Journal of Computers Vol. 29 No. 3, 2018, pp. 83-93
doi:10.3966/199115992018062903008

A Simple and Secure Non-interactive Deniable Authentication Scheme with Privacy Protection using Quantum Bits

Hongfeng Zhu

Software College, Shenyang Normal University, Shenyang 110034, China
zhuhongfeng1978@163.com

Received 28 December 2016; Revised 19 April 2017; Accepted 3 July 2017

Abstract. Deniable authentication is an essential cryptography paradigm, which enables a receiver to identify the source of a given message, but the receiver cannot prove the source of the message to any third party over an insecure network. In this paper, we propose a novel non-interactive deniable authentication quantum bits-based scheme, named NIDAQ, aiming to require one ciphertext with non-interactive process for achieve mutual authentication, deniability and the message transmission secretly without a central node, and at the same time, wiping out the stubborn flaws in traditional communication. Our proposed protocols' security are mainly based on quantum-verifiable and chaotic maps. In contrast to the recent literatures, our proposed scheme not only cares about security and efficiency, but also provides privacy protection which is a very important property in the modern social network. Finally, we give the security proof and the efficiency analysis of our proposed scheme.

Keywords: chaotic maps, deniability, non-interactive, privacy protection, quantum verifiable

1 Introduction

Wide deployment of quantum information science, such as quantum entanglement and single quantum no-cloning principle, has already shown great potential in improving the quality of people. Recently, Zhang et al. [1] presented a technique for implementation of quantum key distribution (QKD) considering a client–server system such that large resources such as laser and detectors, situated at the server side, and the client, requires only an on-chip polarization rotator that may be integrated into a handheld device. So Based on the literature [1], there will appear many applications. Up to now, the general security protection mechanism is still mutual authentication key agreement/exchange (MAKA/E) protocol which is used to set up an authenticated and confidential communication channel. The existing authentication protocols adopt passwords [2], long secret keys [3], or public key [4] as the proofs of identity. However, most of the above methods are impractical or insecure in quantum era. For example, password-based scheme [2] will suffer to guessing attacks (on-line/off-line) easily, and the other two [3-4] are not good for user experience (impractical). Another example, radio frequency identification (RFID) technique has always suffered from relay attack for a long time, because accurate round-trip time (RTT) measurement produces some challenges in implementation of distance-bounding protocols since a small error provides a large inaccuracy in estimation of the distance [6]. In order to solve above-mentioned problems, quantum-verifiable authentication protocols [7] emerge at the right moment. The key idea of the literatures [7] is to provide data integrity via the quantum channel. This method does not require preshared keys or preregistered public keys. So, in this paper, based on the literatures [1, 7], we put forward a Quantum-Verifiable and Non-interactive Deniable authentication scheme with privacy preserving.

Quantum technology is a rapidly growing area which aims to establish the principles of communication and computation for systems based on the theory of quantum mechanics. Quantum communication and cryptography have been developed over the last decades and now been put into commercial use. One of the remarkable achievements of quantum cryptography is QKD [8], where classical key is shared in an unconditionally (there is no computational hardness assumption) secure way.

In a recent work, Zhang et al. [1] demonstrated that QKD could be implemented in a client-server scenario, where client only uses minimal quantum resources, i.e., send/receive qubits and performs polarization operations. However, in that setting, server has more capabilities such as qubits preparation and quantum measurement. In a word, quantum technology can play an important role in the cryptography realm but it is not popularization in nowadays, so we combine quantum technology with computational cryptography which is the best method to avoid many attacks.

Deniable authentication protocol is a cryptographic authentication of unique style in contemporary era. Differ from the traditional authentication protocols, which always under the insecure channel that enable a receiver to confirm the message whether sent by the designed sender, the deniable authentication protocol owns three basic characteristics. First, a receiver is capable of verify the given message at anytime. Second, the receiver cannot prove this message came from the certain sender to a third party. Third, if the receiver reveals the message to the third party deliberately, the sender has the right to deny the source of message. Due to the deniable authentication protocols possess the above properties, so it was used to provide freedom from coercion in electronic voting systems and also build a secure platform for communication over the Internet.

