

A QUANTUM BASED CHALLENGE-RESPONSE USER AUTHENTICATION SCHEME OVER NOISELESS CHANNEL

Abudhahir Buhari¹, Zuriati Ahmad Zukarnain¹, Shamala K. Subramaniam¹,
Hisham Zainuddin² and Suhairi Saharudin³

¹FSKTM, University Putra Malaysia, Serdang, Malaysia
toabu@hotmail.com, zuriati@fsktm.upm.edu.my, shamala@fsktm.upm.edu.my

²INSPEN, University Putra Malaysia, Serdang, Malaysia
hisham@fsas.upm.edu.my

³MIMOS, Technology Park Malaysia, Kuala Lumpur, Malaysia
Suhairi.sh@mimos.my

ABSTRACT

In this paper, we propose a quantum user authentication protocol with a single photon based on short shared secret key and quantum bit error ratio verification. In this scheme, usage of proposed deterministic quantum key distribution technique and simple verification in a public channel culminate reduced photon transmission. Security's analysis proves proposed scheme is resistant to impostors' attacks and eavesdropper. Furthermore, proposed protocol can extend to multiparty environment and permits to re-use many times of the shared secret key without revealing it.

KEYWORDS

Quantum User Authentication, Challenge-Response Quantum Authentication, Single Photon Quantum Key Distribution, Quantum Cryptography

1. INTRODUCTION

Recently, there have been many published works on information security techniques based on quantum physics. Quantum Cryptography (QC) [1] is a promising technology for providing unconditional security. There are many active researches with a different purpose on QC variants, i.e. Quantum Key Distribution (QKD), quantum secret sharing, quantum bit commitment, quantum data hiding and more security schemes. One standard cryptographic task is authentication. This is an important task to be done prior to communication that guarantees that the user identification and the origin of data is genuine because, if a malicious user masquerade as a legitimate user, the key distribution schemes and encryption schemes will be easily compromised.

Conventional or digital cryptography which is widely used in computer networks relies on computational complexity. In other words, dawn of the quantum computer with the quantum algorithms culminates at the end of digital cryptography. Nevertheless, QC can provide unconditional security, especially by its property no-cloning theorem and Heisenberg's uncertainty principle. Quantum based security schemes can classify into two major divisions called single photon and entangled photon. A quantum entangled state is a correlated state between two particles such that result of measurement on one particle affects the state of other particles that is physically separated from the measured particle. QKD is a mature field in both theoretical and practical research. QKD is an active research with versatile applications.

However, impersonation or man-in-middle attack makes QKD vulnerable. Furthermore, authentication task in quantum cryptography is tedious due to its level of complexity.

Researches in quantum authentication can be divided into two types namely quantum user authentication and quantum message authentication [2-4]. Recently many advances have been made in quantum authentication for messages and user identification. We classified most of the existing quantum authentication protocols techniques into five major divisions. Table 1. shows quantum authentication's core idea and its derivatives.

Table 1. Classification of quantum authentication schemes.

Third Party or Arbitrator [5] -[6]	Entanglement [7], [8], [9][10],11],12]	Hybrid [13]	Hash Functions [14]	Single Photon [15], [16],[17]
<ul style="list-style-type: none"> • Trusted server • Semi trusted • Not trusted 	<ul style="list-style-type: none"> • GHZ • EPR • Bell • Catalysis 	<ul style="list-style-type: none"> • Public key • Secret key 	<ul style="list-style-type: none"> • Universal • One-way • Stabilizer code • Algebraic code 	<ul style="list-style-type: none"> • Fainted Laser • product state • Unitary coding • Angle rotation

All the above methods have pros and cons depend on the scenario. From the practical point of view entanglement based protocols are more difficult due to the entangled particles must be shared prior to the communication; each party must share the number of entangled particles as the other parties. When the number of parties is increased to hundreds, thousands or more, it is no longer easy for the authenticator to maintain such large entangled particles. Other prominent techniques i.e. trusted server and hybrid protocol versions lack of unconditional security.

