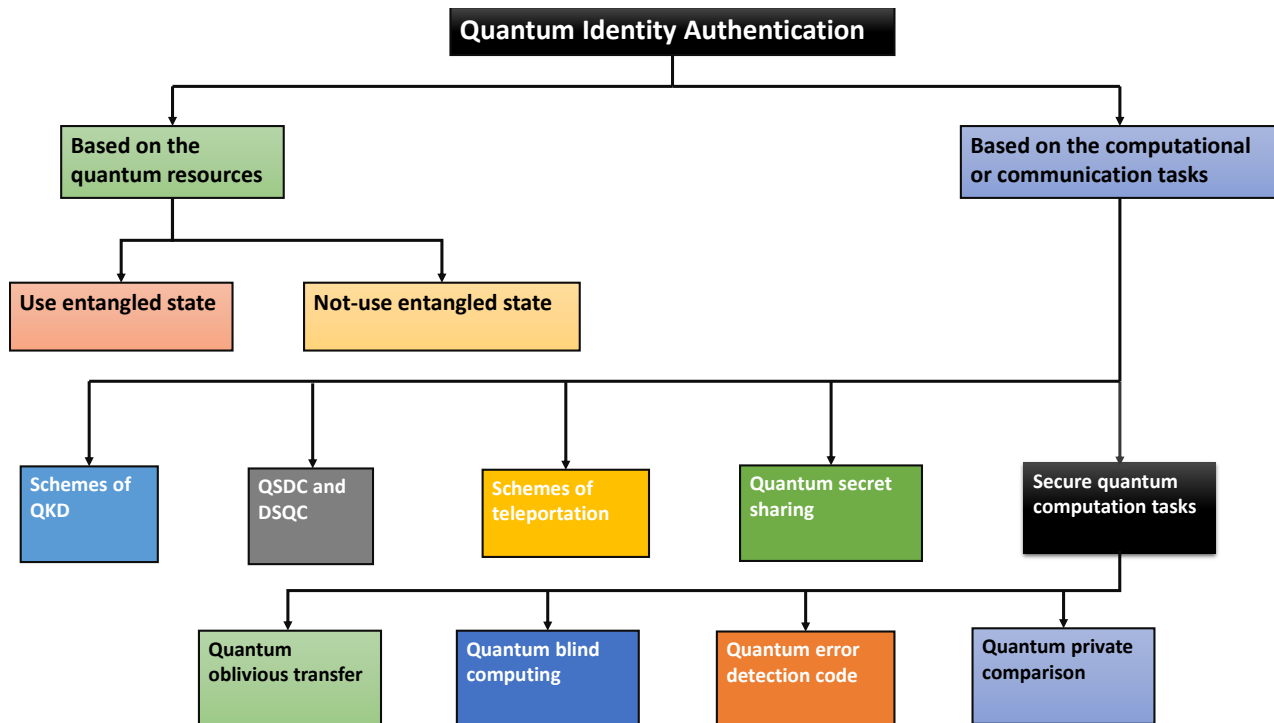


Figure 2: (Color online) Classification of the schemes for QIA.

equivalently to perform a quantum private comparison task by computing  $f(s_A, s_B)$ . Equality of  $s_A$  and  $s_B$  would imply successful authentication. Realization of this connection between the quantum private comparison and QIA enables us to conclude that the existing schemes of quantum private comparison and socialist millionaire problems can be reduced to the protocols for QIA. For example, such protocols designed by some of the present authors and reported in [20, 71, 72, 100, 109] can easily be reduced to the schemes for QIA. Interestingly, some of such reduced schemes for QIA will even work in the semi-quantum framework [71, 72], where all the users need not have access to quantum resources. Here, it may be further noted that capability of performing QD (simultaneous two-way communication between Alice and Bob) or quantum conference [111] ensures the capability of performing direct secure quantum communication (QSDC or DSQC) which can be used to perform QIA (as shown in Section 3.2.2). Thus, even without transforming the schemes of QD or quantum conference into those of quantum private comparison, one can follow a relatively direct route and design QSDC/DSQC based new schemes for QIA.

Classification of the schemes for QIA performed in this section are broadly summarized in Fig. (2). This figure illustrates that QIA can be performed in various ways and using various resources. Choice of a particular scheme would depend on the nature of the task and the available resources. For instance, all the existing schemes may be categorized on the basis of requirement of classical channel, quantum memory and a third party as well as nature of pre-shared key (classical or quantum) and the desired one-way or two-way authentication.

## 4 New protocols for quantum identity authentication

In Section 2 and 3, we have hinted at various possibilities of designing new protocols for QIA. As discussed above there are many possibilities of designing new and modified protocols (of course some of them will be trivial extension/modification of the existing protocols). To establish the validity of our claim and to show that the symmetry among the protocols appeared through the systematic



review of the existing protocols can really be exploited to design new protocols of QIA, here we propose 3 new protocols of QIA, all of which are based on the schemes for secure direct quantum communication (i.e, QSDC and DSQC). These protocols are to be viewed as representative protocols from the set of many protocols which can be designed by using the protocols for other communication and computation tasks. However, before we proceed, we must note that the classification used here is along the lines of the literature of QIA, but in a strict sense the protocols described below and in the existing literature do not qualify as direct communication schemes. At best these schemes may be viewed as QSDC inspired or DSQC inspired schemes for QIA. However, to avoid confusion among the readers we are using here a relatively liberal definition of QSDC and DSQC and classifying the schemes in line with the literature of QIA.

## New protocols based on QSDC

In Section 3.2.2, we have already mentioned that the schemes of secure direct quantum communication can in principle be used to design schemes for QIA, and a set of protocols for QIA has already been proposed using the schemes for QSDC and DSQC. However, the identification of the existing symmetry among these protocols allows us to construct new protocols. As an example, here we propose two new protocols for QIA which are based on QSDC. Let's begin with the first protocol.

### Protocol 1:

This QSDC based protocol for QIA is distinct but analogous to the schemes proposed in [17, 53]. In what follows, this QSDC inspired protocol is referred to as Protocol 1 and its steps are described as Step 1. $j$  (in general Step  $i.j$  :  $i, j \in \{1, 2, \dots\}$  would refer to  $j^{th}$  step of the newly proposed  $i^{th}$  protocol). In this protocol, it's assumed that Alice and Bob possess a pre-shared authentication key  $K = \{k_1, k_2, k_3, \dots, k_{2n}\}$ , and the protocol is described in the following steps.

- *Encoding mode*

Table 1: The preparation method of the decoy sequence (Protocol 1)

$(2i)^{th}$ bit value: $k_{2i}$	0	1
$i^{th}$ qubit of decoy sequence: $K_{d_i}$	$ 0\rangle$ or $ 1\rangle$	$ +\rangle$ or $ -\rangle$

**Step 1.1:** Alice prepares an ordered  $n$ -qubit decoy sequence  $K_d$  depending upon the bits of the pre-shared key  $K$ . If  $k_{2i} = 0$ ,  $i^{th}$  particle of  $K_d$  is prepared in the state  $|0\rangle$  or  $|1\rangle$ , otherwise the  $i^{th}$  particle is prepared in the state  $|+\rangle$  or  $|-\rangle$  with only Alice knowing the exact states of the particles in  $K_d$ .

**Step 1.2:** Alice prepares another particle sequence  $K_a$  to be used as authentication qubits. The  $i^{th}$  particle of  $K_a$  is in state  $|0\rangle$  if  $k_{2i-1} \oplus k_{2i} = 0$ , else in state  $|-\rangle$ . Alice inserts the authentication qubits of  $K_a$  into the sequence  $K_d$  to form an enlarged sequence  $K_A$  according to the rule that if  $k_{2i-1} \oplus k_{2i} = 0$ , then Alice puts the  $i^{th}$  particle of  $K_a$  after the  $i^{th}$  particle in  $K_d$  or else, puts the  $i^{th}$  particle of  $K_a$  before the  $i^{th}$  particle in  $K_d$ . Alice then sends the enlarged sequence  $K_A$  to Bob.

- *Decoding mode*

Table 2: The preparation method of the authentication sequence (Protocol 1)

Additional modulo 2: $k_{2i-1} \oplus k_{2i}$	0	1
$i^{th}$ qubit of authentication sequence: $K_{a_i}$	$ 0\rangle$	$ -\rangle$

Table 3: Measurement basis used by Bob to get the result for the authentication sequence (Protocol 1)

Additional modulo 2: $k_{2i-1} \oplus k_{2i}$	0	1
Measurement basis: $B_i = \{B_z, B_x\}$	$B_z = \{ 0\rangle,  1\rangle\}$	$B_z = \{ +\rangle,  -\rangle\}$
Measurement result:	$ 0\rangle$	$ -\rangle$

**Step 1.3:** According to the pre-shared key  $K$ , Bob calculates the position and the basis used for the decoy qubits and authentication qubits by Alice then Bob measures the decoy qubits  $K_d$  and authentication qubits  $K_a$  sequentially applying the rules that, when  $k_{2i} = 0$ , Bob will use the  $Z$ -basis ( $\{|0\rangle, |1\rangle\}$ ) to measure the particles of  $K_d$ , else he will use  $X$ -basis ( $\{|+\rangle, |-\rangle\}$ ) and measures the authentication qubit  $K_a$  according to the value of  $k_{2i-1} \oplus k_{2i}$  and matches them with the expected outcomes which is described in Table (3). Bob calculates the QBER value using the measurement result of decoy sequence  $K_d$ , if QBER is lesser than a tolerable limit, it confirms that the channel is secure. If the measurement result of authentication sequence  $K_a$  mismatches by greater than the tolerable limit, then Bob discards the protocol, else Bob confirms the identity of Alice.