In the past few years, many scholars dedicated to this field for a stronger protocol. In 1998, Dwork et al. [9] present a notable deniable authentication protocol based on concurrent zero-knowledge proof, which requires timing constrain and the proof of knowledge is subject to a time delay in the authentication process. Another deniable authentication protocol was developed by Aumann and Rabin [10] under the factoring problems, inconveniently, it need a public directory between the sender and the receiver. Later, Deng et al. [11] proposed another scheme based on the factoring and the discrete logarithm problems, but this protocol also requires a trusted directory. Therefore, in 2002, Fan et al. [12] proposed a simple deniable authentication protocol based on Diffie-Hellman key distribution protocol, which adopts certificates to resist the man-in-the-middle attack and provide signatures to identify the message. However, Yoon [13] demonstrated that Fan et al.'s scheme is incapable of rejecting some attacks, where an aggressor can pretend the receiver easily and communicate with the sender, so present an improved scheme to overcome this problem. Feng and Ma [14] put forward a deniable authentication protocol based on witness indistinguishable. Although these schemes have improved on the safe side, they also failed to reduce the cost and time. As we all know, interactive deniable authentication protocols require several communication rounds between the applicant and certifier. Accordingly, with the purpose of decreasing communication cost, researchers have proposed several agreements concerning the non-interactive deniable authentication. Shao [15] first proposed a non-interactive deniable authentication protocol based on ElGamal cryptography in 2004. But in 2007, Lee et al. [16] discovered that in Shao's protocol the receiver enables prove the message to the third party, there is no doubt that the scheme violates the basic rules of deniable authentication. After then, in 2008, Wang and Song [17] demonstrated a non-interactive deniable authentication scheme in the provable-security direction. Later, Hwang and Chao [18] present a non-interactive deniable authentication protocol with anonymous sender protection in 2010. Subsequently, Li [19] proposed an enhanced authentication protocol in 2013 to remove the weakness that disappears in Yoon et al. [20].

The main contributions are shown as below:

(1) Our proposed protocol **improves the security level.** Because the value of authentication is transmitted by qubit channel.

(2) Our proposed protocol can **immune to some attacks in classical cryptography**. Because we use quantum channel in the second round of our protocol, it cannot be cloning (**No-cloning Theorem:** In 1982, Wootters and Zurek [5] proved that one cannot duplicate an unknown quantum state; that is, a user cannot copy a qubit if he/she does not know the polarization basis of the qubit.) which means any attacker cannot eavesdrop the transmissive messages.

(3) Our proposed protocol is the first **quantum deniable authentication protocol** (QDAP).

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Next, a new chaotic maps-based non-interactive deniable authentication scheme is described in Section 3. In Section 4, we give the security of our proposed protocol. The efficiency analysis of our proposed protocol is given in Section 5. This paper is finally concluded in Section 6.

2 Preliminaries

2.1 Definition and Hard Problems of Chebyshev Chaotic Maps

Zhang [21] proved that semi-group property holds for Chebyshev polynomials defined on interval (-∞,+∞). The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) (\mathrm{mod}\, N),$$

where $n \geq 2$, $x \in (-\infty, +\infty)$, and N is a large prime number. Obviously,

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x)).$$

Definition 1. (*Enhanced Chebyshev polynomials*) The enhanced Chebyshev maps of degree n ($n \in N$) are defined as: $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) (\mathrm{mod}\, p)$, where $n \geq 2$, $x \in (-\infty, +\infty)$, and p is a large prime number. Obviously, $T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$.

Definition 2. (*DLP*, Discrete Logarithm Problem) Given an integer a, find the integer r, such that $T_r(x) = a$.

Definition 3. (*CDH*, Computational Diffie–Hellman Problem) Given an integer x, and the values of $T_r(x), T_s(x)$, what is the value of $T_{rs}(x) = ?$

It is widely believed that there is no polynomial time algorithm to solve DLP, CDH with a non-negligible probability.

2.2 The Main Scenes about Deniable Authentication Scheme

Scene 1 (EVS, Electronic Voting System, Fig. 1). In the electronic voting system, Alice is a legal voter and Bob is a manager of tally authority. After finishing voting, Bob will receiver the ballot T with authenticator from Alice. Suppose a third party Tom who intends to know the result of Alice, Bob unable told him because Bob fails to prove the source of ballot T.

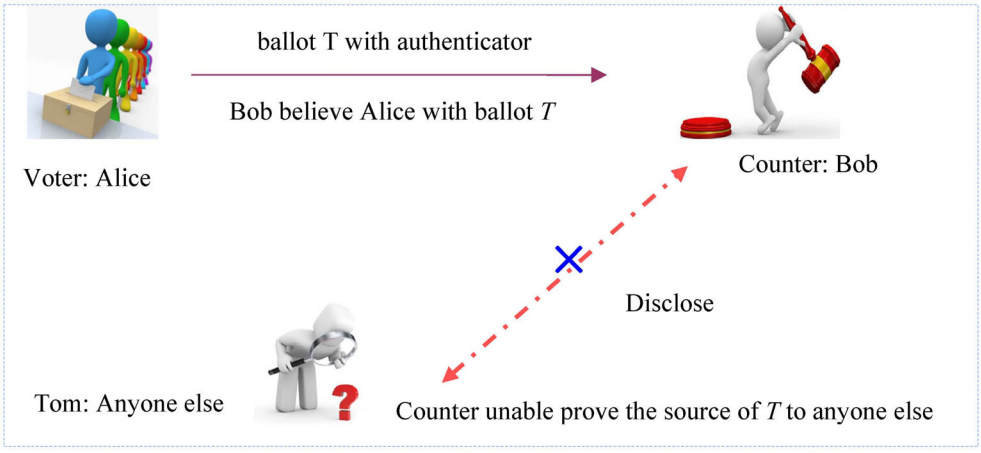

Fig. 1. Non-interactive Deniable authentication protocol in electronic voting system