Practically feasible techniques', i.e. faint laser, product states are a subset of single photon mechanism. These techniques have weak factors like complex iteration; few need quantum storage and tedious extraction methods. Hash Function based protocols to have been explained in theory. These protocols have complex procedures and also some require entanglement. Therefore, to develop a rapid, secure and practical feasible quantum protocol, which can accomplish both user and message authentication is a hot research.

The proposed authentication scheme in this paper is an adaption of digital cryptography challenge-response mechanism. We briefly summarized the digital challenge-response authentication schemes [40] in the following Table 2.

Table 2. Digital challenge-response authentication schemes

Protocol	Characteristics	Mechanism	Advantages	Limitation
Challenge-Handshake Authentication Protocol (CHAP)	Authenticates a user or network host to an authenticating entity.	Shared secret key, One way hash function, three way handshake	Protection against: Replay attack	Distribution of secret key.

CRAM-MD5	SMTP mail agent authentication	Hash function, concatenation , Fresh random challenge	Resist to Replay attack	Lack of Mutual Authentication, Storage of password, Vulnerable to dictionary attack
Kerberos	Network authentication protocol over insecure channel	Issue tickets, Trusted third party,	Mutual Authentication, Resist to Replay attack and eavesdropping	Single point of failure, Vulnerable to man-in-middle attack. Time constraints
Otway-Rees protocol	Network authentication protocol over insecure channel	Usage of Nonce, session identifier, Server.	Resist to Replay attack and eavesdropping	Vulnerable to Intercept and resend attack
Needham-Schroeder protocol	Network authentication protocol over insecure channel	Shared secret key, server	Establish session key and mutual authentication	Key distribution
Wide Mouth Frog protocol	Network authentication protocol over insecure channel	Global clock, Server, shared secret key, BAN logic	Resist replaying attack and eavesdropping. Detection of modification	Key distribution and required trusted server
CAPTCHA, reCAPTCHA	Network user identification non-cryptographic scheme	Images	Widely used in webmail	Availability.
Distance-bounding protocol	cryptographic protocols that enable a verifier V to establish an upper bound on the physical distance to a prover P	Delay time, Radio frequency implementation		
Physical Unclonable Function or PUF	PUF is a function that is embodied in a physical structure and is easy to evaluate but hard to predict.	Hardware implementation of hash function,	Resist to spoofing attacks	Practical implementation and generality

The aim of the paper is to develop simple and efficient quantum user authentication based on single photon. proposed work is constructed from quantum digital signature [18-23] and Quantum Secure Direct Communication (QSDC) [24-34]. Particularly. We used reorder techniques of QSDC variant protocols [35-36]. Hence, before probing into our proposed scheme; we present a critical review on the related literature in the following paragraph.

Quantum digital signature combines quantum theory with classical digital signature is to take advantage of quantum effects to provide the unconditionally secure signature. Most of the proposed quantum signature schemes use entanglement to achieve the aim of signature and verification. The complexities of these schemes are the distribution of initial secret information, key distribution centre, measurement methods, encryption algorithm, etc. Recently, Wang [21] presented a scheme using single photon. This scheme utilizes the shared secret key distributed by the arbitrator. Their scheme implements von Neumann measurement for verification. However, this method requires third-party causes additional overhead during the communication, and practical feasibility is subtle.

