Journal of Computers Vol. 29 No. 3, 2018, pp. 109-120
doi:10.3966/199115992018062903010

A Secure Non-interactive Chaotic Maps-based Deniable Authentication Scheme with Privacy Protection in Standard Model

Hongfeng Zhu*, Yan Zhang

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

Received 14 January 2017; Revised 10 May 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 Chaotic Maps-based scheme, named NIDA, aiming to require one ciphertext with non-interactive process for achieve mutual authentication, deniability and the message transmission secretly. Our scheme is based on chaotic maps, which is a high efficient cryptosystem and is firstly used to construct non-interactive deniable authentication scheme. Inadditon, unlike bilinear pairs and other's cryptosystem that need many redundant algorithms to get anonymity, while our scheme can acquire privacy protection easily. Next, a novel idea of our NIDA scheme is to adopt chaotic maps for mutual authentication and privacy protection, not to encrypt/decrypt messages transferred between the sender and the receiver, which can make our proposed scheme much more efficient. Finally, we give the formal security proof about our scheme in the standard model and efficiency comparison with recently related works.

Keywords: BAN logic, chaotic maps, deniability, non-interactive, privacy protection

1 Introduction

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.

Suppose in an online voting system, Alice is a voter and Bob is a manager of vote tally authority, at this time Alice already has a candidate in her mind. But a third party Tom coerces Alice into electing another candidate while she reluctantly agrees to his request. After filling out the candidate, Alice sends her ballot with the authenticator to the manager Bob. So Bob enable validate the ballot if it from the voter Alice, however, there is no way that Bob can prove the source of the ballot is came from Alice to the third party Tom. Even Bob provide the message of the ballot to Tom, the voter Alice also has the right to deny this information, because Bob cannot prove the authenticity of the ballot outside the voting system. Under this circumstance, no one can compel voters to elect the candidate who they objected before. Thus, we find that for the sake of the voters' right in electronic voting system, the deniable authentication protocol is exactly what we required, such protocol is not only enable the ballot authority to identify the given ballot, but also protect the source of the ballot for fear of disclose to the third party.

In the past few years, many scholars dedicated to this field for a stronger protocol. In 1998, Dwork et

* Corresponding Author

al. [1] 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. Later, Deng et al. [3] 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. [4] 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 [5] 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 [6] 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 [7] first proposed a non-interactive deniable authentication protocol based on ElGamal cryptography in 2004. But in 2007, Lee et al. [8] 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 [9] demonstrated a non-interactive deniable authentication scheme in the provable-security direction. Later, Hwang and Chao [10] present a non-interactive deniable authentication protocol with anonymous sender protection in 2010. Subsequently, Li and Takagi [11] proposed an enhanced authentication protocol in 2013 to remove the weakness that disappears in Yoon et al. [12].

In terms of algorithms, Wang et al. [13] and Lee et al. [8] proposed a protocol using generalized ElGamal cryptography in 2005 and 2007 respectively. The same year in 2005, Lu and Cao [14] proposed a new deniable authentication protocol from bilinear pairings. Then, Lu et al. [15] has used Diffie-Hellman algorithm to present the deniable authentication protocol. Afterwards, in 2009, Meng [16] demonstrated a secure non-interactive deniable authentication protocol with strong deniability based on discrete logarithm problem. However, according to the proposed deniable authentication protocols, we find that these protocols only contribute to security protection but overlooked efficiency. Chaotic maps is a stable encryption algorithm, it owns the property of high performance at the same time succeed in security and simple to use. Recently, the quantum deniable authentication schemes [26-27] begin to appear.

The main contributions are shown as below:

(1) Our proposed protocol improves the security level. Because our scheme is proven in the standard model.

(2) Our proposed protocol improves the efficiency. Because our scheme uses the Chebyshev polynomial computation problem which offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. And at the same time, our scheme is non-interactive communication which can reduce the communicating time.

(3) Our proposed protocol can afford privacy protection and our scheme also applies to electronic voting systems.