Scene 2 (DAOS, Deniable Authentication protocol in Online Shopping, Fig. 2). Suppose that A wants to set up an exchange from the merchant, so A transfers price M and the type of goods S to the merchant. After receiving the information, the merchant will view the customer A as a trusted user. However, if appear a customer B who want to order goods from this shop. The merchant unable show the shopping information of A to B, even the merchant has negotiated with B in private.

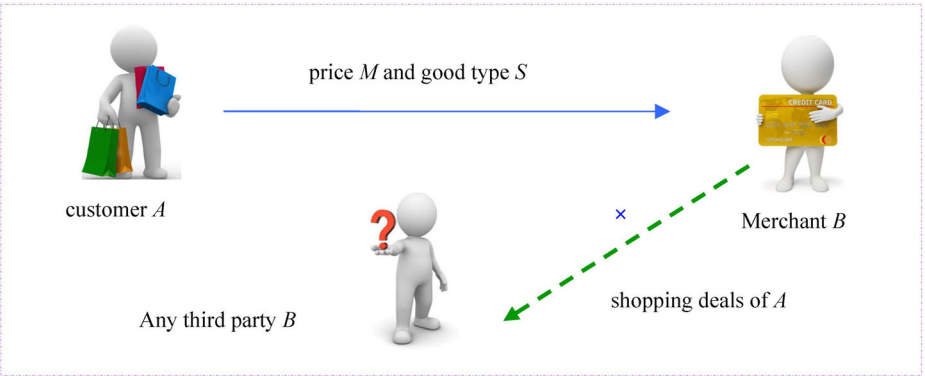

Fig. 2. Non-interactive Deniable authentication protocol in online shopping

3 An Instance Based on Chaotic Maps

The concrete notations used hereafter are shown in Table 1. Fig. 3 illustrates the NIDAQ scheme.

Table 1. Notations

Symbol	Definition
ID_i	the identity of users
a	nonces
$(x, T_{K_i}(x))$	public key of user$_i$ based on Chebyshev chaotic maps
K_i	secret key of user$_i$ based on Chebyshev chaotic maps
H	A secure one-way hash function
$\|\|$	concatenation operation

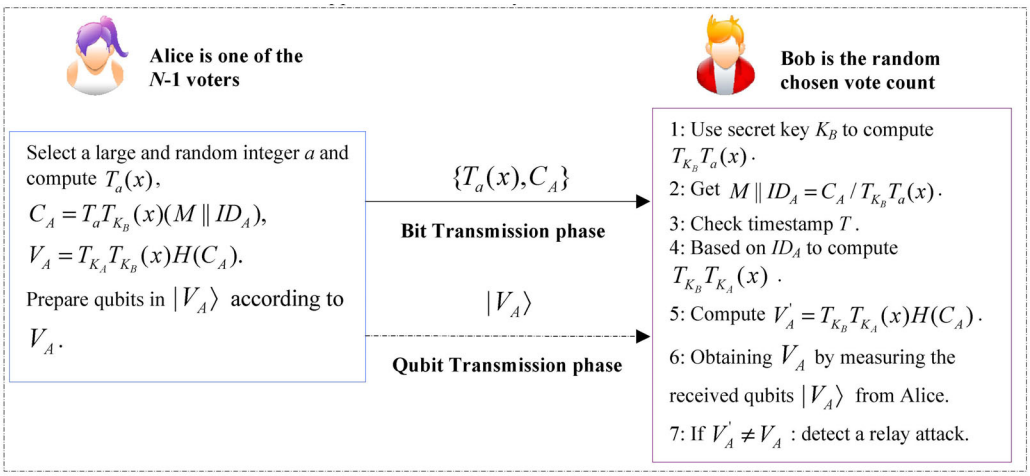

Fig. 3. The non-interactive deniable authentication scheme with privacy protection

3.1 Setup

Simply speaking, without loss of generality, we choose Alice as one of the N-1 voters, her public key is $(x, T_{K_A}(x))$ and the corresponding secret key is K_A. For the random chosen vote count node/person, we choose Bob, his public key is $(x, T_{K_B}(x))$ and the corresponding secret key is K_B. Due to space limitation in this paper, we are not able to discuss the details about how to distribute the public-private key pairs of the users. Moreover, We assume that each voter is equipped with a device capable of preparing/sending photons and also polarization rotators. On the other hand, we suppose vote count node, in addition to receive qubits, are able to measure qubits.