In recent years, QSDC which can transmit secret messages directly without establishing a shared private key to encrypt has been so active. Since Beige et al.[24] proposed a QSDC protocol in 1999, many QSDC schemes had been presented. Most of the QSDC protocols are based on the secret transmission order of particles. Moreover, they almost follow the same mode: after confirming that the receiver receives all particles, the sender announces the secret order of the particles through a public channel. In fact, it is very difficult to perform in an actual communication, and it is also insecure about some attacks, such as the Trojan horse attack. The legitimate communicators may be impersonated by an attacker; thus, these protocols are insecure against the man-in-the-middle attack. These protocols also require third party to establish the key. F.Gao et al.[37] [38] presented attack strategies which an eavesdropper can utilize a special property of GHZ states and teleportation to elicit all or part of the transmitted secrets without being detected. Thus, our proposed scheme aims to cover some gaps of previous works in order to achieve robust and efficient quantum user identification protocol. However, exclusion of noise is the limitation factor of this current work.

The paper is organized as follows. In this Section, we provide a brief summary to digital challenge-response authentication schemes and a review concerning the quantum authentication provided by quantum digital signature and QSDC. In Section 2, we describe our proposed user authentication scheme in a detailed manner. Section 3 examines security of the scheme with some attack scenario. Conclusion and future works are presented in the Section 4.

2. PROPOSED SCHEME METHODOLOGY

This section presents our proposed quantum user authentication scheme in a detailed manner. We assumed that Eve or impostors can listen to public channel but not able to alter whereas the quantum channel is alterable. Our scheme implements a new protocol called Identification Group Key (IGK) function to derive authentication keys from the shared secret key. The authentication key can be acted as an initial authentication key which is utilized before any quantum communication or a session authentication key which acts as a user authentication during the quantum transmission. This protocol is based on short shared secret key and modified QSDC's reorder technique. The proposed quantum user scheme utilizes quantum bit error rate (QBER) verification to authenticate the user.

IGK protocol mainly based on short shared secret key between the parties called Identification Key (IK). Unlike other QKD protocols, our protocol requires short shared secret key. From that short key, we can derive multiple long keys as secret as the shared key.

2.1. Identification Key (IK)

IK is a short shared secret key or common key shared between the parties. IK is a set of n bits. Each bit represents 0 or 1. The total length of key is important for choosing the polarization encoding. Fig. 1 represents the format of IK.

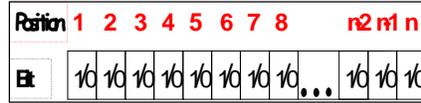


Figure 1. Format of IK

2.2. Identification Group Key (IGK)

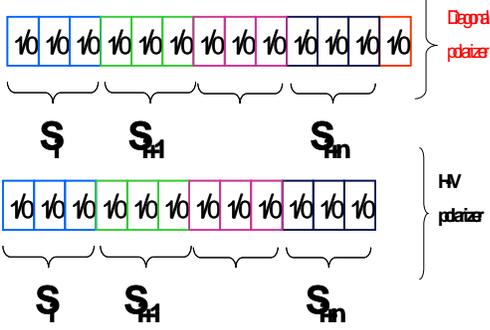
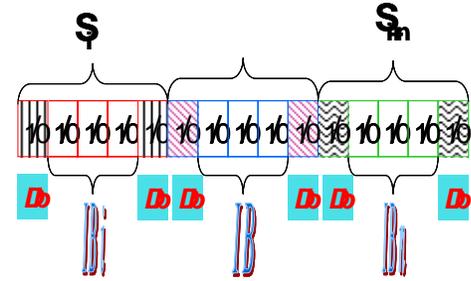
IGK protocol is a set of methods to manipulate the IK to derive authentication keys and session keys (IGK). This protocol is exchanged through public channel and to derive the collection of Identification Group (IG) keys. The number of IG keys in an IGK depends on user’s demand. Table 3 illustrates the IGK function header. IGK protocol’s header consists of n IG keys. To derive the IG key, two parameters namely x and Identification Block (IB) are needed. The parameter x is positive integer value, and IB is a set of natural number elements.