**Step 1.4:** Bob prepares the decoy sequence  $K'_d$  using the same method described in Step 1.1 and also prepares the authentication qubit sequence  $K'_a$  applying same encoding rules and uses this rule to form an enlarged sequence  $K_B$ . Bob then sends the enlarged sequence  $K_B$  to Alice.

**Step 1.5:** Alice separates the decoy sequence from the authentication qubits and confirms the identity of Bob in a manner similar to that mentioned in Step 1.3.

## Protocol 2:

As in the previous protocol, Alice and Bob are assumed here to pre-share an authentication key  $K = \{k_1, k_2, k_3, \dots, k_{4n}\}$  with the only difference with the previous protocol is that the length of the pre-shared key is now  $4n$  which is double in comparison to the previous scheme.

- *Encoding mode*

Table 4: The preparation method of the authentication sequence (Protocol 2)

Additional modulo 2: $k_{2i-1} \oplus k_{2i}$	0		1	
Bit value: $k_{2i}$	0	1	0	1
Prepared authentication state: $K_{A_i}$	$ 0\rangle$	$ 1\rangle$	$ +\rangle$	$ -\rangle$

**Step 2.1:** Alice prepares an ordered  $n$ -particle sequence  $K_A$  using the first half of the pre-shared authentication key ( $2n$  bits) with the condition that when  $k_{2i-1} \oplus k_{2i} = 0$ , then Alice prepares the particle state as  $|0\rangle$  and  $|1\rangle$  respectively for  $k_{2i} = 0$  and  $k_{2i} = 1$ . Further, when  $k_{2i-1} \oplus k_{2i} = 1$ , then Alice prepares the particle state as  $|+\rangle$  and  $|-\rangle$  respectively for  $k_{2i} = 0$  and  $k_{2i} = 1$ . Alice then sends the ordered particle sequence  $K_B$  to Bob.

**Step 2.2:** Bob performs a measurement on the  $i^{th}$  particle of the ordered sequence  $K_B$  in the  $Z$ -basis ( $\{|0\rangle, |1\rangle\}$ ) if  $k_{2i-1} \oplus k_{2i} = 0$  or else use  $X$ -basis ( $\{|+\rangle, |-\rangle\}$ ). Bob forms a classical bit sequence  $S_B$  by using the knowledge that quantum states  $|0\rangle$  and  $|+\rangle$  represent 0 while  $|1\rangle$  and  $|-\rangle$  represent 1. Bob compares the  $i^{th}$  bit of  $S_B$  with  $k_{2i}$  and for an ideal case it should be  $K_B = k_{2i}$ . If the error rate is less than the tolerable limit, then Bob confirms the identity of Alice.

- *Decoding mode*

Table 5: Measurement basis used by Bob to get the result for the authentication sequence (protocol 2)

Additional modulo 2: $k_{2i-1} \oplus k_{2i}$	0	1
Bit value: $k_{2i}$	0 1	0 1
Measurement basis: $B_i = \{B_z, B_x\}$	$B_z = \{ 0\rangle,  1\rangle\}$	$B_z = \{ +\rangle,  -\rangle\}$
Measurement result:	$ 0\rangle \quad  1\rangle$	$ +\rangle \quad  -\rangle$

**Step 2.3:** Bob performs the Step 2.1 similar to that of Alice with the rest half of the pre-shared authentication key.

**Step 2.4:** Alice performs as the Step 2.2 to confirm the identity of Bob.

As mentioned above Protocols 1 and 2 are just examples of the protocols which can be designed using the schemes for QSDC. Following the same line, other existing schemes of QSDC can also be modified to obtain the schemes for QIA. The security of these schemes of QIA will be analyzed in Section 5. Before we proceed to security analysis, let us propose another scheme for QIA.

## New protocol based on controlled DSQC

We know that QSDC is one facet of the secure direct quantum communication, and DSQC is the other facet of it. We have already presented two schemes based on QSDC, let us know provide an example establishing that schemes of DSQC (more precisely a controlled version of DSQC, i.e., Controlled DSQC (CDSQC)) can also be modified to design schemes for QIA. Before we explicitly describe our 3<sup>rd</sup> protocol, we would like to briefly describe the basic idea behind the designing of this protocol.

### Basic idea

This protocol is based on the properties of Bell state and entanglement swapping. The corresponding relations between the Bell state and the pre-shared authentication key is as follows:

$$\begin{aligned}
 00 : |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
 01 : |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
 10 : |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\
 11 : |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
 \end{aligned} \tag{1}$$

Also, the relations between the corresponding Pauli operations and pre-shared authentication key is as follows:

$$\begin{aligned}
00 : I &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\
01 : \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\
10 : i\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0|, \\
11 : \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|.
\end{aligned} \tag{2}$$

Now, let us briefly describe the idea behind this protocol. Suppose Alice and Bob have previously shared authentication key (bit string) of a certain length. Consider the bit string as 10, so Alice and Bob prepare the Bell states as per (1)

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{12(34)} + |10\rangle_{12(34)}), \tag{3}$$

With the subscripts 1,2 and 3,4 representing the particles of Alice and Bob, respectively. Alice (Bob) sends Particle 2 (4) to (semi-honest) Charlie, who acts as the third party authenticator. Charlie prepares one of the following quantum states

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_5 \pm |1\rangle_5). \tag{4}$$

Let's assume, Charlie chooses  $|-\rangle$  state. The combined state of Alice, Bob and Charlie can be expressed as

$$|\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34} \otimes |-\rangle_5 = \frac{1}{2\sqrt{2}}[(|01\rangle + |10\rangle)_{12} \otimes (|01\rangle + |10\rangle)_{34} \otimes (|0\rangle - |1\rangle)_5].$$

Charlie performs a CNOT operation with Particle 5 acting as control qubit and the target qubit chosen randomly between Particle 2 or 4. Charlie then sends the Particle 2 to Bob and Particle 4 to Alice. Meanwhile, Alice and Bob perform  $i\sigma_y$  operator (according to their secret key  $S_{AB} = \{10\}$ ) as shown in (2) on their Particles 1 and 3 respectively. Let us suppose that for the CNOT gate, the target is particle 2 then the final joint state after performing the CNOT operation and Pauli operation can be written as,

$$\begin{aligned}
|\Psi\rangle_{12345} &= \frac{1}{2\sqrt{2}}[|11110\rangle - |10111\rangle - |11000\rangle + |10001\rangle \\
&- |00110\rangle + |01111\rangle + |00000\rangle - |01001\rangle]_{12345},
\end{aligned}$$

This equation can be rearranged and written as

$$\begin{aligned}
|\Psi\rangle_{14235} &= \frac{1}{2\sqrt{2}}[(|\phi^+\rangle_{14} \otimes |\phi^+\rangle_{23} + |\phi^-\rangle_{14} \otimes |\phi^-\rangle_{23} \\
&- |\psi^+\rangle_{14} \otimes |\psi^+\rangle_{23} - |\psi^-\rangle_{14} \otimes |\psi^-\rangle_{23}) \otimes |0\rangle_5 \\
&+ (-|\phi^+\rangle_{14} \otimes |\psi^+\rangle_{23} + |\phi^-\rangle_{14} \otimes |\psi^-\rangle_{23} \\
&+ |\psi^+\rangle_{14} \otimes |\phi^+\rangle_{23} - |\psi^-\rangle_{14} \otimes |\phi^-\rangle_{23}) \otimes |1\rangle_5.
\end{aligned} \tag{5}$$

Alice and Bob then perform the Bell measurements on the particles which they have right now (i.e., 1 and 4 with Alice and 2 and 3 with Bob) and send to Charlie the classical bits corresponding to their measurement outcomes (as per (1)). Charlie then measures the Particle 5 in the computational basis ( $\{|0\rangle, |1\rangle\}$ ) to get either the state  $|0\rangle$  or  $|1\rangle$  with  $\frac{1}{2}$  probability. Charlie then performs the XOR operation on the classical bits sent by Alice and Bob. The list of possible outcomes as per the measurements performed by Alice, Bob and Charlie for the above example has been shown in Table (6).

We can see from the Table 6 that if the Charlie gets the state  $|0\rangle$  then XOR of the classical bits sent by Alice and Bob will always be 00. For the case in which Charlie gets the state  $|1\rangle$  then XOR of the classical bits sent by Alice and Bob will always be 10. Any deviation from from the mentioned outcomes reveals the presence of an Eve.

Table 6: The possible measurement results by all the parties in Protocol 3 for QIA.