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 Pseudo-random Function Ensembles

If a function ensemble $F = \{F_n\}_{n\in N}$ is pseudo-random [21], then for every probabilistic polynomial oracle $\mathcal{A}$ and all large enough n, we have that:

$$Adv^F(\mathcal{A}) = |\Pr[\mathcal{A}^{F_n}(1^n) = 1] - \Pr[\mathcal{A}^{G_n}(1^n) = 1]| < \varepsilon(n),$$

where $G = \{G_n\}_{n\in N}$ is a uniformly distributed function ensemble, $\varepsilon(n)$ is a negligible function, $Adv^F = \max_{\mathcal{A}}\{Adv^F(\mathcal{A})\}$ denotes all oracle $\mathcal{A}$, and $Adv^F(\mathcal{A})$ represents the accessible maximum.

2.2 Definition and Hard Problems of Chebyshev Chaotic Maps

Let n be an integer and let x be a variable with the interval $[-1,1]$. The Chebyshev polynomial [22] $T_n(x):[-1,1]\to[-1,1]$ is defined as $T_n(x)=\cos(n\cos^{-1}(x))$. Chebyshev polynomial map $T_n:R\to R$ of degree n is defined using the following recurrent relation:

$$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x),$$
$$\text{where } n\geq 2,\ T_0(x)=1, \text{ and } T_1(x)=x.$$

The first few Chebyshev polynomials are:

$$T_2(x)=2x^2-1,\ T_3(x)=4x^3-3x,\ T_4(x)=8x^4-8x^2+1,\ \ldots$$

One of the most important properties is that Chebyshev polynomials are the so-called semi-group property which establishes that

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

An immediate consequence of this property is that Chebyshev polynomials commute under composition

$$T_r(T_s(x))=T_s(T_r(x)).$$

Zhang [23] proved that semi-group property holds for Chebyshev polynomials defined on interval (-∞,+∞). The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n\left(x\right)=(2xT_{n-1}(x)-T_{n-2}(x))(\bmod N),$$

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 $\mathrm{n}\,(n\in N)$ are defined as: $T_n\left(x\right)=(2xT_{n-1}(x)-T_{n-2}(x))(\bmod p)$, 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, Co mputational 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.

2.3 The Main Scenes about Deniable Authentication Scheme

The framework of Non-interactive Deniable authentication protocol in electronic voting system is shown in 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.

3 The Proposed NIDA Scheme

In this section, we first present a novel Chaotic Maps-based Non-interactive Deniable Authentication scheme which is made up of three steps: Setup, encrypt and dencrypt.

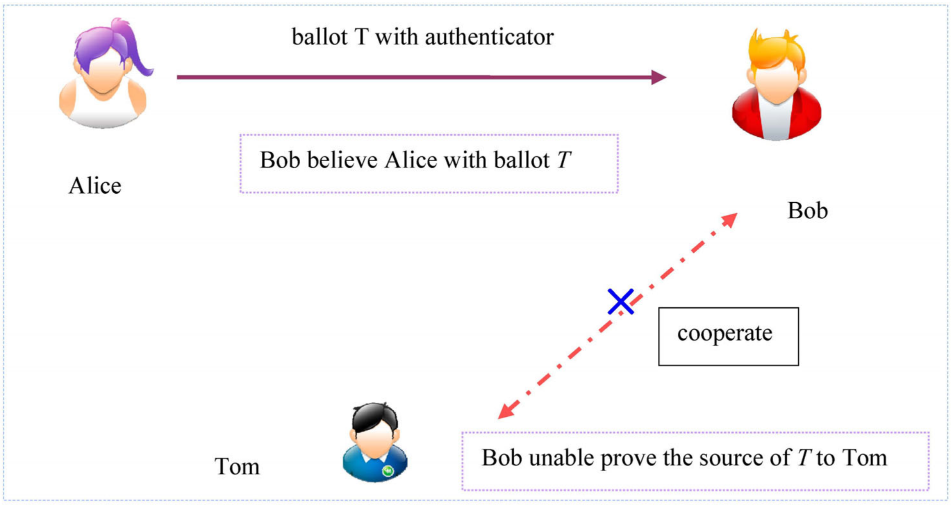
ballot T with authenticator
Alice
Bob believe Alice with ballot T
Bob
cooperate
Tom
Bob unable prove the source of T to Tom

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

3.1 Notations

The concrete notations used hereafter are shown in Table 1.