3.2 Encrypt for N-1 Voters

When Alice wants to send the message *m* to the receiver Bob, she chooses one large and random integer *a*. Next, Alice computes $T_a(x)$, $C_A = T_a T_{K_B}(x)(M \| ID_A), V_A = T_{K_A} T_{K_B}(x) H(C_A)$. Then, Alice prepares qubits in $|V_A\rangle$ according to $M \| ID_A = C_A / T_{K_B} T_a(x)$. Finally, Alice sends $\{T_a(x), C_A\}$ to the Bob by classical channel and sends $|V_A\rangle$ by qubit channel.

3.3 Dencrypt for Vote Count Node/Person.

(1) Upon receiving $\{T_a(x), C_A\}$ from Alice, Bob can recover the identity of the sender by using secret key K_B to compute $T_{K_B} T_b(x)$ and get $M \| ID_A = C_A / T_{K_B} T_a(x)$.

(2) Firstly, based the sender's identity ID_A, Bob can get the public key $T_{K_A}(x)$ and compute $T_{K_B} T_{K_A}(x)$ and $V_A' = T_{K_B} T_{K_A}(x) H(C_A)$. This step is also authenticating the sender, if the sender is the "Alice", the messages *M* will be the valid information, if not, the recovered messages *M* will be as the invalid information.

(3) Bob obtains $M \| ID_A = C_A / T_{K_B} T_a(x)$ by measuring the received qubits $|V_A\rangle$ from Alice. Then Bob authenticates the message integrity $V_A' = V_A$?. If yes, the messages *M* are valid. Otherwise, the messages *M* are invalid or there are some attacks happened, such as relay attack.

4 Security Consideration

4.1 Security Analysis for Security Requirements

The deniability of our scheme.

Theorem 4.1. Our proposed scheme owns deniability under the CMBDLP and CMBDHP assumptions.

Proof: **Fig. 4** illustrates the simulated processes of proposed scheme. To prove that the proposed protocol is deniable, we should prove that all transcripts transmitted between Alice and Bob could be simulated by Bob itself. Although there has the private key of sender (Alice's K_A) involved, Bob (the receiver) still can simulate the whole transcript process. Bob cannot get the private key of Alice and he still can compute $T_{K_B} T_{K_A}(x) = T_{K_A} T_{K_B}(x)$ based on public key of Alice. To simulate the transcripts on message, Bob selects a large and random integer *a*. Then Bob computes $T_a(x)$, $C_A = T_a T_{K_B}(x)(M \| ID_A)$ and $V_A = T_{K_B} T_{K_A}(x) H(C_A)$. The transcripts $\{T_a(x), C_A, |V_A\rangle\}$ in simulation are indistinguishable from those of the sender Alice. Therefore, the receiver Bob cannot prove to a third party that the transcripts were produced by Alice. The core reason is that Bob can use his own secret key and the voter's public key to simulate all the processes. Furthermore, our proposed scheme has also achieved the strong deniability (Strong deniability [23] means that the sender can deny to have ever authenticated anything to receiver after execution of the protocol).

The security of ciphertext with mutual authentication.

Theorem 4.2. Our proposed scheme is ciphertext with authentication under the CMBDLP and CMBDHP assumptions.

Proof: Our proposed scheme is based on PKC (Public Key Cryptosystem), so there are two key points should be taken into account: the transcripts must mix with a large random nonce and any public key cannot be used to encrypt secret message directly. Therefore, we construct $C_A = T_a T_{K_B}(x)(M \| ID_A)$ to covered the secret message *M* and others' necessary information. And for assuring integrity, we construct $V_A = T_{K_A} T_{K_B}(x) H(C_A)$. Only Bob can decrypt C_A using his own secret key which are secure under the CMBDLP and CMBDHP assumptions, and furthermore authenticate the integrity by comparing with the $H(C_A)$, which is protected under the quantum communication. Additionally, since the value *a* of the random element is very large, attackers cannot directly guess the values *a* of the random elements to generate $T_a(x)$. Therefore, the proposed scheme provides ciphertext with mutual authentication security.