Table 3. Format of IGK header

IG_1	IG_2	IG_3	IG_n
$x, IB\{, \}$	$x, IB\{, \}$	$x, IB\{, \}$	$x, IB\{, \}$

IGK is a combination of all IG keys. To derive an IG key, four functions are required. As we already mentioned, this function relies on IK. The first function called total number of set (S_n) is to divide the IK into n group of bits or set of bits/blocks based on a user defined parameter x (See Table 4). After division, each set refers as S_i (where i is an element of n). If n is an even number, then horizontal-vertical polarization is applied for encoding the photons during quantum transmission. Otherwise, encode in diagonal polarization for odd n value. Secondly, Discard bit (Db) function discards the first and last bit of a set S_i . Next, Identification Block (IB) function is to convert all S_i into IB set by applying Db. These functions make the key’s length shorter and encoding in different polarization. Both horizontal-vertical and diagonal polarizations encoding makes key complexity higher. Finally, Identification Group (IG) function is to obtain IG key by combining all IB set. The detailed description of IGK protocol’s function with picture illustration is explained in Table 4. It is divided into two columns; the left column explains the protocol’s function in a pseudo code, while the right column illustrates functions in picture or equation.

Table 4. Detailed description of IGK protocol's functions

IGK Functions	Example
<p>(1) <u>Total number of set</u> (S_n)</p> <p>S_n is the total number of set after dividing the IK by positive integer.</p> <p>$S_n = (IK \text{ divide } x)$ <i>{x is a positive integer}</i></p> <p>If ($IK \bmod x = 0$) then use X basis polarization for encode.</p> <p>If ($IK \bmod x = 1$) then use Z polarization for encode.</p> <p>S_i refers to a set or group of bits after dividing IK into many set</p>	 <p style="text-align: center;">Figure 2. Choosing polarization</p>
<p>(2) <u>Discard bits</u> (Db)</p> <p>This function will discard first and last bit of S_i.</p> <p>(3) <u>Identification Block</u> (IB)</p> <p>This is a modified S_i in which Db is applied</p> <p style="text-align: center;">$IB_i = Db(S_i)$</p>	 <p style="text-align: center;">Figure 3. Db & IB functions</p>
<p>(4) <u>Identification Group</u> (IG)</p> <p>IG is a set of all IB elements in a user defined order.</p>	<p style="text-align: center;">$IG \subset \{IB_p, IB_q, \dots, IB_r\}$</p> <p style="text-align: center;">Here $p, q, r \in IB \{i_0, i_1, \dots, i_n\}$</p>

Now, let see the derivation of IGK or authenticate keys from the IK as follows,

IK (Identification Key) is a shared short secret key between parties. IK is set of n binary bits.

(1)

To derive IGK (Identification Group Key) from IK by two user's inputs x and y

(IB). x is a positive integer and y is a set of positive integers. We divide the IK by x to obtain sets of block (S). The total number of sets refers as S_n and S_i denotes i set. Each element of y refers to element of IB .

$$x \in \mathbb{Z}^+, y = \{y_1, \dots, y_n\} \quad (2)$$

$$S_n = \left\lfloor \frac{|IK|}{x} \right\rfloor \quad (3)$$

$$\{S_i\} = \{(0,1)^k \mid S_i \in IK\} \quad (4)$$

$$y = \{p, q, r, s, \dots, z\} \text{ where } p, q, r, \dots, z \in \mathbb{Z}^+ \quad (5)$$

$$y \in IB \text{ and } 1 \leq |y| \leq S_n \quad (6)$$

$$\text{i.e. } y = Db(S_i) \quad (7)$$

Discard bits (Db) is a function to remove first and last bits of the set.

$$Db: Db(S_i^n) \quad (8)$$

Identification Block is a set corresponding to S after applying Db function.

$$IB_i = Db(S_i) \quad (9)$$

Each Identification Group is an union/concatenation of IB blocks

$$IG_i = \cup IB_j^k \quad (10)$$

IGK is a union/concatenation of all IG blocks.

$$IGK = \cup IG_i^n \quad (11)$$

2.3. IGK Protocol Example

This is simple IGK protocol illustration. For example, Alice requests initial authentication key or session authentication key to Bob using IGK protocol. She simply sends the IGK header in a public channel. In fact, she knows the outcome or key value before actually receiving on the quantum channel. Thus, user verification process is simple. Table 5 is an example of IGK header. For each IG key, it requires x and IB elements value.