Table 1. Notations

Symbol	Definition
ID_i	the identity of users
a,b	nonces
$(x,T_{K_i}(x))$	public key of useri based on Chebyshev chaotic maps
K_i	secret key of useri based on Chebyshev chaotic maps
F	pseudo-random function
$\|\|$	concatenation operation

3.2 NIDA Scheme

Fig. 2 illustrates the NIDA scheme.

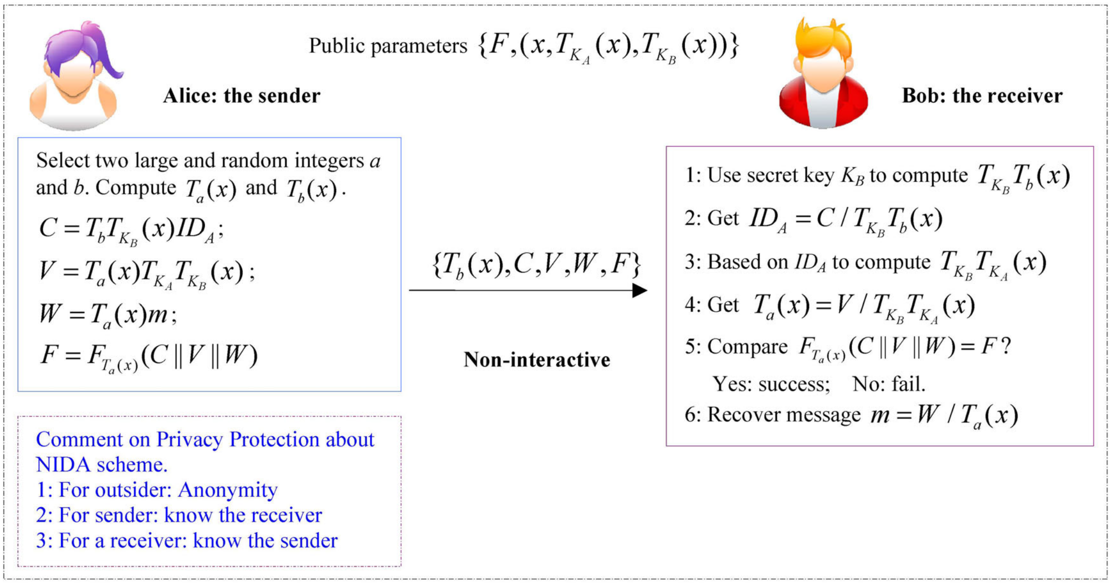
Public parameters $\{F,(x,T_{K_A}(x),T_{K_B}(x))\}$
Alice: the sender
Bob: the receiver
Select two large and random integers a and b. Compute $T_a(x)$ and $T_b(x)$.
$C=T_bT_{K_B}(x)ID_A$;
$V=T_a(x)T_{K_A}T_{K_B}(x)$;
$W=T_a(x)m$;
$F=F_{T_a(x)}(C\|V\|W)$
$\{T_b(x),C,V,W,F\}$
Non-interactive
1: Use secret key K_B to compute $T_{K_B}T_b(x)$
2: Get $ID_A=C/T_{K_B}T_b(x)$
3: Based on ID_A to compute $T_{K_B}T_{K_A}(x)$
4: Get $T_a(x)=V/T_{K_B}T_{K_A}(x)$
5: Compare $F_{T_a(x)}(C\|V\|W)=F$?
Yes: success; No: fail.
6: Recover message $m=W/T_a(x)$
Comment on Privacy Protection about NIDA scheme.
1: For outsider: Anonymity
2: For sender: know the receiver
3: For a receiver: know the sender

Fig. 2 Chaotic maps-based non-interactive deniable authentication scheme with privacy protection scheme

Setup. Simply speaking, for the sender Alice, her public key is $(x,T_{K_A}(x))$ and the corresponding secret key is K_A. For the receiver 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.