Alice and Bob's possible combination result	Charlie's result	Additional modulo 2
$ \phi^+\rangle_{14} \oplus  \phi^+\rangle_{23}$	$ 0\rangle_5$	$00 \oplus 00 = 00$
$ \phi^-\rangle_{14} \oplus  \phi^-\rangle_{23}$	$ 0\rangle_5$	$01 \oplus 01 = 00$
$ \psi^+\rangle_{14} \oplus  \psi^+\rangle_{23}$	$ 0\rangle_5$	$10 \oplus 10 = 00$
$ \psi^-\rangle_{14} \oplus  \psi^-\rangle_{23}$	$ 0\rangle_5$	$11 \oplus 11 = 00$
$ \phi^+\rangle_{14} \oplus  \psi^+\rangle_{23}$	$ 1\rangle_5$	$00 \oplus 10 = 10$
$ \phi^-\rangle_{14} \oplus  \psi^-\rangle_{23}$	$ 1\rangle_5$	$01 \oplus 11 = 10$
$ \psi^+\rangle_{14} \oplus  \phi^+\rangle_{23}$	$ 1\rangle_5$	$10 \oplus 00 = 10$
$ \psi^-\rangle_{14} \oplus  \phi^-\rangle_{23}$	$ 1\rangle_5$	$11 \oplus 01 = 10$

### Protocol 3:

Here, two parties Alice and Bob wish to verify themselves as authenticated users through a third party Charlie. In this protocol, Alice and Bob have a pre-shared sequence of a classical secret key  $K_{AB} = \{k_1^1 k_2^1, k_1^2 k_2^2, k_1^3 k_2^3, \dots, k_1^i k_2^i, \dots, k_1^n k_2^n\}$ . The steps involved in the authentication are as follows:

**Step 3.1:** Alice and Bob separately prepare a sequence of  $n$  Bell states  $A_{12}$  and  $B_{34}$  respectively as per the pre-shared key  $K_{AB}$  and rule mentioned in (1).

$$\begin{aligned} A &= \{|A\rangle_{12}^1, |A\rangle_{12}^2, |A\rangle_{12}^3, \dots, |A\rangle_{12}^i, \dots, |A\rangle_{12}^n\} \\ B &= \{|B\rangle_{34}^1, |B\rangle_{34}^2, |B\rangle_{34}^3, \dots, |B\rangle_{34}^i, \dots, |B\rangle_{34}^n\} \end{aligned} \quad (6)$$

The subscripts 1, 2, 3 and 4 are just used to distinguish the particles in the sequences. Ideally,  $A = B$ .

**Step 3.2:** Alice and Bob divide each state of their Bell states into two ordered sequences of  $n$  particles, each with the first particle of each Bell state forming one sequence while the second particle of Bell states forming the other sequence.

$$\begin{aligned} S_1 &= \{s_1^1, s_1^2, s_1^3, \dots, s_1^i, \dots, s_1^n\} \\ S_2 &= \{s_2^1, s_2^2, s_2^3, \dots, s_2^i, \dots, s_2^n\} \\ S_3 &= \{s_3^1, s_3^2, s_3^3, \dots, s_3^i, \dots, s_3^n\} \\ S_4 &= \{s_4^1, s_4^2, s_4^3, \dots, s_4^i, \dots, s_4^n\} \end{aligned} \quad (7)$$

Here  $S_1$  is the sequence of the first particles of all Bell states in  $A$  and  $S_2$  is the sequence of the second particles of all Bell states in  $A$ . Similarly,  $S_3$  is the sequence of the first particles of all Bell states in  $B$  and  $S_4$  is the of sequence the second particles of all Bell states in  $B$ . Alice and Bob respectively hold the particle sequence  $S_1$  and  $S_3$  with themselves. Further, Alice (Bob) randomly inserts the decoy particles  $d_a$  ( $d_b$ ) into the sequence  $S_2$  ( $S_4$ ) to form an enlarged sequence  $S'_2$  ( $S'_4$ ). Alice (Bob) sends the sequence  $S'_2$  ( $S'_4$ ) through the quantum channel to Charlie.

**Step 3.3:** Charlie receives the sequence  $S'_2$  and  $S'_4$  and performs the security tests using the decoy particles. After the successful security tests, Charlie removes the decoy particles  $d_a$  ( $d_b$ ) to get the original sequence  $S_2$  ( $S_4$ ). Further, Charlie also prepares a sequence of  $n$  qubits  $S_5 = \{s_5^1, s_5^2, s_5^3, \dots, s_5^i, \dots, s_5^n\}$  with each qubit arbitrary in the state  $|+\rangle$  or  $|-\rangle$ . Charlie then performs a CNOT operation with the particles of sequence  $S_5$  acting as control qubit and the particles of sequence  $S_2$  or  $S_4$  as the target qubit randomly.

**Step 3.4:** Charlie then prepares decoy particles  $d_c$  ( $d_d$ ) and inserts them randomly into sequence  $S_2$  and  $S_4$  to form an enlarged sequence  $S'_2$  ( $S'_4$ ). Charlie sends the sequence  $S'_2$  ( $S'_4$ ) to Bob (Alice). After successfully performing the security checks with the decoy particles and removing them, Alice (Bob) now holds the sequences  $S_1$  and  $S_4$  ( $S_2$  and  $S_3$ ).

**Step 3.5:** Alice (Bob) performs the Pauli operation on the particles of the sequence  $S_1$  ( $S_3$ ) corresponding to pre-shared classical key as per (2). After the Pauli operation the sequences change into  $S_1^*$  and  $S_3^*$ . Now, Alice performs the Bell measurement on the particles of sequence  $S_1^*$  and  $S_4$  and notes the measurement outcome as classical sequence  $R_{14} = \{r_{14}^1, r_{14}^2, \dots, r_{14}^i, \dots, r_{14}^n\}$  as per (1). Bob also performs the Bell measurement on the particles of sequence  $S_2$  and  $S_3^*$  and notes the measurement outcome in form of classical sequence  $R_{23} = \{r_{23}^1, r_{23}^2, \dots, r_{23}^i, \dots, r_{23}^n\}$ . Alice and Bob send their classical sequences  $R_{14}$  and  $R_{23}$  to Charlie. Meanwhile, Charlie also measures the sequence  $S_5$  in the computational basis  $\{|0\rangle, |1\rangle\}$  to get a sequence  $R_5 = \{r_5^1, r_5^2, \dots, r_5^i, \dots, r_5^n\}$ , with  $r_5^i = 0$  or  $r_5^i = 1$  corresponding to the situations  $|0\rangle$  and  $|1\rangle$ .

**Step 3.6:** Now, the third party Charlie has three classical sequences namely  $R_{14} = \{r_{14}^1, r_{14}^2, \dots, r_{14}^i, \dots, r_{14}^n\}$ ,  $R_{23} = \{r_{23}^1, r_{23}^2, \dots, r_{23}^i, \dots, r_{23}^n\}$  and  $R_5 = \{r_5^1, r_5^2, \dots, r_5^i, \dots, r_5^n\}$ . Charlie then performs the XOR on the bit strings  $R_{14}$  and  $R_{23}$ , that are in the same positions. For the value of  $r_5^i$  as 0 (1), if the XOR outcome is  $r_{14}^i \oplus r_{23}^i = 00$  ( $r_{14}^i \oplus r_{23}^i = 10$ ), then the identity of Alice and Bob is authenticated by Charlie.

**Step 3.7:** Charlie announces publicly the authenticity of Alice and Bob are simultaneously satisfied using an unjammable public channel.

## 4.1 Comparison of the existing and the proposed protocols

Criticisms of many of the existing protocols (including that of the pioneering work of Crépeau et al. [8]) arise from the fact that they are based on the two-party secure multiparty computational (two-party SMC) tasks which are not allowed in the domain of non-relativistic quantum mechanics. To understand this particular shortcoming of a class of protocols, we have to briefly state the important results obtained by Lo in 1997 [112], and Lo and Chau in 1998 [113]. These works essentially established that quantum bit commitment, quantum remote coin tossing<sup>5</sup> and quantum oblivious transform (OT) cannot be performed with unconditional security by using quantum means in two-party scenario. Here, it must be noted that Crépeau et al.'s pioneering protocol [8] of QIA was based on OT, but when it was published then Lo-Chau results were not known. Interestingly, even after the works of Lo and Chau, and many others in the same line [114,115], a large number of schemes for QIA have been proposed using computational tasks which are apparently not allowed to be performed in an unconditionally secure manner by the Lo Chau and similar results. For example, secure quantum private comparison is not allowed in the two-party scenario, but the protocols for QIA have been proposed using the schemes of secure quantum private comparison. The question is whether Lo and Chau results nullify the validity of all such schemes for QIA. The answer is no. Here, we argue, why is it so. Further, the vulnerability of the scheme of Mihara [18] and how to circumvent that is discussed above. In addition, it may be noted that there are many theoretical proposals for QIA which requires quantum memory (for example protocols described in Refs. [9,11–13,16,18,35,37,42,49,51,66,75]). As quantum memory in the true sense is not yet available, these schemes of QIA are not good candidates for practical realization at the moment. Of course, one can circumvent the need of quantum memory to some extent using delay. However, that's a restricted choice. Here it would be apt to note that even

<sup>5</sup>Only a weak version of coin tossing can be implemented using quantum resources.

an effort to implement Protocol 3 proposed here would face this technological hindrance. Another problem associated with the implementation of QIA over long distance is the unavailability of quantum repeaters. In some schemes, like Zhou et al. scheme for QIA [35] entanglement swapping is used to address this issue. However, in such an approach the device in the middle used for entanglement swapping needs to be trusted, which carries with it a security concern.