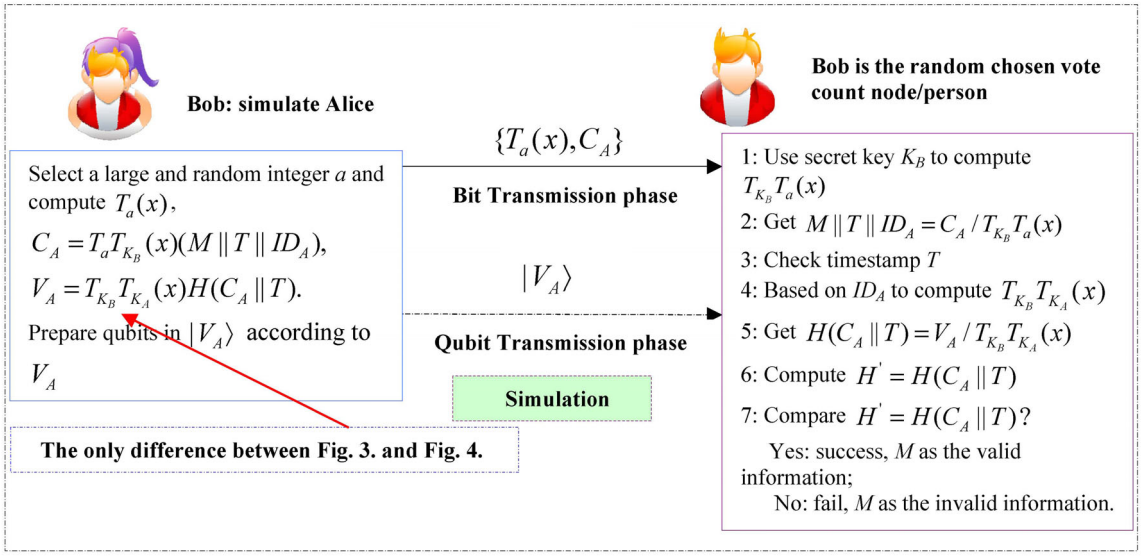

Fig. 4. The simulated processes of proposed scheme

The security of privacy protection.

Theorem 4.3. Our proposed scheme is privacy protection under the CMBDLP and CMBDHP assumptions.

Proof: We divide the participants into three characters: the sender, the receiver and the outsiders (including attacker, any curious nodes and so on). The sender's identity is anonymity for outsiders because ID_A is covered by $C_A = T_a T_{K_B}(x)(M \| ID_A)$, and then only the legal receiver Bob can use his secret key to recover the ID_A. Due to PKC-based about our scheme, the ID_A must be emerged to the legal receiver, or they cannot know the public key of the sender. The sender must know the receivers's identity because our scheme is adopted PKC and chaotic maps.

we construct $C_A = T_a T_{K_B}(x)(M \| ID_A)$ to covered the sender's identity. The encrypted message C_A is generated from a which is different in each session and is only known by the sender Alice. The receiver can decrypt C_A using $T_a(x)$ and his own secret key which are secure under the CMBDLP and CMBDHP assumptions. Additionally, since the values a of the random elements is very large, attackers cannot directly guess the value b of the random elements to generate $T_a(x)$. Therefore, the proposed scheme provides privacy protection.

About the privacy protection of our NIDAQ scheme, we must emphasize that any outsider cannot get any information (sender or receiver) about our proposed scheme.

The security of quantum-verifiable.

Theorem 4.4. An adversary A can relay a qubit sent by the voter Alice to the vote counter Bob correctly with probability 3/4 when A does not know anything about the basis of the qubit.

Proof: Let Alice encode a single bit d into its logical qubit $|d\rangle$, in the basis b, and send it to Bob. When an adversary A receives the qubit, since it does not know about b, in which the qubit is encoded, it chooses a random basis b_A. Then, it measures the qubit in that basis to obtain a single bit d_A. when the adversary A guesses the basis incorrectly, the vote counter Bob obtains it correctly with probability of half. So, the probability of the event that the single bit measured by Bob is equal to the single bit sent by Alice when the adversary relays the single bit between the reader and the tag as:

$$P[d' = d] = P[d' = d \mid b_A = b]P[b_A = b] + P[d' = d \mid b_A \neq b]P[b_A \neq b] \quad \textbf{(1)}$$

Since the adversary A guesses the basis randomly, it guesses the basis correctly with probability of half. It means that $P[b_A = b] = P[b_A \neq b] = 1/2$. Also, when $b_A = b$, the attacker A obtains a correct single bit. So, in this case, the adversary encodes the logical qubit correctly for sending to the vote counter Bob, and the outcome of measuring it by Bob will be equal to d. Thus, we get $P[d' = d \mid b_A = b] = 1$. However, when the attacker A guesses the basis incorrectly, i.e., $b_A \neq b$, the attacker A obtains a random single bit

and uses it to encode logical bit. Now it is easy to see that $P[d' = d \mid b_A \neq b]P[b_A \neq b] = 1/4$. Using Eq. 1, we conclude that the probability of a successful relay attack by A when a single qubit is sent from Alice to Bob, is $P[d' = d] = 3/4$. Consequently, when the adversary A relays a message $|V_A\rangle$ containing l qubits, the success probability of A is $(3/4)^l$.