Encrypt. When the sender Alice wants to send the message m to the receiver Bob, she chooses two large and random integers a and b. Next, Alice computes $T_a(x)$, $T_b(x)$, $C = T_b T_{K_B}(x) ID_A$, $V = T_a(x) T_{K_A} T_{K_B}(x)$, $W = T_a(x)m$ and $F = F_{T_a(x)}(C \| V \| W)$. Finally, Alice sends $\{T_b(x), C, V, W, F\}$ to the Bob.

Dencrypt.

(1) Upon receiving $\{T_b(x), C, V, W, F\}$ from the sender, Bob can recover the identity of the sender by using secret key KB to compute $T_{K_B} T_b(x)$ and get $ID_A = C / T_{K_B} T_b(x)$.

(2) Based the sender's identity IDA, Bob can get the public key $T_{K_A}(x)$ and compute $T_{K_B} T_{K_A}(x)$ for getting $T_a(x) = V / T_{K_B} T_{K_A}(x)$. This step is also authenticating the sender, if the sender is the "sender", the last step Bob can recover the right message, if not, the recovered message will not be the plaintext.

(3) Bob authenticates the message integrity $F_{T_a(x)}(C \| V \| W) = F$? . If yes, the ciphertext is valid. Otherwise, the ciphertext is invalid or has been damaged during transmission.

(4) Finally, based on their secret key KB, Bob can recover the message $m = \dfrac{W}{V / T_{K_B} T_{K_A}(x)}$.

3.3 Consistency

Let $\{T_b(x), C, V, W, F\}$ be a valid ciphertext, for Bob, we have

$$\frac{W}{V / T_{K_B} T_{K_A}(x)} = \frac{W}{V / T_{K_A} T_{K_B}(x)} = \frac{W}{T_a(x)} = m .$$

4 Security Consideration

4.1 Security Analysis for Security Requirements

Firstly, we discuss three main security attributes: deniability, ciphertext with authentication and privacy protection. Then, we give some attacking method that our scheme can resist naturally. Finally, we give simplified proof about the others' attacks.

The deniability of our scheme.

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

Proof: Fig. 3 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 KA) 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 two large and random integers a and b. Then Bob computes $T_a(x), T_b(x)$, $C = T_b T_{K_B}(x) ID_A$, $V = T_a(x) T_{K_B} T_{K_A}(x)$, $W = T_a(x)m$ and $F = F_{T_a(x)}(C \| V \| W)$. The transcripts $\{T_b(x), C, V, W, F\}$ 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. Furthermore, our proposed scheme has also achieved the strong deniability (Strong deniability [20] means that the sender can deny to have ever authenticated anything to receiver after execution of the protocol).