## 5 Security analysis

Here, we analyze the security of the proposed protocols against some of the commonly discussed attacks by an outsider (Eve). Insider attacks are not relevant in the context of identity authentication and consequently they are not discussed here. To begin with, we will discuss impersonation attack and discuss the security of all the protocols proposed above (against this attack) in a sequential manner.

### 5.1 Impersonation attack

In this kind of attacks, an outsider Eve may try to impersonate the legal user Alice (or Bob) and pass the authentication process. In what follows, we will show that the proposed protocols are not vulnerable under such an attack of Eve.

#### 5.1.1 Security analysis on Protocol 1 against impersonation attack by Eve

Let us consider the situation in which Eve is trying to impersonate Alice. As per the protocol,  $n$  authentication particles are to be inserted in the  $n$ -particle decoy sequence. The probability of Eve to correctly guess the correct authentication state is  $\frac{1}{2}$ . Further, Eve has to correctly guess the position of decoy particle too, and probability of that is also  $\frac{1}{2}$ . Hence the probability of Eve to impersonate Alice is  $(\frac{1}{4})^n$ . So, the probability of detecting Eve's presence is  $P_1 = 1 - (\frac{1}{4})^n$  and for large value of  $n$ , it ( $P_1$ ) tends to 1 (see Fig.(3)). In the case of Eve to impersonate Bob, the situation will be similar to that for impersonating Alice.

#### 5.1.2 Security analysis on Protocol 2 against impersonation attack by Eve

Consider that Eve prepares a  $2n$  random classical sequence and to impersonate Alice, she computes  $k_{2i-1} \oplus k_{2i}$ . Here, probability to get the same result as that of Alice would be  $\frac{1}{2}$ . Additionally, the probability of Eve to prepare the correct state and send them to Bob is  $\frac{1}{2}$ . So, the probability of detecting of Eve's presence would be  $P_2 = 1 - (\frac{1}{4})^n$ . Thus, against this attack Protocol 2 will be as secure as Protocol 1 is.

#### 5.1.3 Security analysis of Protocol 3 against impersonation attack by Eve

Without any loss of generality, we may consider the situation described in Section 4. Eve (impersonating Alice) chooses  $|\phi^+\rangle_{12}$  and sends the particle (particle 2) sequence  $S_{e2}$  to Charlie. Charlie follows the protocol and sends back the sequence  $S_{2e}$  ( $S_4$ ) to Bob (Eve). Eve performs all the steps of protocol as expected from real Alice and for this case will apply Pauli operation  $I$  on the Particle 1. Bob and Eve perform the Bell measurements and Table (7) shows all the possible measurement scenarios that reveals the presence of Eve. As the correct key  $K_{AB}$  is not known to Eve, so the probability of Eve choosing the correct Bell state is  $\frac{1}{4}$  and Eve has to successfully guess all the  $n$  Bell states in order to escape from the security check. So, the probability of successful impersonation attack by Eve is  $(\frac{1}{4})^n$ . If  $n$  is very large, the probability of the success of impersonation attack will

be close to zero. Thus, the probability  $P_3$  to detect the presence of Eve is  $1 - (\frac{1}{4})^n$ . For large  $n$  value the probability  $P_3$  will be approximately 1 and impersonation attack can be identified. It may be noted that  $P_1 = P_2 = P_3 = P(n) = 1 - (\frac{1}{4})^n$ , the relationship between  $P(n)$  and  $n$  is shown in Fig.(3) which clearly shows that the minimum 6, 6 and 10 classical bits information is needed as pre-shared key to detect the Eve's presence for Protocol 1, Protocol 3 and Protocol 2, respectively.

Table 7: The possible measured results

Eve and Bob's possible combined result	Charlie's result	Additional modulo 2
$ \psi^+\rangle_{14} \otimes  \psi^-\rangle_{23}$	$ 0\rangle_5$	$10 \otimes 11 = 01$
$ \psi^-\rangle_{14} \otimes  \psi^+\rangle_{23}$	$ 0\rangle_5$	$11 \otimes 10 = 01$
$ \phi^+\rangle_{14} \otimes  \phi^-\rangle_{23}$	$ 0\rangle_5$	$00 \otimes 01 = 01$
$ \phi^-\rangle_{14} \otimes  \phi^+\rangle_{23}$	$ 0\rangle_5$	$01 \otimes 00 = 01$
$ \psi^+\rangle_{14} \otimes  \phi^-\rangle_{23}$	$ 1\rangle_5$	$10 \otimes 01 = 11$
$ \psi^-\rangle_{14} \otimes  \phi^+\rangle_{23}$	$ 1\rangle_5$	$11 \otimes 00 = 11$
$ \phi^+\rangle_{14} \otimes  \psi^-\rangle_{23}$	$ 1\rangle_5$	$00 \otimes 11 = 11$
$ \phi^-\rangle_{14} \otimes  \psi^+\rangle_{23}$	$ 1\rangle_5$	$01 \otimes 10 = 11$

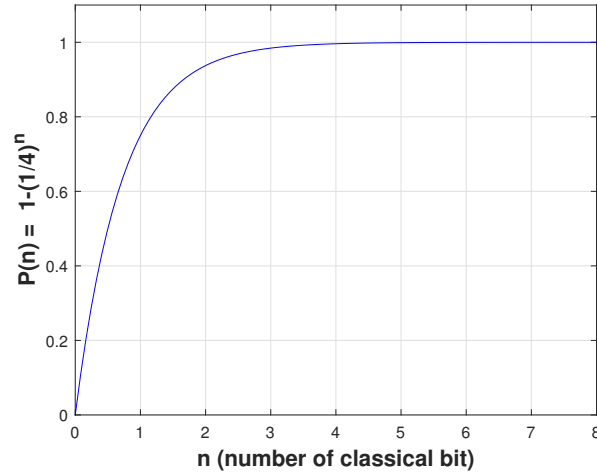


Figure 3: (Color online) The relationship between the probability of detecting of Eve's presence  $P(n)$  and number of using classical bit  $n$ .

## 5.2 Measurement and resend attack

### 5.2.1 Security analysis on Protocol 1 against measure-resend attack

In this attack strategy, Eve will measure the sequence of qubits traveling from Alice to Bob, and send new states to Bob depending upon the measurement result. For Eve to impersonate Alice, it is advisable for Eve to separate decoy qubits from the authentication qubits, but Eve has no information about the position of the decoy states. Consequently, in her effort to implement measure-resend attack, she eventually attacks the information qubits, too and that leads to detectable traces of her presence. To visualize this, let us assume that Eve attacks all the qubits traveling through the channel (the analysis and conclusion will be similar even if she attacks a fraction  $f$  of the traveling qubits). Here, Eve measures all the qubits of the sequence either in  $\{|0\rangle, |1\rangle\}$  basis or in  $\{|+\rangle, |-\rangle\}$



basis randomly (i.e., the probability that a particular basis is used to measure a specific qubit is  $\frac{1}{2}$ ). Before going further, let us calculate mutual information between Alice and Bob for the case of authentication particles under the presence of Eve. Here  $P(B, A)$  is the joint probability for getting measurement result  $B$  by Bob when Alice prepares the state  $A$  and  $P(B)$  be the total probability of getting result in state  $B$  from Bob's measurement.

$$P(B, A) = \begin{cases} \frac{1}{8} & \text{when } B \text{ and } A \text{ are measured in the same basis but different outcomes are obtained} \\ \frac{1}{4} & \text{when } B \text{ and } A \text{ are measured in the same basis and the same outcomes are obtained} \\ 0 & \text{when } B \text{ and } A \text{ are measured in the different basis} \end{cases}$$

and

$$P(B = |0\rangle) = P(B = |-\rangle) = \frac{3}{8}$$

$$P(B = |1\rangle) = P(B = |+\rangle) = \frac{1}{8}$$

where  $A \in \{|0\rangle, |-\rangle\}$  and  $B \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ .

The conditional entropy<sup>6</sup> is  $H(B|A) = \left[2 \times \frac{1}{2} \left(-\frac{3}{4} \log_2 \frac{3}{4} - \frac{1}{4} \log_2 \frac{1}{4}\right)\right] = 0.811278$  bit,  $H(A) = 1$  bit and  $H(B) = 2 \times \left(-\frac{3}{8} \log_2 \frac{3}{8} - \frac{1}{8} \log_2 \frac{1}{8}\right) = 1.811278$  bit. The mutual information between Alice and Bob is  $I(A : B) = H(B) - H(B|A) = 1.0$  bit<sup>7</sup>.