Because our proposed scheme is NIDAQ type with one message without exchanging process, there are many security requirements no need to discuss (see Table 2).

Table 2. Definition and the reasons why we do not disscuss

Attack Type	Attack method	Definition	Reasons why we do not disscuss
Automatic validation attacks	Guessing attacks (On-line or off-line)	In an off-line guessing attack, an attacker guesses a password or long-term secret key and verifies his/her guess, but he/she does not need to participate in any communication during the guessing phase. In an undetectable on-line guessing attack, an attacker searches to verify a guessed password or long-term secret key in an on-line transaction and a failed guess cannot be detected and logged by the server.	No password involved
	Losting smart device and guessing attacks	An adversary gets the user's smart device and then carries out the guessing attacks.	No password involved
	Human Guessing Attacks	In human guessing attacks, humans are used to enter passwords in the trial and error process.	No password involved
No freshness verify attacks	Perfect forward secrecy	An authenticated key establishment protocol provides perfect forward secrecy if the compromise of both of the node's secret keys cannot results in the compromise of previously established session keys.	No session key produced
	Known session key security	Each execution of the protocol should result in a unique secret session key. The compromise of one session key should not compromise the keys established in other sessions.	No session key produced

Next, from the Table 3, we can see that the proposed scheme can provide Man-in-the-middle attack, impersonation attack and so on.

Table 3. Definition and simplified proof

Attack Type	Attack method	Definition	Simplified proof	Hard problems
Missing encrypted identity attacks	Man-in-the-middle attack (MIMA)	The MIMA attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.	All the information includes the *ID* and some nonces: a and the another form $T_a(x)$. An attacker cannot construct V_A because he has not K_A.	Chaotic maps problems and a secure one-way hash function with a secure quantum communication
	Impersonation attack	An adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.		
No freshness verify attacks	Replay/Relay attack	A replay/relay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently.		
Design defect attacks	Stolen-verifier attacks	An adversary gets the verifier table from servers by a hacking way, and then the adversary can launch any other attack which called stolen-verifier attacks.	There are no any verification tables in any node.	

Next, from the Table 4, we can see that the proposed scheme is more secure and has much functionality compared with the recent related scheme.

Table 4. Comparison PAQKAPs among and Other Protocols

	ZZ00 [26]	Case 8 of [27]	Case 2 of [27]	3QKDPMA [28]	Our scheme
Cryptographic Mechanism	Quantum	Classical	Classical	Quantum+Classical	Quantum+Classical
Pre-shared secret key	EPR pairs	Long-termed	Long-termed	Long-termed	No
Communication round	6	4	3	3	1
Quantum channel	Yes	No	No	Yes	Yes
Clock synchronization	No	No	Yes	No	No
Vulnerable to man-in-the-middle attack	No	No	No	No	No
Vulnerable to passive attack	No	Yes	Yes	No	No
Vulnerable to replay attack	No	No	No	No	No
Formal security proof	No	No	No	Yes	Yes
Deniability	No	No	No	No	Yes

4.2 Security Proof Based on the BAN Logic [22]

The notations used in the BAN logic analysis and logical postulates of BAN logic, please see Table 5 and Table 6 respectively. According to analytic procedures of BAN logic, the processes of our proposed instance is described in **Simulation**.

Table 5. Notations of the BAN logic

Symbol	Definition
$P \mid\equiv X$	P believes a statement X.
$\#(X)$	X is fresh.
$P \mid\Rightarrow X$	P has jurisdiction over the statement X.
$P \lhd X$	P sees the statement X**.**
$P \mid\sim X$	P once said the statement X.
(X,Y)	X or Y is one part of the formula (X,Y).
$\langle X \rangle_Y$	X combined with the formula Y.
$\{X\}_Y$	X is encrypted under the key K.
$(X)_Y$	X is chaotic maps-based hash function with the key K.
$P \xleftrightarrow{K} Q$	P and Q use the shared key K to communicate.
$\xrightarrow{K} P$	The public key of P, and the secret key is described by K^{-1}

Table 6. Logical postulates of the BAN logic

Symbol	Definition	
$P \mid\equiv P \xleftrightarrow{K} Q, P\{X\}_K \Big/ P \mid\equiv Q \mid\sim X$	The message-meaning rule	(R_1)
$P \mid\equiv \#(X) \Big/ P \mid\equiv \#(X,Y)$	The freshness-conjuncatenation rule	(R_2)
$P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X \Big/ P \mid\equiv Q \mid\equiv X$	The nonce-verification rule	(R_3)
$P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X \Big/ P \mid\equiv X$	The jurisdiction rule	(R_4)
$P \mid\equiv Q \mid\equiv (X,Y) \Big/ P \mid\equiv Q \mid\equiv X$	The belief rules	(R_5)