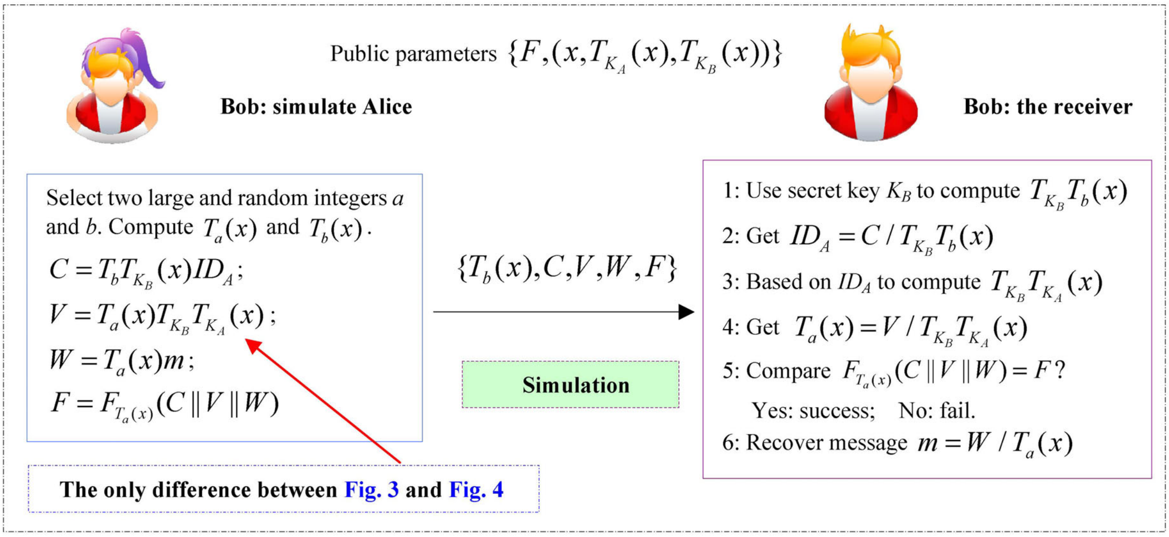
Public parameters $\{F,(x,T_{K_A}(x),T_{K_B}(x))\}$
Bob: simulate Alice
Bob: the receiver
Select two large and random integers a and b. Compute $T_a(x)$ and $T_b(x)$.
$C = T_b T_{K_B}(x) ID_A$;
$V = T_a(x) T_{K_B} T_{K_A}(x)$;
$W = T_a(x)m$;
$F = F_{T_a(x)}(C \| V \| W)$
$\{T_b(x),C,V,W,F\}$
Simulation
1: Use secret key K_B to compute $T_{K_B}T_b(x)$
2: Get $ID_A = C / T_{K_B}T_b(x)$
3: Based on ID_A to compute $T_{K_B}T_{K_A}(x)$
4: Get $T_a(x) = V / T_{K_B}T_{K_A}(x)$
5: Compare $F_{T_a(x)}(C \| V \| W) = F$?
Yes: success; No: fail.
6: Recover message $m = W / T_a(x)$
The only difference between Fig. 3 and Fig. 4

Fig. 3 The simulated processes of proposed scheme

The security of ciphertext with 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 $V = T_a(x)T_{K_A}T_{K_B}(x)$ to covered the secret message m with $W = T_a(x)m$. The encrypted message W is generated from a which is different in each session and is only known by the sender Alice. Bob can decrypt W using his own secret key: the middle process value $T_{K_A}T_{K_B}(x)$ only can be computed by the corresponding receiver which is secure under the CMBDLP and CMBDHP assumptions, and furthermore getting the $m = W / T_a(x)$. Additionally, since the values a of the random elements 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 authentication security.

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

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

Because our proposed scheme is NIDA type with one message without exchanging process, there are many security requirements no need to disscuss (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, b and the another form $T_a(x), T_b(x)$.	Chaotic maps problems
	Impersonation attack	An adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.	All the information includes the ID, (pk_i, sk_i) and some nonces: a, b and the another form $T_a(x), T_b(x)$.	Chaotic maps problems
No freshness verify attacks	Replay attack	A replay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently.	Every important message includes the nonces: a, b and the another form $T_a(x), T_b(x)$.	Chaotic maps problems
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.	Chaotic maps problems

4.2 Security Proof Based on the BAN Logic [2]

For convenience, we first give the description of some notations (Table 4) used in the BAN logic analysis and define some main logical postulates (Table 5) of BAN logic.

Table 4. Notations of the BAN logic

Symbol	Definition
$P \mid\equiv X$	The principal P believes a statement X, or P is entitled to believe X.
$\#(X)$	The formula X is fresh.
$P \mid\Rightarrow X$	The principal P has jurisdiction over the statement X.
$P \lhd X$	The principal P sees the statement X.
$P \mid\sim X$	The principal P once said the statement X.
(X,Y)	The formula X or Y is one part of the formula (X,Y).
$\langle X \rangle_Y$	The formula X combined with the formula Y.
$\{X\}_Y$	The formula X is encrypted under the key K.
$(X)_Y$	The formula X is pseudo-random function with the key K.
$P \overset{K}{\longleftrightarrow} Q$	The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q.
$\xrightarrow{K} P$	The public key of P, and the secret key is described by K^{-1}

Table 5. Logical postulates of the BAN logic

Symbol	Definition	
$\dfrac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P\{X\}_K}{P \mid\equiv Q \mid\sim X}$	The message-meaning rule	(R1)
$\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$	The freshness-conjuncatenation rule	(R2)
$\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$	The nonce-verification rule	(R3)
$\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$	The jurisdiction rule	(R4)
$\dfrac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X}$	The belief rules	(R5)
Remark 3: Molecule can deduce denominator for above formulas.		