In a similar way, the probabilities for Alice and Eve are

$$P(E, A) = \begin{cases} 0 & \text{when } E \text{ and } A \text{ are measured in the same basis but different outcomes are obtained} \\ \frac{1}{4} & \text{when } E \text{ and } A \text{ are measured in the same basis and the same outcomes are obtained} \\ \frac{1}{8} & \text{when } E \text{ and } A \text{ are measured in the different basis} \end{cases}$$

and

$$P(E = |0\rangle) = P(E = |-\rangle) = \frac{3}{8},$$

$$P(E = |1\rangle) = P(E = |+\rangle) = \frac{1}{8},$$

where  $A \in \{|0\rangle, |-\rangle\}$  and  $E \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ .

The conditional entropy is  $H(E|A) = \left[2 \times \frac{1}{2} \left(-\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{4} \log_2 \frac{1}{4} - \frac{1}{4} \log_2 \frac{1}{4}\right)\right] = 1.5$  bit and  $H(E) = 2 \times \left(-\frac{3}{8} \log_2 \frac{3}{8} - \frac{1}{8} \log_2 \frac{1}{8}\right) = 1.811278$ . The mutual information between Eve and Alice is  $I(A : E) = H(E) - H(E|A) = 0.311278$  bit. Further, we know that the mutual information between Alice and Eve  $I(A : E)$  is restricted by Holevo bound [116] which for this case is 0.600876. We can see that  $I(A : E) \leq 0.600876$  and  $I(A : B) > I(A : E)$ , which implies that Eve's information is considerably lesser than that of Bob.

To impersonate Bob, Eve has to attack the enlarged particle sequence  $K_B$  which is returned by Bob. This scenario is the same as that required for impersonating Alice.

<sup>6</sup>Conditional probability,  $P(B = |i\rangle|A = |j\rangle) = \frac{P(B=|i\rangle, A=|j\rangle)}{P(A=|j\rangle)}$  and conditional entropy,  $H(B|A) = -\sum_j P(A = |j\rangle) \sum_i P(B = |i\rangle|A = |j\rangle) \log_2 P(B = |i\rangle|A = |j\rangle)$ .

<sup>7</sup>The mutual information between two parties is bounded by the Shannon entropy of probability distributions for a single particle, i.e.,  $0 \leq I(A : B) \leq \min[H(A), H(B)]$  as  $H(A, B) := [\max[H(A), H(B)], H(A) + H(B)]$ , and  $I(A : B) := H(A) + H(B) - [\max[H(A), H(B)], H(A) + H(B)]$ , so  $I(A : B) := [0, \min[H(A), H(B)]]$ .

### 5.2.2 Security analysis on Protocol 2 against measure-resend attack

Eve performs a random measurement on particles sent by Alice and gets some outcomes. Similar to Protocol 1, we can compute the mutual information between Alice and Bob as

$$P(B, A) = \frac{1}{16} + \frac{1}{8}\delta_{A,B} \text{ and } P(B = |0\rangle) = P(B = |+\rangle) = (B = |1\rangle) = P(B = |-\rangle) = \frac{1}{4},$$

$\delta_{A,B} = 1(0)$  when the measurement outcomes of Alice and Bob are the same (different) using the same basis.

The conditional entropy will be  $H(B|A) = \frac{1}{4} \left[ 4 \times \left( -\frac{3}{4} \log_2 \frac{3}{4} \right) + 4 \times \left( -\frac{1}{4} \log_2 \frac{1}{4} \right) \right] = 0.81127$  bit and  $H(A) = H(B) = 4 \times \left[ -\frac{1}{4} \log_2 \frac{1}{4} \right] = 2$  bits. The mutual information between Alice and Bob is  $I(A : B) = H(B) - H(B|A) = 1.18872$  bit which is more than one because they have already identical classical information as pre-shared key.

For mutual information between Alice and Eve,

$$P(E, A) = \begin{cases} 0 & \text{when } E \text{ and } A \text{ are measured in the same basis but different outcomes are obtained} \\ \frac{1}{8} & \text{when } E \text{ and } A \text{ are measured in the same basis and the same outcomes are obtained} \\ \frac{1}{16} & \text{when } E \text{ and } A \text{ are measured in the different basis} \end{cases}$$

and

$$P(E = |0\rangle) = P(E = |1\rangle) = P(E = |+\rangle) = P(E = |-\rangle) = \frac{1}{4}.$$

So, conditional entropy is  $H(E|A) = \frac{1}{4} \times [8 \times (-\frac{1}{4} \log_2 \frac{1}{4}) - 4 \times (-\frac{1}{2} \log_2 \frac{1}{2})] = 1.5$  bit and  $H(E) = 4 \times [-\frac{1}{4} \log_2 \frac{1}{4}] = 2$  bits. The mutual information between Eve and Alice is  $I(A : E) = H(E) - H(E|A) = 0.5$  bit. Further, we know that the mutual information between Alice and Eve,  $I(A : E)$  is bound by Holevo quantity [116] which is 1 in this case. We can see that  $I(A : E) \leq 1$  and  $I(A : B) > I(A : E)$ , which satisfies the requirement for a secure communication without disclosing meaningful information to Eve. Similar are the results for the case when Eve tries to impersonate Bob.

### 5.2.3 Security analysis on Protocol 3 against measurement and resend attack

In this protocol, Alice and Bob prepares the Bell states depending upon their pre-shared secret key. Alice and Bob both do not dispatch their quantum states as a whole. So Eve has to attack only one particle at a time. Without loss of generality, we consider that Eve will attack Particle 2 (Particle 4) when Alice sends it to Charlie (Charlie sends it to Alice). Eve may extract the maximum information from the quantum channel which is restricted by Holevo bound or Holevo quantity [116]

$$\chi(\rho) = S(\rho) - \sum_i p_i S(\rho_i), \quad (8)$$

Where  $S(\rho) = -Tr(\rho \log_2 \rho)$  is the von Neumann entropy,  $\rho_i$  is a component in the mixed state  $\rho$  with probability  $p_i$ . We have already discussed that Eve will attack on Particle 2 (4), for this situation (8) can be rewritten as:

$$\chi(\rho_2) = S(\rho_2) - \sum_i p_i S(\rho_{2_i}) \quad (9)$$

where  $\rho_2$  and  $\rho_{2_i}$  are the reduced density matrix of  $\rho$  and  $\rho_i$  respectively after partial trace over 1, 4, 3, 5 particles. From (5), we can write  $\rho = [|\Psi\rangle\langle\Psi|]_{14235}$ . The reduced density matrix for Particle 2 (4) always has the form,

$$\rho_2 = Tr_{1435} (|\Psi\rangle\langle\Psi|)_{14235} = \frac{1}{2}I$$

and  $\rho_{2_i}$  will be the corresponding reduced density matrix. The probability of choosing another combination of authentication key by Alice and Bob is  $\frac{1}{4}$  i.e., here  $p_i = \frac{1}{4}$ . Here, also  $\rho_{2_i} = \frac{1}{2}I$ . Substituting  $\rho_2$  and  $\rho_{2_i}$  into (9) gives,  $\chi(\rho_2) = 0$ . Similar result can be obtained for Particle 4. This result implies Eve cannot get any information in direct measurement attack on Particle 2 (and 4).

### 5.3 Impersonated fraudulent attack

#### 5.3.1 Security analysis on Protocol 1 against impersonated fraudulent attack strategy by forging new qubits

Here, Eve tries to impersonate Alice by introducing a unitary operation  $U_E$  to correlate Alice's qubit with an ancilla qubit. After application of unitary operator, the quantum state can be written as

$$U_E|0\chi\rangle_{Ae} = |\psi\rangle_0 = a_0|00\rangle + b_0|01\rangle + c_0|0+\rangle + d_0|0-\rangle,$$

$$U_E|1\chi\rangle_{Ae} = |\psi\rangle_1 = a_1|10\rangle + b_1|11\rangle + c_1|1+\rangle + d_1|1-\rangle,$$

$$U_E|+\chi\rangle_{Ae} = |\psi\rangle_+ = a_+|+0\rangle + b_+|+1\rangle + c_+|++\rangle + d_+|+-\rangle,$$

$$U_E|-\chi\rangle_{Ae} = |\psi\rangle_- = a_-| - 0\rangle + b_-| - 1\rangle + c_-| - +\rangle + d_-| - -\rangle.$$

So, we obtain the entire state as,

$$|\rho\rangle = \frac{1}{4} (|\psi\rangle_{00}\langle\psi| + |\psi\rangle_{11}\langle\psi| + |\psi\rangle_{++}\langle\psi| + |\psi\rangle_{--}\langle\psi|). \quad (10)$$

The probability of getting the correct measurement result for each state of authentication sequence as well as the decoy sequence by Bob is  $\frac{1}{2}$ . Suppose, we take the correct state as  $|0\rangle$ , then the probability of detecting Eve is  $P_0 = \frac{1}{2}$ . Similarly, we obtain  $P_1 = P_+ = P_- = \frac{1}{2}$ . The detection possibility for each qubit is  $P_d = \frac{1}{4}(P_0 + P_1 + P_+ + P_-) = \frac{1}{2}$ . According to the Simmons theory [117], the protocol is unconditionally secure under impersonated fraudulent attack using (10).

