A Novel and Concise Multi-receiver Protocol Based on Chaotic Maps with Privacy Protection

Yang Sun[1], Hongfeng Zhu[2], and Xueshuai Feng[3]
(Corresponding author: Hongfeng Zhu)

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang 110034, P.R. China
(Email:17247613@qq.com[1]; zhuhongfeng1978@163.com[2]; 1275064307@qq.com[3])
(Received Sept. 8, 2015; revised and accepted Feb. 10 & Mar. 9, 2016)

Abstract

Multi-receiver encryption is an essential cryptography paradigm, which can transmit one message securely among the users by the to form over an insecure network. In this paper, we propose a novel Multi-Receiver scheme using Chaotic Maps, named MRCM, aiming to require one ciphertext with non-interactive process for achieve authentication and the message transmission secretly. Our scheme eliminates the private key generators (PKG) in one domain or multi-domain, in other words, our scheme will be highly decentralized and aim to capture distributed. Our goals are to minimize the hazards of single-point of security, single-point of efficiency and single-point of failure about the PKG. Next, our scheme is based on chaotic maps, which is a high efficient cryptosystem and is firstly used to construct multi-receiver public key encryption. Furthermore, unlike bilinear pairs cryptosystem that need many redundant algorithms to get anonymity, while our scheme can acquire privacy protection easily. Moreover, a novel idea of our MRCM scheme is to adopt chaotic maps for mutual authentication and privacy protection, not to encrypt/decrypt messages transferred between the sender and the receivers, 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, multi-receiver, privacy protection

1 Introduction

Multi-receiver encryption is an essential cryptography paradigm, which enables flexible, on-demand, and low computing to transmit one message securely over an insecure network, especially for wire/wireless communications. In 2000, Bellare et al. [1] first proposed the scheme of the multi-receiver in public key encryption. Since then, the growing number of researchers started pay attention to this field, a significant proportion of the protocols have been proposed in various areas, aiming at improving properties and narrowing calculation expense. Generally, in a multi-receiver public key encryption scheme, all users share the common public key encryption system to implement messages sending and receiving. Let us suppose that there are $n+1$ users in the system, including receivers indexed by $1, ..., n$, indicating each receiver have a pair (pk_i, sk_i) as their public and private key for $i = 1, ..., n$ respectively.

If a sender wants to send a message $M_i (i = 1, \cdots, n)$ to n receivers, a sender has to employ all receivers public key to encrypt message, afterwards sends the ciphertexts $(E_i, \cdots, E_n)$ to the common channel. According to the ciphertexts, every receiver picks out respective message and decrypts it by its private key sk_i to catch information. It is worth noting that in this encryption system, the sender and receiver are not invariable, it means each user can become a sender at this moment may also turn to a receiver next time. But we always in a definite model of 1-to-n (one sender-to-n receivers) and single-message $(M_1 = ... = M_i ... = M_n)$ encryption communications. This setting of public key encryption is called as 1-to-n multi-receiver public key encryption system in the following documents [7, 14, 21]. Such as the signcryption mechanism proposed by Sun and Li [22] in 2010, its protocol requires only one or none pairing computation to signcrypt a message for multiple receivers instead of computing bilinear paring repeatedly.

It is generally known that the network platform is insecure for us to communicate, so many researchers put emphasis on keep anonymity [4, 18, 25, 30]. Meanwhile in the field of multiple receivers, researchers also pursue identity privacy protection. In 2013, Wang [24] proposed an anonymous multi-receiver remote data retrieval model for pay-TV in public clouds, which can withstand malicious corporation and consumer. In the same year, Pang et al.

present a novel multi-recipient signcryption scheme [16] with complete anonymity that can achieve both the signer and the receiver anonymity. Motivated by the notion of multi-receiver [1] and identity-based which was presented by Shamir [20], Baek et al. [1] proposed a new multi-receiver identity-based encryption (MR-IBE) scheme in 2005.

In this protocol, a sender encrypt a message to receivers with each identifier information instead of the public key, then each receiver decrypt this message by his private key, which connected with their ID. And different with the protocol of [5], this scheme only needs one or none pairing computation, it is greatly shorten the calculation time. There is no denying the fact that this new model opens a new road for the network security management. Based on this protocol, Fan et al. [8] proposed an anonymous multi-receiver identity-based encryption scheme, it illustrated that the identity of any receiver can be concealed to anyone else. However, in the following years, the researchers conducted a series of improvement [13, 26, 32] to solve this anonymity problem. In the year of 2011, Qin et al. [17] introduced a threshold signcryption scheme, which can solve the problem of single-point failure among a number of participants.

Unlike the previous encryption system for multi-receiver, in this paper, we construct a new efficient scheme based on chaotic maps named MRCM. As a basic algorithm, chaotic maps [9, 12, 23, 28] not only meet the operation efficiency, but also possess strong functionality. Therefore, we utilize traditional public key encryption method which based on chaotic maps to realize information transmission. Besides, as far as we know, it is the very first time that the researchers introduce a chaotic maps-based encryption scheme in the multi-receiver setting.