Remark. $(X)_Y$ means that the formula X is hash function with the key K. But in our scheme, we redefine $(X)_Y$: the formula X is pseudo-random function with the key K to adopt the standard model.

According to analytic procedures of BAN logic and the requirement of deniable scheme, our NIDA scheme should satisfy the following goals in Table 6. The deniability cannot described by BAN logic, so please see the **Theorem 4.1**.

Table 6. Goals of the proposed scheme

Goals	
Goal 1. $Alice \mid\equiv (Alice \overset{m}{\longleftrightarrow} Bob)$;	Goal 2. $Alice \mid\equiv Bob \mid\equiv (Alice \overset{m}{\longleftrightarrow} Bob)$;
Goal 3. $Bob \mid\equiv (Bob \overset{m}{\longleftrightarrow} Alice)$;	Goal 4. $Bob \mid\equiv Alice \mid\equiv (Bob \overset{m}{\longleftrightarrow} Alice)$;
Where Alice means the sender, Bob means the receiver, and m means the messages.	

First of all, we transform the process of our protocol to the following idealized form.

$(Alice \rightarrow Bob)C : Bob \lhd T_b(x), T_b T_{K_B}(x) ID_A, T_a(x) T_{K_A} T_{K_B}(x), T_a(x)m, (C \| V \| W)_{T_a(x)}$;

According to the description of our protocol, we could make the following assumptions about the initial state, which will be used in the analysis of our protocol in Table 7.

Table 7. Assumptions about the initial state of our protocol

Initial states	
$P_1 : Alice \mid\equiv \xrightarrow{T_{K_B}(x)} Bob$	$P_2 : Bob \mid\equiv \xrightarrow{T_{K_A}(x)} Alice$
$P_3 : Alice \mid\equiv \#(a)$	$P_4 : Alice \mid\equiv \#(b)$
$P_5 : Alice \mid\equiv Alice \xleftrightarrow{T_{K_A}T_{K_B}(x)} Bob$	$P_6 : Bob \mid\equiv Bob \xleftrightarrow{T_{K_B}T_{K_A}(x)} Alice$

Based on the above assumptions, the idealized form of our protocol is analyzed as follows. The main steps of the proof are described as follows:

According to the ciphertext C and P_2, P_6 and attributes of chaotic maps, and relating with R_1, we could get:

$$S_1 : Bob \mid\equiv Alice \mid\sim C$$

Based on the initial assumptions P_3, P_4, and relating with R_2, we could get:

$$S_2 : Bob \mid\equiv \# C$$

Combine $S_1, S_2, P_3, P_4, P_5, P_6, R_3$ and attributes of chaotic maps, we could get:

$$S_3 : Bob \mid\equiv \# ID_A, T_a(x), T_b(x)$$

Based on R_5, we take apart S_3 and get:

$$S_4 : Bob \mid\equiv \# T_b(x),\ S_5 : Bob \mid\equiv \# T_a(x)$$

Combine S_3, S_4 and attributes of chaotic maps, we can get the fresh and privacy protection about Alice's identity.

Combine S_5 and attributes of chaotic maps, we can get the message m for Bob.

Combine. Because Alice and Bob communicate each other just now, they confirm the other is on-line. Moreover, since the Bob can get ID_A from the $T_b T_{K_B}(x) ID_A$ with his own secret key, and based on S_5, R_4 with chaotic maps problems, we could get:

Goal 1. $Alice \mid\equiv (Alice \xleftrightarrow{m} Bob)$; Goal 2. $Alice \mid\equiv Bob \mid\equiv (Alice \xleftrightarrow{m} Bob)$;

Goal 3. $Bob \mid\equiv (Bob \xleftrightarrow{m} Alice)$; Goal 4. $Bob \mid\equiv Alice \mid\equiv (Bob \xleftrightarrow{m} Alice)$;

According to (Goal 1~Goal 4), we know that both sender Alice and the receiver Bob believe that the Bob can authenticate Alice and recover the message based on the fresh nonces a, b and the $\{F, (x, T_{K_A}(x), T_{K_B}(x))\}$.