Table 6. Logical postulates of the BAN logic (continue)

Remark: Molecule can deduce denominator for above formulas.	
Simulation 1	BAN logic of NIDAQ
Goals:	Goal1. $A \mid\equiv (A \xleftrightarrow{M} B)$; Goal2. $B \mid\equiv A \mid\equiv (B \xleftrightarrow{M} A)$;
Idealized forms of NIDAQ instance:	**(A → B)** $C_1 : T_a(x), T_a T_{K_B}(x) M \parallel ID_A$;
Initial states:	($P_1 : A, B \mid\equiv A \xleftrightarrow{\lvert V_A \rangle} B$, quantum channel), $P_2 : A \mid\equiv \#(a)$
1: For C_1: According to the ciphertext C_1 and P_1, P_2 and attributes of chaotic maps, and relating with R_1,	we could get: $S_1 : B \mid\equiv A \mid\sim C_1$
2: Based on the initial assumptions P_1, P_2, and relating with R_2	we could get: $S_2 : B \mid\equiv \#C_1$
3: Combining S_1, S_2, P_1, P_2, R_3 and attributes of chaotic maps	we could get: $S_3 : B \mid\equiv \#T_a(x), T_a T_{K_B}(x) M \parallel ID_A$
4: Based on R_5	we take apart S_3 and get: $S_4 : B \mid\equiv \#T_a(x), S_5 : B \mid\equiv \#T_a T_{K_B}(x) M \parallel ID_A$
5: Combining P_1, S_5 and attributes of chaotic maps with a secure hash function	we can verify that the message C_1 is fresh and comes from Alice exactly.
6: Combining P_1, P_2, S_{10} and attributes of chaotic maps	we can get the fresh and privacy protection about identity of Alice.
7: Whole combination:	Since Alice and Bob communicate to each other just now, they confirm the other is on-line. Moreover, since Bob can get $\{ \lvert V_A \rangle \}$ from the quantum channel securely, and based on S_4, S_5, R_4 with chaotic maps problems, and this shows that that Bob could get the message $V_A^{'} = T_{K_B} T_{K_A}(x) H(C_A)$. and Goal1. $A \mid\equiv (A \xleftrightarrow{M} B)$; Goal2. $B \mid\equiv A \mid\equiv (B \xleftrightarrow{M} A)$. □

5 Efficiency Analysis

Table 7 shows performance comparisons between our proposed scheme and the literatures of [24]. Because there is no related work with quantum-verifiable deniable authentication scheme, we use the human-verifiable scheme as the contrasted scheme. We sum up these formulas [25] into one so that it can reflect the relationship among the running time of algorithms intuitively. $T_p \approx 10T_m \approx 30T_c \approx 72.6T_s \approx 1263.24T_h$, where: T_p: Time for bilinear pair operation, T_m: Time for a point scalar multiplication operation, T_c: The time for executing the $T_n(x)$ mod p in Chebyshev polynomial, T_s: Time for symmetric encryption algorithm, T_h: Time for Hash operation.

Table 7. Comparisons between our proposed schemes and the related literatures

Protocols (Authentication phase)		[24] (2013)	Ours
Computation	**A**	4Th + 1Ts+ 2Tp	1Th + 2Tc
	B	2Th + 1Ts + 2Tp	1Th + 2Tc
Communication	Messages	6	2
	rounds	2	1
Design	Concise design	No	Yes
	Number of nonces	2	1
	Model	Random Oracle with human-verifiable	Random Oracle with quantum-verifiable

Based on Table 4 and Table 7, we can draw a conclusion that the proposed scheme has achieved an improvement in both efficiency and security.

6 Conclusion

In this paper, we propose NIDAQ, a novel scheme towards building a deniable authentication scheme with quantum channel, and at the same time, achieving privacy protection. The core idea we have followed is that the most existing deniable authentication schemes are bilinear pairing-based, modular exponentiation and so on, for improving the efficiency, should be exploited to securely change another efficient cryptosystem, such as, chaotic maps in this paper. Since chaotic maps is adopted to a new encrypted algorithm without using symmetrical encryption, the proposed solution offers significant high-efficiency with respect to a human-verifiable authentication protocols. Compared with the related works, our NIDAQ scheme is not the trade off between security and efficiency, but is comprehensively improved scheme. In the future, three-party/N-party protocols, combining the advantages of classical cryptography with quantum cryptography, are the new directions which will arise many achievements.

Acknowledgements

This work is supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 201602680).

References

[1] P. Zhang, K. Aungskunsiri, E. Martyn-Lopez, J. Wabnig, M. Lobino, R.W. Nock, J. Munns, D. Bonneau, P. Jiang, H.W. Li, A. Laing, J.G. Rarity, A.O. Niskanen, M.G. Thompson, J.L. OBrien, Reference frame independent quantum key distribution server with telecom tether for on-chip client, Physical Review Letters 112(13)(2014) 1153-1165.