#### 5.3.2 Security analysis on Protocol 2 against impersonated fraudulent attack strategy by forging new qubits

In this protocol, Alice only uses the authentication state in the computational and Hadamard basis with equal probability and the expected measurement result by Bob also equally probable. So, the attack situation is similar to the Protocol 1. In this context, Protocol 2 is also secure under the impersonated fraudulent attack.

### 5.3.3 Security analysis on Protocol 3 against impersonated fraudulent attack strategy by forging new qubits

To impersonate Alice, an optimal strategy by Eve is to operate the traveling particle (particle 2) sent by Alice with her ancillary state. After operating the general operation with traveling particle, the state can be denoted as follows,

$$U_E|1\chi\rangle_{2e} = (a_0|10\rangle + b_0|11\rangle + c_0|00\rangle + d_0|01\rangle)_{2e}, \quad (11)$$

$$U_E|0\chi\rangle_{2e} = (a_1|10\rangle + b_1|11\rangle + c_1|00\rangle + d_1|01\rangle)_{2e}, \quad (12)$$

Here,  $|\chi\rangle_e$  is the ancillary state which is created by Eve, the subscript  $e$  refers to state prepared by Eve and 2 refers the traveling particle of Alice. For normalization  $|a_0|^2 + |b_0|^2 + |c_0|^2 + |d_0|^2 = |a_1|^2 + |b_1|^2 + |c_1|^2 + |d_1|^2 = 1$ .

Eve's operation creates the following state,

$$|\Psi'\rangle_{12e} = \frac{1}{\sqrt{2}} (a_0|010\rangle + b_0|011\rangle + c_0|000\rangle + d_0|001\rangle + a_1|110\rangle + b_1|111\rangle + c_1|100\rangle + d_1|101\rangle) \quad (13)$$

For simplicity, Eve employs a general operation on the traveling particle and keep her own qubit with herself and sends the Alice's particle to Charlie. Charlie does the necessary operation and returns this particle according to protocol. Here we aim to calculate the final composite state after consideration of Eve's attack along with the scenario described in Section 4 as follows,

$$\begin{aligned} |\Psi''\rangle_{12e345} &= \frac{1}{2\sqrt{2}} [a_0|110110\rangle - a_0|100111\rangle - a_0|110000\rangle + a_0|100001\rangle \\ &+ b_0|111110\rangle - b_0|101111\rangle - b_0|111000\rangle + b_0|101001\rangle \\ &- c_0|100110\rangle - c_0|110111\rangle - c_0|100000\rangle + c_0|110001\rangle \\ &+ d_0|101110\rangle - d_0|111111\rangle - d_0|101000\rangle + d_0|111001\rangle \\ &- a_1|010110\rangle + a_1|000111\rangle + a_1|010000\rangle + a_1|000001\rangle \\ &- b_1|011110\rangle + b_1|001111\rangle + b_1|011000\rangle - b_1|001001\rangle \\ &- c_1|000110\rangle + c_1|010111\rangle + c_1|000000\rangle - c_1|010001\rangle \\ &- d_1|001110\rangle + d_1|011111\rangle + d_1|001000\rangle - d_1|011001\rangle] \end{aligned} \quad (14)$$

After receiving the particle 4 from Charlie, Eve and Bob perform the Bell measurement on their particles that they have and sends the classical sequence of measurement result to Charlie. By applying the authentication condition, we can easily find the success probability and the failure probability of Eve to pass the authentication is  $\frac{1}{4}(|b_0|^2 + |c_0|^2) + \frac{1}{8}$  and  $\frac{1}{4}(|a_0|^2 + |d_0|^2 + 1) + \frac{3}{8}$  respectively. Suppose that Eve prepares the ancillary state such that the value of  $|b_0|^2 + |c_0|^2$  will be maximum and the value of  $|a_0|^2 + |d_0|^2$  will be minimum, then she can deceives maximally as an authenticated member with probability  $P_3^2 = \frac{3}{8}$ . For rest of the cases,  $P_3^2 \leq \frac{3}{8}$ . From this discussion, it can be concluded that the protocol is secure under some acceptable error limit for the best case scenario of collective attack by Eve.

## 6 Conclusions

We have reviewed the existing protocols for QIA with an intention to understand the intrinsic symmetry among them. The analysis has revealed the symmetry among various protocols and that has helped us in classifying the existing protocols for QIA and to identify various simple strategies which may be used to transform the existing protocols for different quantum computation and communication tasks into new schemes for QIA. To establish this point, a few new protocols for QIA are also

proposed and established to be secure against a set of potential attacks. Interestingly, among the protocols discussed above (including the existing and the newly proposed protocols) all are not really implementable with the present technology. For example, there are several protocols where one of the users need to keep a photon (for example, consider ping-pong type scheme for QIA described in [14] or the authentication schemes described in [11–13, 16, 18, 35, 51, 75]) with him/her until travel photon(s) is (are) returned to him/her. Such protocols of QIA would require quantum memory which is not available at this moment. In fact, most of the entangled state based QSDC type protocols for QIA and entangled state based protocols which are based on schemes for quantum private comparison and the schemes for QIA involving a third party, Trent who keeps a photon with himself, will face the same problem. Thus, at the moment, protocols for QIA which does not require quantum memory should be preferred. There are many proposals for building quantum memory and these schemes (schemes requiring quantum memory) may be useful in future, but direct teleportation based schemes for QIA (e.g., schemes proposed in [35, 51]) are not expected to find many applications, even in future. This is so because teleportation can be directly used for secure quantum communication only when the quantum channel is noise free. Further, any scheme that requires shared entanglement (e.g., schemes described in [11, 13, 18, 30, 31, 35]) may require entanglement purification or concentration (as the shared entanglement will disintegrate due to decoherence) which in turn would require unwanted and unsafe interaction between Alice and Bob. Despite these limitations and technological issues, the domain of QIA related research is growing fast because the claimed unconditional security of quantum cryptography schemes is also based on the security of identity authentication scheme used.

This review would remain incomplete, unless we mention that a large number of post-quantum authentication schemes [118, 119] have also been proposed in the recent past. We have not discussed those schemes as they are classical in nature and conditionally secure. A very strong assumption behind these schemes is that a quantum computer will not be able to efficiently solve problems outside bounded-error quantum polynomial time (BQP) complexity class. There is no such proof and this assumption is technically equivalent to presuppose that if we don't know any efficient algorithm for a given computational task at the moment, no one will be able to construct that in future, too.

## Acknowledgment:

The authors thank DRDO India for the support provided through the project number ANURAG/MMG / CARS/2018-19/071. The authors also thank Dr. Kishore Thapliyal and Dr. Sandeep Mishra for their interest and technical feedback on this work.

## References

- [1] David P DiVincenzo and Daniel Loss. Quantum computers and quantum coherence. *Journal of Magnetism and Magnetic Materials*, 200(1-3):202–218, 1999.
- [2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing, in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India, 1984), pp. 175-179., 1984.
- [3] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.
- [4] Gilles Brassard. Brief history of quantum cryptography: A personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 19–23. IEEE, 2005.

- [5] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661, 1991.
- [6] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.
- [7] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.
- [8] Claude Crépeau and Louis Salvail. Quantum oblivious mutual identification. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 133–146. Springer, 1995.
- [9] Guihua Zeng and Xinmei Wang. Quantum key distribution with authentication. *arXiv preprint quant-ph/9812022*, 1998.
- [10] Miloslav Dušek, Ondřej Haderka, Martin Hendrych, and Robert Myška. Quantum identification system. *Physical Review A*, 60(1):149, 1999.
- [11] Xiaoyu Li and Howard Barnum. Quantum authentication using entangled states. *International Journal of Foundations of Computer Science*, 15(04):609–617, 2004.
- [12] Jian WANG, Quan ZHANG, and Chao-Jing TANG. Multiparty simultaneous quantum identity authentication based on entanglement swapping. *Chinese Physics Letters*, 23(9):2360–2363, 2006.
- [13] Yong-Sheng Zhang, Chuan-Feng Li, and Guang-Can Guo. Quantum authentication using entangled state. *arXiv preprint quant-ph/0008044*, 2000.
- [14] Zheshen Zhang, Guihua Zeng, Nanrun Zhou, and Jin Xiong. Quantum identity authentication based on ping-pong technique for photons. *Physics Letters A*, 356(3):199–205, 2006.
- [15] Shun Zhang, Zhang-Kai Chen, Run-Hua Shi, and Feng-Yu Liang. A novel quantum identity authentication based on Bell states. *International Journal of Theoretical Physics*, 59(1):236–249, 2020.
- [16] 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(7):159, 2018.
- [17] Yan Chang, Chunxiang Xu, Shibin Zhang, and Lili Yan. Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *Chinese Science Bulletin*, 59(21):2541–2546, 2014.
- [18] Takashi Mihara. Quantum identification schemes with entanglements. *Physical Review A*, 65(5):052326, 2002.
- [19] Preeti Yadav, R Srikanth, and Anirban Pathak. Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. *Quantum Information Processing*, 13(12):2731–2743, 2014.
- [20] Chitra Shukla, Vivek Kothari, Anindita Banerjee, and Anirban Pathak. On the group-theoretic structure of a class of quantum dialogue protocols. *Physics Letters A*, 377(7):518–527, 2013.