5 Efficiency Analysis

5.1 The Comparisons among Different Algorithms

Compared with ECC encryption algorithm, Chaotic maps encryption algorithm avoids scalar multiplication and modular exponentiation computation, effectively improves the efficiency. However, Wang [22] proposed several methods to solve the Chebyshev polynomial computation problem. To be more precise, on an Intel Pentium4 2600 MHz processor with 1024 MB RAM, where n and p are 1024 bits long, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, an elliptic curve point multiplication operation and Chebyshev polynomial operation is 0.0005s, 0.0087s, 0.063075s and 0.02102s separately [24]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. According to the results in [25], one pairing operation requires at least 10 times more multiplications in the underlying finite field than a point scalar multiplication in ECC does in the same finite field.

Through the above mentioned analysis, we can reached the conclusion approximately as follows:

$$T_p \approx 10T_m, T_m \approx 3T_c, T_c \approx 2.42T_s, T_s \approx 17.4T_h,$$

we sum up these formulas into one so that it can reflect the relationship among the time of algorithms intuitively.

$$T_p \approx 10T_m \approx 30T_c \approx 72.6T_s \approx 1263.24T_h,$$

where: Tp: Time for bilinear pair operation, Tm: Time for a point scalar multiplication operation, Tc: The time for executing the Tn(x) mod p in Chebyshev polynomial, Ts: Time for symmetric encryption algorithm, Th: Time for Hash operation.

About these algorithms, our proposed multi-receiver scheme only used the chaotic cipher as the main algorithm which is more efficient bilinear pair operation and a point scalar multiplication operation ECC-based. As for Hash operation and pseudo-random function, it can be ignored compared with the other three algorithms.

5.2 The Efficient Usage about Chaotic Maps

Most of chaotic maps-based protocols for achieving key agreement or encrypted messages usually adopt Chaotic Maps-Based Diffie-Hellman (CDH) problem to get the same session key to encrypting/ decrypting messages transferred between user and server [17-19]. But our proposed scheme only uses CDH problem to get temporary key for attaching messages to it, which can make our scheme more efficient, and the users' privacy information is protected. In other words, we change the usage of chaotic maps from the form $E_{T_a T_b(x)}(messages)$ to another form $T_a T_b(x) \cdot messages$, obviously, the latter is much more efficient than the former.

5.3 The Efficiency Comparison

In this section, we make a comparison between the NIDA and two related schemes [9, 11] to judge its function and competence. From Table 8, we can conclude that our scheme is more efficient than the two schemes, because our scheme is mainly based on chaotic maps while the schemes [9, 11] are mainly based on the exponentiation operation. Moreover, Li's scheme is an interactive protocol in random oracle model.

Table 8. Comparisons between our proposed scheme and the related literatures

Protocols (Login and Authentication)			Li et al. [11]	Wang et al. [9]	Ours
Efficiency	Computation	The sender	3Th + 4Te + 1Txor	1Th + 3.5Te	1Tf + 2Tc
		The receiver	3Th + 4Te + 1Txor	1Th + 4.5Te	1Tf + 2Tc
		Total	6Th + 8Te + 2Txor	2Th + 8Te	2Tf + 4Tc
	Communication	Messages	2	1	1
		rounds	2	1	1
Security	Requirements	Provide user anonymity	Yes	Yes	Yes
		Provide mutual authentication	Yes	Yes	Yes
		Provide perfect forward secrecy	Yes	Yes	Yes
		Provide deniability	Yes	Yes	Yes
		Provide strong deniability	No discussion	No discussion	Yes
		Resist replay attack	Yes	Yes	Yes
		Resist man-in-the-middle attack	Yes	Yes	Yes
		Resist insider attack	Yes	Yes	Yes
		Resist impersonation attack	Yes	Yes	Yes
		Resist off-line password guessing attack	Yes	Yes	Yes
	Design	No synchronized	Yes	Yes	Yes
		Non-interactive	No	Yes	Yes
		Number of nonces	2	2	2
		Cryptosystem	Public key cryptography	Public key cryptography	Public key cryptography
		Model	Random Oracle	Random Oracle	Standard Model