Table 5. IGK Header format

IG₁	IG₂	IG₃	IG₄
5, IB{1,3,4,7}	7, IB{2,3,4,6}	4, IB{1,3,6,8,9}	8, IB{1,4,6,}

When Bob receives the header, he prepares the authentication key or IGK value based on above-mentioned IGK's protocol functions. Then, he sends the qubits according to IGK (12) value to Alice.

$$IGK = IG_1 \cup IG_2 \cup IG_3 \cup IG_4 \quad . \quad (12)$$

2.4. Quantum User Authentication Scheme over Noiseless Channel

This section explains the proposed user authentication scheme. Our scheme utilizes both the IGK protocol and QBER calculation. We assumed noiseless channel as idealistic environment in which source, line and detector are perfect.

This scheme consumes both quantum channel and public channel. Our proposed scheme utilizes the public channel efficiently and reduces the usage of quantum channel. Thus, our scheme is cost-effective in terms of minimizing the photon transmission. In addition, our proposed scheme can capable of authenticate both the users. Furthermore, this scheme is the deterministic outcome due to IGK protocol. Thus, both the users know the outcome which leads quantum distribution accurate unlike BB84. In five steps, the proposed scheme achieves the user authentication. Now we see the proposed scheme with channel usage. Figure 4. is a simple illustration of the proposed authentication scheme.

Let say Alice wants to authenticate Bob and vice versa using our scheme.

1. Alice sends *IGK* header (authentication key or session key) to Bob (*Public Channel*)
2. Bob sends *IGK* outcome with erroneous qubits to Alice (*Quantum channel*)
3. Alice records and calculates qubits, then she sends QBER value to Bob (*Public channel*)
4. Bob compares with actual QBER value, if correct, and then Bob sends actual QBER value and erroneous bit position. Otherwise, Bob terminates the operation (*Public Channel*)
5. Alice verifies and confirms Bob, otherwise. Alice terminates operation. (*Public Channel*)



Figure 4. Quantum user authentication scheme

3. DISCUSSION

In this Section, we discuss elaborately about our scheme. User authentication is an important and compulsory task for any security transmission. For instance, Alice and Bob want to initiate QKD process using any existing quantum protocols. Before initiate their operation, they have to authenticate themselves. Our proposed scheme can be used as an authentication key for initial authentication as well as during the communication by session keys.

In step 1, Alice requests for an authentication key by sending IGK header to Bob. Meanwhile, eavesdropper Eve or impostor can listen to public channel but not able to alter. During step 2, receiver Bob sends IGK outcome with erroneous qubits to Alice. Here erroneous bits are considered as wrong polarization or ignore some qubits. As we assumed, our scheme works on idealistic environment. Thus, this step is the vital action for authenticate users effectively. When Alice receives bits, she calculates the QBER value and records wrong bit position. Then she informs QBER value to Bob in public channel. This is the crucial activity in this scheme to find the impostor. As we mentioned before, the quantum environment is perfect, so changes in QBER can only be caused by eavesdropper or impostor influence. After, Bob verifies with actual value and if the value is correct, then he sends actual QBER value and erroneous bit position. In step 4, Bob authenticates Alice. Consequently, in step 5, Alice verifies the result and confirms Bob. In other words, Alice authenticates Bob. During this process, predicting or guessing the outcome for both quantum channel and public channel are very hard for the unauthorized users. The probability of predicting the results is negligible. To make our proposed scheme is feasible with current imperfect environment, is to find a normalized threshold value for noise from the quantum channel, detector and source is our future work.