- [21] Chitra Shukla and Anirban Pathak. Orthogonal-state-based deterministic secure quantum communication without actual transmission of the message qubits. *Quantum Information Processing*, 13(9):2099–2113, 2014.
- [22] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.
- [23] Howard N Barnum. Quantum secure identification using entanglement and catalysis. *arXiv preprint quant-ph/9910072*, 1999.
- [24] Ritajit Majumdar and Sanchari Das. Sok: An evaluation of quantum authentication through systematic literature review. In *Proceedings of the Workshop on Usable Security and Privacy (USEC)*, 2021.
- [25] Daniel Ljunggren, Mohamed Bourenmane, and Anders Karlsson. Authority-based user authentication in quantum key distribution. *Physical Review A*, 62(2):022305, 2000.
- [26] Guihua Zeng and Guangcan Guo. Quantum authentication protocol. *arXiv preprint quant-ph/0001046*, 2000.
- [27] Jens G Jensen and Ruediger Schack. Quantum authentication and key distribution using catalysis. *arXiv preprint quant-ph/0003104*, 2000.
- [28] N Srinatha, S Omkar, R Srikanth, Subhashish Banerjee, and Anirban Pathak. The quantum cryptographic switch. *Quantum Information Processing*, 13(1):59–70, 2014.
- [29] Kishore Thapliyal and Anirban Pathak. Applications of quantum cryptographic switch: various tasks related to controlled quantum communication can be performed using Bell states and permutation of particles. *Quantum Information Processing*, 14(7):2599–2616, 2015.
- [30] Marcos Curty and David J Santos. Quantum authentication of classical messages. *Physical Review A*, 64(6):062309, 2001.
- [31] Marcos Curty, David J Santos, Esther Pérez, and Priscila García-Fernández. Qubit authentication. *Physical Review A*, 66(2):022301, 2002.
- [32] Wim van Dam. Comment on "Quantum identification schemes with entanglements". *Physical Review A*, 68(2):026301, 2003.
- [33] Rishi Dutt Sharma, Kishore Thapliyal, Anirban Pathak, Alok Kumar Pan, and Asok De. Which verification qubits perform best for secure communication in noisy channel? *Quantum Information Processing*, 15(4):1703–1718, 2016.
- [34] Anirban Pathak. *Elements of quantum computation and quantum communication*. CRC Press Boca Raton, 2013.
- [35] Nanrun Zhou, Guihua Zeng, Wenjie Zeng, and Fuchen Zhu. Cross-center quantum identification scheme based on teleportation and entanglement swapping. *Optics Communications*, 254(4-6):380–388, 2005.
- [36] M Peev, M Nölle, O Maurhardt, T Lorünser, M Suda, A Poppe, R Ursin, A Fedrizzi, and Anton Zeilinger. A novel protocol-authentication algorithm ruling out a man-in-the-middle attack in quantum cryptography. *International Journal of Quantum Information*, 3(01):225–231, 2005.

- [37] Hwayean Lee, Jongin Lim, and HyungJin Yang. Quantum direct communication with authentication. *Physical Review A*, 73(4):042305, 2006.
- [38] Kim Boström and Timo Felbinger. Deterministic secure direct communication using entanglement. *Physical Review Letters*, 89(18):187902, 2002.
- [39] Zhan-jun Zhang, Jun Liu, Dong Wang, and Shou-hua Shi. Comment on "Quantum direct communication with authentication". *Physical Review A*, 75(2):026301, 2007.
- [40] Yang Yu-Guang and Wen Qiao-Yan. Economical multiparty simultaneous quantum identity authentication based on Greenberger–Horne–Zeilinger states. *Chinese Physics B*, 18(8):3233, 2009.
- [41] Stefan Rass, Peter Schartner, and Michaela Greiler. Quantum coin-flipping-based authentication. In *2009 IEEE International Conference on Communications*, pages 1–5. IEEE, 2009.
- [42] Liu Dan, Pei Chang-Xing, Quan Dong-Xiao, and Zhao Nan. A new quantum secure direct communication scheme with authentication. *Chinese Physics Letters*, 27(5):050306, 2010.
- [43] Peng Huang, JUN Zhu, Yuan Lu, and Gui-Hua Zeng. Quantum identity authentication using gaussian-modulated squeezed states. *International Journal of Quantum Information*, 9(02):701–721, 2011.
- [44] Chang-Qing Gong, Hu Tang, and Da-Wei Zhang. Identity authentication and key distribution protocol based on quantum one-way function. *Computer Engineering*, 38(6):161–160, 2012.
- [45] Robert Gelfond and Audrius Berzanskis. Key management and user authentication for quantum cryptography networks, December 25 2012.
- [46] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.
- [47] Sebastianus A Goorden, Marcel Horstmann, Allard P Mosk, Boris Škorić, and Pepijn WH Pinkse. Quantum-secure authentication of a physical unclonable key. *Optica*, 1(6):421–424, 2014.
- [48] Thomas Ziola, Zdenek Paral, Srinivas Devadas, Gookwon Edward Suh, and Vivek Khandelwal. Authentication with physical unclonable functions, July 15 2014.
- [49] Yu-Guang Yang, Ju Tian, Juan Xia, and Hua Zhang. Quantum authenticated direct communication using Bell states. *International Journal of Theoretical Physics*, 52(2):336–344, 2013.
- [50] Kishore Thapliyal, Amit Verma, and Anirban Pathak. A general method for selecting quantum channel for bidirectional controlled state teleportation and other schemes of controlled quantum communication. *Quantum Information Processing*, 14(12):4601–4614, 2015.
- [51] Xiaoqing Tan and Lianxia Jiang. Identity authentication by entanglement swapping in controlled quantum teleportation. *International Journal of Embedded Systems 4*, 6(1):3–13, 2014.
- [52] Wei-Min Shi, Yi-Hua Zhou, and Yu-Guang Yang. Quantum deniable authentication protocol. *Quantum Information Processing*, 13(7):1501–1510, 2014.
- [53] Hao Yuan, Yi-min Liu, Guo-zhu Pan, Gang Zhang, Jun Zhou, and Zhan-jun Zhang. Quantum identity authentication based on ping-pong technique without entanglements. *Quantum Information Processing*, 13(11):2535–2549, 2014.



- [54] Marco Lucamarini and Stefano Mancini. Secure deterministic communication without entanglement. *Physical Review Letters*, 94(14):140501, 2005.
- [55] Hong Lai, Jinghua Xiao, Mehmet A Orgun, Liyin Xue, and Josef Pieprzyk. Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes. *Quantum Information Processing*, 13(4):895–907, 2014.
- [56] Wei-Min Shi, Jian-Biao Zhang, Yi-Hua Zhou, and Yu-Guang Yang. A novel quantum deniable authentication protocol without entanglement. *Quantum Information Processing*, 14(6):2183–2193, 2015.
- [57] Hongxin Ma, Peng Huang, Wansu Bao, and Guihua Zeng. Continuous-variable quantum identity authentication based on quantum teleportation. *Quantum Information Processing*, 15(6):2605–2620, 2016.
- [58] Feihu Xu, Marcos Curty, Bing Qi, Li Qian, and Hoi-Kwong Lo. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nature Photonics*, 9(12):772–773, 2015.
- [59] Stefan Rass, Sandra König, Stefan Schauer, and Oliver Maurhart. Implementation and evaluation of intrinsic authentication in quantum key distribution protocols. *International Journal on Advances in Security*, 9(1), 2016.
- [60] Boris Škorić. Quantum readout of physical unclonable functions. *International Journal of Quantum Information*, 10(01):1250001, 2012.
- [61] Yao Yao, Ming Gao, Mo Li, and Jian Zhang. Quantum cloning attacks against puf-based quantum authentication systems. *Quantum Information Processing*, 15(8):3311–3325, 2016.
- [62] Boris Škorić, Allard P Mosk, and Pepijn WH Pinkse. Security of quantum-readout pufs against quadrature-based challenge-estimation attacks. *International Journal of Quantum Information*, 11(04):1350041, 2013.
- [63] Patrick Hayden, Debbie W Leung, and Dominic Mayers. The universal composable security of quantum message authentication with key recycling. *arXiv preprint arXiv:1610.09434*, 2016.
- [64] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.
- [65] Chang ho Hong, Jino Heo, Jin Gak Jang, and Daesung Kwon. Quantum identity authentication with single photon. *Quantum Information Processing*, 16(10):236, 2017.
- [66] Hussein Abulkasim, Safwat Hamad, Amal Khalifa, and Khalid El Bahnasy. Quantum secret sharing with identity authentication based on Bell states. *International Journal of Quantum Information*, 15(04):1750023, 2017.
- [67] Georgios M Nikolopoulos and Eleni Diamanti. Continuous-variable quantum authentication of physical unclonable keys. *Scientific Reports*, 7:46047, 2017.
- [68] Christopher Portmann. Quantum authentication with key recycling. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 339–368. Springer, 2017.