[2] V. Boyko, P. MacKenzie, S. Patel, Provably secure password authenticated key exchange using Diffie-Heilman, in: Proc. Advances in Cryptology-Eurocrypt, 2000.

[3] I. Spaliaras, S. Dokouzyannis, Design and evaluation of a new scheme based on secret sharing mechanisms that increases the security of conditional access systems in satellite pay-TV, Wireless Personal Communications 82(3)(2015) 1461-1481.

[4] X. Wang, C. Xiang, F.W. Fu, Secret sharing schemes for compartmented access structures, Cryptography & Communications 9(5)(2017) 625-635.

[5] W.K. Wootters, W.H. Zurek, A single quantum cannot be cloned, Nature 299(1992) 802-803.

[6] G.P. Hancke, Design of a secure distance-bounding channel for RFID, Journal of Network & Computer Applications 34(3)(2011) 877-887.

[7] H. Jannati, E. Ardeshir-Larijani, Detecting relay attacks on RFID communication systems using quantum bits, Quantum Inf Process 15(11)(2016) 4759-4771.

[8] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proc. the IEEE International Conference on Computers, Systems and Signal Processing, 1984.

[9] C. Dwork, A. Sahai, Concurrent zero-knowledge: reducing the need for timing constraints, Computer Science 1462(1998) 442-457.

[10] Y. Aumann, M. Rabin, Efficient, deniable authentication of long messages, in: Proc. Conference on Theoretical Computer Science , 1998.

[11] X. Deng, C.H. Lee, H. Zhu, Deniable authentication protocols, IEE Proceedings Computers and Digital Techniques

148(2)(2001) 101-104.

[12] L. Fan, C.X. Xu, J.H. Li, Deniable authentication protocol based on Diffie-Hellman algorithm, Electronics Letters 38(2002) 705-706.

[13] E.J. Yoon, E.-K. Ryu, K.-Y. Yoo, Improvement of Fan et al.'s deniable authentication protocol based on Diffie-Hellman algorithm, Applied Mathematics and Computation 167(1)(2005) 274-280.

[14] F. Tao, M.J. Feng, Universally composable security concurrent deniable authentication based on witness indistinguishable, Journal of Software 18(11)(2007) 2871-2881.

[15] Z. Shao, Efficient deniable authentication protocol based on generalized ElGamal signature scheme, Computer Standards and Interfaces 26(5)(2004) 449-454.

[16] W.-B. Leea, C.-C. Wua, W.-J. Tsaurb, A novel deniable authentication protocol using generalized ElGamal signature scheme, Information Sciences 177(6)(2007) 1376-1381.

[17] W. Bin, S.Z. Xia, A non-interactive deniable authentication scheme based on designatedverifier proofs, Information Sciences 179(6)(2009) 858-865.

[18] S.-J. Hwang, C.-H. Chao, An efficient non-interactive deniable authentication protocol with anonymous sender protection, Journal of Discrete Mathematical Sciences and Cryptography 13(3)(2010) 219-231.

[19] F. Li, T. Takagi, Cryptanalysis and improvement of robust deniable authentication protocol, Wireless Personal Communications 69(4)(2013) 1391-1398.

[20] E.-J. Yoon, K.-Y. Yoo, S.-S. Yeo, C. Lee, Robust deniable authentication protocol, Wireless Personal Communications 55(1)(2010) 81-90.

[21] L. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems, Chaos Solitons Fractals 37(3)(2008) 669-674.

[22] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Transactions on Computer Systems 8(1)(1990) 18-36.

[23] M.D. Raimondo, R. Gennaro, New approaches for deniable authentication, in: Proc. the 12th ACM Conference, Computer and Communications Security, 2005.

[24] C.-M. Chen, K.-H. Wang, T.-Y. Wu, J.-S. Pan, H.-M. Sun, A scalable transitive human-verifiable authentication protocol for mobile devices, IEEE Transactions on Information Forensics and Security 8(8)(2013) 1318-1330.

[25] L. Kocarev, S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, Springer-Verlag Berlin Heidelberg, Berlin, 2011.

[26] G. Zeng, W. Zhang, Identity verification in quantum key distribution, Physical Rev. A 61(2)(2000) 22303.

[27] G. Li, Efficient network authentication protocols: lower bounds and optimal implementations, Distributed Computing 9(3)(1995) 131-145.

[28] T. Hwang, K.C. Lee, C.M. Li, Provably secure three-party authenticated quantum key distribution protocols, IEEE Trans, Dependable Secure Comput 4(1)(2007) 71.