For both initial authentication and session authentication operations, the above scheme is same. The only difference between the two operations is IG key length. Usually, initial authentication involves larger key than the session key is to increase the performance of time. To ensure the user's identification during the transmission users can request session keys. In addition, polarization of qubits in a single IG key is varied. Therefore, Eve attacks on qubits to analyze qubits during transmission are difficult. We discuss more security analysis on Section 3.

This scheme can extend to multiparty environment. Each pair in a network requires having IK key. But this is not an efficient way because IK grows in a proportion as following equation.

4. EFFICIENCY AND SECURITY ANALYSIS

In this section, we discuss the efficiency and security analysis of our scheme. The efficiency of the proposed authentication scheme is high due to various factors like multiple re-use of IK, efficient usage of public channel and simple quantum verification function. The QBER verification for authentication is the highlight of the scheme. This reduces much computational time and overhead unlike quantum hash function or quantum error correction code. Furthermore, qubits distribution is in a deterministic mode. Hence, experimental setup requires minimal time and efficiency level of qubits measurement is so high. A figure of merit is the total efficiency η defined as [39].

$$\eta = \frac{b_s}{q_t + b_t} \quad (13)$$

where b_s is the number of secret bits in the key, q_t is the number of qubit used, and b_t is the number of classical bits exchanged between parties. For instance, the total efficiency of BB84 is

$\eta = 25\%$ as half of the instances will be discarded and at least one bit of classical information exchanged for each qubit, i.e., $b_s = 0.5$, $q_t = 1$ and $b_t = 1$. The total efficiency of our proposed scheme approaches $\eta = 1$ as $b_s = q_t$ and $b_t = 1$, because in our scheme, the secret bit is same as qubit and also there is no discard of any qubit. Therefore, our efficiency formula is followed,

$$\eta = \frac{b_s}{b_t} \quad (14)$$

Therefore, efficiency of proposed scheme reach 100%, where $b_s = b_t = 1$. Let us consider the security of the scheme by analysing with some attacks. The following section explains security analysis in a detailed way. The security analysis is an important evaluation criterion for any quantum cryptography protocols.

4.1 No message attack

Now we assume that an eavesdropper, Eve wants to impersonate Alice to pass the authentication while Alice is not present. Let assume Eve controls both quantum channel and public channel between Alice and Bob. According to our protocol, she must send IGK keys to pass authentication scheme. Eve can send IGK request to Bob in a public channel. When Bob prepares and sends back to Alice system. Eve tries to measure incoming photons by random polarization or specific polarization. She sends QBER value to Bob. Eventually, the prediction of correct QBER value is hard. Bob verifies with QBER value and terminates the operation. Let say, Eve guessed initial authentication correctly but the probability of passing on session key authentication is very difficult.

Our proposed authentication scheme can provide security, even though Eve got quantum computer or unlimited computing process. Furthermore, IGK protocol can also serve as efficient quantum key distribution protocol. Native QKD protocol involves post classical procedures like sifting, error correction, and privacy amplification; this is due to probabilistic nature of qubit. Our protocol is deterministic for legitimate users and stochastic outcome protocol for illegitimate or impostor. Moreover, it increases the key rate and transmission of the photon is reduced highly.

4.2 Man-in-middle attack

The purpose of the authentication scheme is to detect the man-in-middle attack or impostor's attack. We assumed that IK is a short shared secret key, and Eve cannot make a copy of photons due to no-cloning theorem. Furthermore, she cannot measure correctly due to Heisenberg's uncertainty principle. In our scheme polarization of the photon varies due to the IGK protocol. It takes both horizontal and diagonal polarization in a single IGK protocol. For the intercept-resend attack, the effect of QBER value triggers the legitimate user about presence of impostors.