- [69] Richard John Hughes, Charles Glen Peterson, James T Thrasher, Jane E Nordholt, Jon T Yard, Raymond Thorson Newell, and Rolando D Somma. Multi-factor authentication using quantum communication, February 6 2018.
- [70] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical Bob. *Physical Review Letters*, 99(14):140501, 2007.
- [71] Chitra Shukla, Kishore Thapliyal, and Anirban Pathak. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Information Processing*, 16(12):295, 2017.
- [72] Kishore Thapliyal, Rishi Dutt Sharma, and Anirban Pathak. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. *International Journal of Quantum Information*, 16(05):1850047, 2018.
- [73] Sandeep Mishra, Kishore Thapliyal, Abhishek Parakh, and Anirban Pathak. Quantum anonymous veto: A set of new protocols. *arXiv preprint arXiv:2109.06260*, 2021.
- [74] Pramod Asagodu, Kishore Thapliyal, and Anirban Pathak. Quantum and semi-quantum sealed-bid auction: Vulnerabilities and advantages. *arXiv preprint arXiv:2108.06388*, 2021.
- [75] Xiao-Jun Wen, Xing-Qiang Zhao, Li-Hua Gong, and Nan-Run Zhou. A semi-quantum authentication protocol for message and identity. *Laser Physics Letters*, 16(7):075206, 2019.
- [76] Bin Liu, Zhifeng Gao, Di Xiao, Wei Huang, Zhiqing Zhang, and Bingjie Xu. Quantum identity authentication in the counterfactual quantum key distribution protocol. *Entropy*, 21(5):518, 2019.
- [77] Xiao-yi Zheng and Yin-xiang Long. Controlled quantum secure direct communication with authentication protocol based on five-particle cluster state and classical xor operation. *Quantum Information Processing*, 18(5):129, 2019.
- [78] Prosanta Gope and Tzonelih Hwang. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Transactions on Industrial Electronics*, 63(11):7124–7132, 2016.
- [79] Chang Yan, Zhang Shi-Bin, Yan Li-Li, and Han Gui-Hua. Robust quantum secure direct communication and authentication protocol against decoherence noise based on six-qubit df state. *Chinese Physics B*, 24(5):050307, 2015.
- [80] Zhiguo Qu, Xinzhu Liu, and Shengyao Wu. Quantum identity authentication protocol based on three-photon quantum error avoidance code in edge computing. *Transactions on Emerging Telecommunications Technologies*, page e3945, 2020.
- [81] Min Xiao and Shumei Lei. Quantum private query with authentication. *Quantum Information Processing*, 20(5):166, 2021.
- [82] Nayana Das, Goutam Paul, and Ritajit Majumdar. Quantum secure direct communication with mutual authentication using a single basis. *arXiv preprint arXiv:2101.03577*, 2021.
- [83] Piotr Zawadzki. Quantum identity authentication without entanglement. *Quantum Information Processing*, 18(1):7, 2019.

- [84] Carlos E González-Guillén, María Isabel González Vasco, Floyd Johnson, and Ángel L Pérez del Pozo. An attack on zawadzki’s quantum authentication scheme. *Entropy*, 23(4):389, 2021.
- [85] H Shelton Jacinto, A Matthew Smith, and Nader I Raffla. Utilizing a fully optical and reconfigurable puf as a quantum authentication mechanism. *OSA Continuum*, 4(2):739–747, 2021.
- [86] Mina Doosti, Niraj Kumar, Mahshid Delavar, and Elham Kashefi. Client-server identification protocols with quantum puf. *ACM Transactions on Quantum Computing*, 2(3):1–40, 2021.
- [87] Koustubh Phalak, Abdullah Ash-Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh. Quantum puf for security and trust in quantum computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 11(2):333–342, 2021.
- [88] Hongfeng Zhu, Liwei Wang, and Yuanle Zhang. An efficient quantum identity authentication key agreement protocol without entanglement. *Quantum Information Processing*, 19(10):381, 2020.
- [89] Marcin Sobota, Adrian Kapczyński, and Arkadiusz 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*, volume 2, pages 799–802. IEEE, 2011.
- [90] S Srikara, Kishore Thapliyal, and Anirban Pathak. Continuous variable direct secure quantum communication using gaussian states. *Quantum Information Processing*, 19(4):132, 2020.
- [91] Anindita Banerjee and Anirban Pathak. Maximally efficient protocols for direct secure quantum communication. *Physics Letters A*, 376(45):2944–2950, 2012.
- [92] Stefano Pirandola, Samuel L. Braunstein, Stefano Mancini, and Seth Lloyd. Quantum direct communication with continuous variables. *EPL (Europhysics Letters)*, 84(2):20013, oct 2008.
- [93] Xiaoyu Li and Liju Chen. Quantum authentication protocol using Bell state. In *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*, pages 128–132. IEEE, 2007.
- [94] Hoi-Kwong Lo and Hoi Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.
- [95] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 449–458. IEEE, 2002.
- [96] YuGuang Yang, Qiaoyan Wen, and Xing Zhang. Multiparty simultaneous quantum identity authentication with secret sharing. *Science in China Series G: Physics, Mechanics and Astronomy*, 51(3):321–327, 2008.
- [97] Hussein Abulkasim, Safwat Hamad, Khalid El Bahnasy, and Saad Z Rida. Authenticated quantum secret sharing with quantum dialogue based on Bell states. *Physica Scripta*, 91(8):085101, 2016.
- [98] Run-Hua Shi. Useful equations about Bell states and their applications to quantum secret sharing. *IEEE Communications Letters*, 24(2):386–390, 2019.

- [99] Aihan Yin and Tong Chen. Authenticated semi-quantum secret sharing based on GHZ-type states. *International Journal of Theoretical Physics*, 60(1):265–273, 2021.
- [100] Anindita Banerjee, Chitra Shukla, Kishore Thapliyal, Anirban Pathak, and Prasanta K Panigrahi. Asymmetric quantum dialogue in noisy environment. *Quantum Information Processing*, 16(2):49, 2017.
- [101] Gan Gao, Yue Wang, Dong Wang, and Liu Ye. Comment on "Authenticated quantum secret sharing with quantum dialogue based on Bell states". *Physica Scripta*, 93(2):027002, 2018.
- [102] Hussein Abulkasim, Safwat Hamad, and Ahmed Elhadad. Reply to comment on "Authenticated quantum secret sharing with quantum dialogue based on Bell states". *Physica Scripta*, 93(2):027001, 2018.
- [103] Andrew M. Childs. Secure assisted quantum computation. *Quantum Information and Computation*, 5(6):456–466, 2005.
- [104] Qin Li, Zhulin Li, Wai Hong Chan, Shengyu Zhang, and Chengdong Liu. Blind quantum computation with identity authentication. *Physics Letters A*, 382(14):938–941, 2018.
- [105] Junyu Quan, Qin Li, Chengdong Liu, Jinjing Shi, and Yu Peng. A simplified verifiable blind quantum computing protocol with quantum input verification. *Quantum Engineering*, 3(1):e58, 2021.
- [106] Rui-Ting Shan, Xiubo Chen, and Kai-Guo Yuan. Multi-party blind quantum computation protocol with mutual authentication in network. *Science China Information Sciences*, 64(6):162302, 2021.
- [107] Wei Li, Ronghua Shi, and Ying Guo. Blind quantum signature with blind quantum computation. *International Journal of Theoretical Physics*, 56(4):1108–1115, 2017.
- [108] Zhiguo Qu, Xinzhu Liu, and Shengyao Wu. Quantum identity authentication protocol based on three-photon quantum error avoidance code. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 471–475. IEEE, 2019.
- [109] Ashwin Saxena, Kishore Thapliyal, and Anirban Pathak. Continuous variable controlled quantum dialogue and secure multiparty quantum computation. *International Journal of Quantum Information*, 18(04):2050009, 2020.
- [110] Claude Crépeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. In *Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*, pages 643–652, 2002.
- [111] Anindita Banerjee, Kishore Thapliyal, Chitra Shukla, and Anirban Pathak. Quantum conference. *Quantum Information Processing*, 17(7):161, 2018.
- [112] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154, 1997.
- [113] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

- [114] Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters*, 109(16):160501, 2012.
- [115] Roger Colbeck. Impossibility of secure two-party classical computation. *Physical Review A*, 76(6):062308, 2007.
- [116] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.
- [117] Gustavus J Simmons. A survey of information authentication. *Proceedings of the IEEE*, 76(5):603–620, 1988.
- [118] Liu-Jun Wang, Kai-Yi Zhang, Jia-Yong Wang, Jie Cheng, Yong-Hua Yang, Shi-Biao Tang, Di Yan, Yan-Lin Tang, Zhen Liu, Yu Yu, Qiang Zhang, and Jian-Wei Pan. Experimental authentication of quantum key distribution with post-quantum cryptography. *npj Quantum Information*, 7(1):67, 2021.
- [119] Mark A. Mendiola, James. T. Gillis, Andrew J. Binder, and Ranwa Haddad. Post-quantum authentication schemes. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pages 3812–3825, 2020.