6 Conclusion

In this paper, we propose NIDA, a novel scheme towards building a deniable authentication scheme for a sender sending only one encrypted message with some authentication information to the receiver, 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 the hash function is not used, and chaotic maps is adopted to a new encrypted algorithm without using symmetrical encryption, the proposed solution offers significant advantages (the standtard model and high-efficiency) with respect to a traditional deniable authentication protocols. Compared with the related works, our NIDA scheme is not the trade off between security and efficiency, but is comprehensively improved scheme. In the further, the crossing field will be considered, such as qubit deniable authentication scheme, entanglement deniable authentication scheme and so on.

Acknowledgements

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

References

[1] C. Dwork, A. Sahai, Concurrent zero-knowledge: reducing the need for timing constraints, in: H. Krawczyk (Ed.), Advances in Cryptology-Proceedings of CRYPTO 1998, LNCS 1462, Springer-Verlag, Berlin, 1998, pp. 442-457.

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

[3] X. Deng, C.H. Lee, H. Zhu, Deniable authentication protocols, IEE Proceedings Computers and Digital Techniques 148(2)(2001) 101-104.

[4] L. Fan, C.X. Xu, J.H. Li, Deniable authentication protocol based on Diffie-Hellman algorithm, Electronics Letters 38(4)(2002) 705-706.

[5] 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.

[6] T. Feng, T.-F. Ma, Universally composable security concurrent deniable authentication based on witness indistinguishable, Journal of Software 18(11)(2007) 2871-2881.

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

[8] 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.

[9] B. Wang, Z.X. Song, A non-interactive deniable authentication scheme based on designatedverifier proofs, Information Sciences 179(6)(2009) 858-865.

[10] 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.

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

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

[13] Y.J. Wang, J.H. Li, L. Tie, A simple protocol for deniable authentication based on ElGamal cryptography, Networks 45(4)(2005) 193-194.

[14] R.X. Lu, Z.F. Cao, A new deniable authentication protocol from bilinear pairings, Applied Mathematics and Computation 168(2)(2005) 954-961.

[15] R.X. Lu, X.D. Lin, Z.F. Cao, L.Q. Qin, X.H. Liang, A simple deniable authentication protocol based on the Diffie–Hellman algorithm, International Journal of Computer Mathematics 85(9)(2008) 1315-1323.

[16] B. Meng, A secure non-Interactive deniable authentication protocol with strong deniability based on discrete logarithm problem and its application on internet voting protocol, in Information Technology Journal 8(3)(2009) 302-309.

[17] J.H. Yang, T.J. Cao, Provably secure three-party password authenticated key exchange protocol in the standard model, in J. Syst. Softw 85(2012) 340-350.

[18] C. Guo, C.C. Chang, Chaotic maps-based password-authenticated key agreement using smart cards, Communications in Nonlinear Science and Numerical Simulation 18(2013) 1433-1440.

[19] Q. Xie, J.M. Zhao, X.Y. Yu, Chaotic maps-based three-party password-authenticated key agreement scheme, Nonlinear Dyn 74(2013) 1021-1027.

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

[21] P.R. Newswire, Ticketmaster Launches New, Innovative CAPTCHA Solutions, Making The Fan Experience Better, PR Newswire US, 2013.

[22] X. Wang, J. Zhao, An improved key agreement protocol based on chaos, Commun. Nonlinear Sci. Numer. Simul 15(12)(2010) 4052-4057.

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

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

[25] P. Barreto, B. Lynn, M. Scott, On the selection of pairing-friendly groups, in: Proc. International Conference on Selected Areas in Cryptography 3006(2004) 17-25.

[26] W.-M. Shi, J.-B. Zhang, Y.-H. Zhou, Y.-G. Yang, A novel quantum deniable authentication protocol without entanglement, Quantum Information Processing 14(6)(2015) 2183-2193.

[27] W.-M. Shi, Y.-H. Zhou, Y.-G. Yang, Quantum deniable authentication protocol, Quantum Information Processing 13(2014) 1501-1510.