4.3 Denial of service attack

Eve captures and performs same measurement on the photons from one-party transmission, i.e. either Alice to Bob or Bob to Alice. This is also zero error probability to guess the Eve's attacks. At the end, legitimate party knows that the received qubits are meaningless. In our proposed scheme, session authentication key and calculation of QBER value notify the presence of Eve and prevent this attack.

4.4 Invisible photon attack

This attack is impossible due to the proposed scheme implements one-way communication.

4.5 Disturbance attack

Eve disturbs the photons and makes it truly random. This is similar to denial of service attack. The proposed scheme's QBER value factor will indicate the presence of Eve.

4.6 Trojan horse attack

In this scenario, Eve could attack Alice or Bob's apparatuses, or she could exploit weaknesses in the actual implementation of abstract QKD. However, in the proposed scheme guessing probability is low.

4.7 USD attack (Unambiguous State Attack)

This attack can be balked by the mixture of key state and also guessing probability is low.

5. CONCLUSIONS

We provide a quantum user authentication scheme using new proposed protocol called IGK and verification of QBER value. IGK protocol modifies rearrangement of photon technique in an efficient way where only legitimate users can derive authentication keys and session keys. Furthermore, our scheme can be used as deterministic quantum key distribution with reduced transmission of photons. We proved that unalterable public channel combine with proposed scheme over idealistic environment provides efficient quantum user authentication. Proposed quantum user authentication can be applicable on any quantum key distribution protocol and able to authenticate the legitimate users efficiently. Next step in our research is towards enhancing our scheme for message authentication and feasible with current technology. Moreover, to find an acceptable threshold value for noise and imperfect hardware for a practical feasibility is a challenge.

REFERENCES

- [1] Bennett, C.H. and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. 1984.
- [2] Barnum, H., Quantum message authentication codes. Arxiv preprint quant-ph/0103123, 2001.
- [3] Crepeau, C., et al., Authentication of Quantum Messages. 2001: Citeseer.
- [4] Müller-Quade, J., Quantum pseudosignatures. Journal of Modern Optics, 2002. 49(8): p. 1269-1276.
- [5] Ljunggren, D., M. Bourennane, and A. Karlsson, Authority-based user authentication in quantum key distribution. Physical Review A, 2000. 62(2): p. 9413.
- [6] Kuhn, D.R., A Quantum Cryptographic Protocol with Detection of Compromised Server. Arxiv preprint quant-ph/0311085, 2003.
- [7] Jensen, J.G. and R. Schack, Quantum authentication and key distribution using catalysis. Arxiv preprint quant-ph/0003104, 2000.
- [8] Zhang, Y.S., C.F. Li, and G.C. Guo, Quantum authentication using entangled state. Arxiv preprint quant-ph/0008044, 2000.
- [9] Shi, B.S., et al., Quantum key distribution and quantum authentication based on entangled state. Physics Letters A, 2001. 281(2-3): p. 83-87.
- [10] Li, X. and H. Barnum, Quantum authentication using entangled states. International Journal of Foundations of Computer Science, 2004. 15(4): p. 609-617.
- [11] Hong, C., et al., Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping. Arxiv preprint quant-ph/0601194, 2006.

- [12] Li, X. and L. Chen. Quantum Authentication Protocol Using Bell State. 2007.
- [13] Kuhn, D.R., A Hybrid Authentication Protocol Using Quantum Entanglement and Symmetric Cryptography. Arxiv preprint quant-ph/0301150, 2003.
- [14] Medeiros, R.A.C., et al., Quantum authentication scheme based on algebraic coding. Arxiv preprint quant-ph/0307095, 2003.
- [15] Pérez, E., et al., Quantum authentication with unitary coding sets. Journal of Modern Optics, 2003. 50(6): p. 1035-1047.
- [16] Zhang, D. and X. Li. Quantum authentication using orthogonal product states. 2007.
- [17] Kanamori, Y., et al., Authentication Protocol using Quantum Superposition States. International Journal, 2009.
- [18] Lu, X. and D.G. Feng, An arbitrated quantum message signature scheme. CIS2004 Lecture Notes in Computer Science, 2004. 3314: p. 1054-1060.
- [19] Gottesman, D. and I. Chuang, Quantum digital signatures. Arxiv preprint quant-ph/0105032, 2001.
- [20] Zeng, G. and C.H. Keitel, Arbitrated quantum-signature scheme. PHYSICAL REVIEW-SERIES A-, 2002. 65(4; PART A): p. 42312-42312.
- [21] Wang, J., Q. Zhang, and C. Tang, Quantum signature scheme with single photons. Arxiv preprint quant-ph/0511224, 2005.
- [22] Lee, H., et al., Arbitrated quantum signature scheme with message recovery. Physics Letters A, 2004. 321(5-6): p. 295-300.
- [23] Wen, X., Y. Liu, and N. Zhou, Realizable Quantum Broadcasting Multi-Signature Scheme. International Journal of Modern Physics B, 2008. 22(24): p. 4251-4259.
- [24] Beige, A., et al., Secure communication with a publicly known key. Acta Physica Polonica A, 1999. 101: p. 357.
- [25] Barnum, H.N., Quantum secure identification using entanglement and catalysis. Arxiv preprint quant-ph/9910072, 1999.
- [26] Huang, D., et al., Quantum Secure Direct Communication Based on Chaos with Authentication. Journal of the Physical Society of Japan, 2007. 76(12): p. 124001.
- [27] Yu-Guang, Y., W. Qiao-Yan, and Z. Fu-Chen, An efficient quantum secure direct communication scheme with authentication. CHINESE PHYSICS-BEIJING-, 2007. 16(7):
- [28] Liu, W.J., et al., GENERAL: Efficient Quantum Secure Direct Communication with Authentication. Chinese Physics Letters, 2008. 25(7): p. 2354-2357.
- [29] Jie, S., Z. Ai-Dong, and Z. Shou, Quantum secure direct communication protocol with blind polarization bases and particles' transmitting order. CHINESE PHYSICS-BEIJING-, 2007.
- [30] Jin, X.R., et al., Three-party quantum secure direct communication based on GHZ states. Physics Letters A, 2006. 354(1-2): p. 67-70.
- [31] Wang, C., et al., Quantum secure direct communication with high-dimension quantum superdense coding. Physical Review A, 2005. 71(4): p. 44305.
- [32] Wang, C., F.G. Deng, and G.L. Long, Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Optics communications, 2005. 253(1-3): p. 15-20.
- [33] Xi-Han, L., et al., Quantum secure direct communication with quantum encryption based on pure entangled states. CHINESE PHYSICS-BEIJING-, 2007. 16(8): p. 2149.
- [34] Zhong-Xiao, M. and X. Yun-Jie, Quantum secure direct communication via partially entangled states. CHINESE PHYSICS-BEIJING-, 2007. 16(5): p. 1197.
- [35] Zhu, A.D., et al., Secure direct communication based on secret transmitting order of particles. Physical Review A, 2006. 73(2): p. 22338.

- [36] Wang, J., Q. Zhang, and C. Tang, Quantum secure direct communication based on order rearrangement of single photons. *Physics Letters A*, 2006. 358(4): p. 256-258.
- [37] Gao, F., et al., GENERAL: A Special Eavesdropping on One-Sender Versus N-Receiver QSDC Protocol. *Chinese Physics Letters*, 2008. 25: p. 1561-1563.
- [38] Gao, F., Q.Y. Wen, and F.C. Zhu, GENERAL: Teleportation attack on the QSDC protocol with a random basis and order. *Chinese Physics B*, 2008. 17: p. 3189-3193.
- [39] A. Cabello *Phy.Rev. Lett.* 85. 5635, 2000
- [40] http://en.wikipedia.org/wiki/Challenge-response_authentication