Due to in the IBE model [1], where the private key is allocated by a trusted private key generator (PKG), the unique private key generator is under great deal of work pressure. If the PKG system collapsed, all of the legal receivers will unable obtain their own private key, which will seriously affect the communication between the sender and receivers. For the purpose of overcome this potential problem, our scheme uses the conventional public/private key pairing (pk_i, sk_i) to achieve message encrypt/decrypt. With this method, the single-point is dispersed into multi-point so that can eliminate the insecurity cased by PKG, and improve the efficiency indirectly. At the same time, different from the scheme which depends on bilinear pairing to obtain anonymity in [24] and [16], endowed with anonymity by nature is our biggest advantage.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Next, a new chaotic maps-based multi-receiver 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 [15], then for every probabilistic polynomial oracle A and all large enough n, we have that:

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

where $G = \{G\}_{n\in N}$ is a uniformly distributed function ensemble, $\varepsilon(n)$ is a negligible function, $Adv^F = max_A\{Adv^F(A)\}$ denotes all oracle A, and $Adv^F(A)$ 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 [27] $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ is defined as $T_n(x) = cos(ncos^{-1}(x))$. Chebyshev polynomial map $T_n : R \rightarrow R$ of degree n is defined using the following recurrent relation:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

where $n \geq 2$, $T_0(x) = 1$, and $T_1(x) = x$.

The first few Chebyshev polynomials are:

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

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

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

In order to enhance the security, Zhang [33] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. The enhanced Chebyshev polynomials are used in the proposed protocol:

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

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. *(Semi-group property) Semi-group property of Chebyshev polynomials:* $T_{rs}(x) = T_r(T_s(x)) = cos(rcos^{-1}(scos^{-1}(x))) = cos(rscos^{-1}(x)) = T_s(T_r(x)) = T_{sr}(x)$, *where* r *and* s *are positive integer and* $x \in [-1, 1]$.

Table 1: Notations

Symbol	Definition
ID_i	The identity of users
$U_i(0 \leq i \leq n)$	The users involved in CRRM scheme
a, b	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
F	Pseudo-random function
$\|\|$	Concatenation operation

Definition 2. *(Chaotic Maps-Based Discrete Logarithm (CDL) problem) Given x and y, it is intractable to find the integer s, such that $T_s(x) = y$. The probability that a polynomial time-bounded algorithm A can solve the CDL problem is defined as $Adv_A^{CDL}(p) = Pr[A(x, y) = r : r \in Z_p^*, y = T_r(x) \bmod p]$.*

Definition 3. *(CDL assumption) For any probabilistic polynomial time-bounded algorithm A, $Adv_A^{CDL}(p)$ is negligible, that is, $Adv_A^{CDL}(p) \leq \varepsilon$, for some negligible function ε.*

Definition 4. *(Chaotic Maps-Based Diffie-Hellman (CDH) problem) Given $x, T_r(x)$ and $T_s(x)$, it is intractable to find $T_{rs}(x)$. The probability that a polynomial time-bounded algorithm A can solve the CDH problem is defined as $Adv_A^{CDH}(p) = Pr[A(x, T_r(x) \bmod p, T_s(x) \bmod p) = T_{rs}(x) \bmod p : r, s \in Z_p^*]$.*

Definition 5. *(CDH assumption) For any probabilistic polynomial time-bounded algorithm A, $Adv_A^{CDH}(p)$ is negligible, that is, $Adv_A^{CDH}(p) \leq \varepsilon$, for some negligible function ε.*

2.3 Definition and Properties of Chebyshev Chaotic Maps [6, 10]

Definition 6. *$f : J \to J$ is said to be topologically transitive if for any pair of open sets $U, V \subset J$, there exists $k > 0$ such that $f^k(U) \cap V \neq \phi$.*

Definition 7. *$f : J \to J$ has sensitive dependence on initial conditions if there exists $\delta > 0$ such that for any $x \in J$ and any neighborhood N of x, there exist $y \in N$ and $n \geq 0$ such that $|f^n(x) - f^n(y)| > \delta$.*

Definition 8. *Let V be a set, then $f : V \to V$ is said to be chaotic on V if*

1) *f has sensitive dependence on initial conditions.*
2) *f is topologically transitive.*
3) *Periodic points are dense in V.*

Definition 9. *Let $f : A \to A, f : B \to B$ be two maps, if there exists a continuous surjection $h : A \to B$ such that $h \cdot g = g \cdot h$, we say that these two maps f and g are topologically semi-conjugate.*

Theorem 1. *A non-zero polynomial is the n^{th} Chebyshev polynomial or its constant times iff the nonzero polynomial is the root of the differential equation*

$$(1 - x^2)y'' - xy' + n^2 y = 0 (n \in Z_+).$$

Lemma 1. *If $f : A \to A, g : B \to B$ are topologically semi-conjugate,*

1) *When p is the periodic point of f, then $h(p)$ is the periodic point of g;*
2) *When the periodic point of f is dense in A, the periodic point of g is dense in B, where h is the topologically semi-conjugate between f and g.*

Lemma 2. *Assume $f : A \to B$ is a map, $A_0, A_1 \subset A$, then $f(A_0 \cap A_1) \subset f(A_0) \cap f(A_1)$.*

Lemma 3. *When $f : A \to A$ is topologically transitive, $g : B \to B$ is topologically semi-conjugate f via h, then g is topologically transitive.*

Lemma 4. *Let $R : S' \to S'$ be a map of the circle into itself, then $R(\theta) = n\theta (n \in Z, n \geq 2)$ is chaotic, where θ is the radian value.*

The concrete proof of chaotic properties can be found in the literature [10] and the enhanced properties of Chebyshev polynomials that defined on interval $(-\infty, +\infty)$ still have the semi-group property (see [33]).

3 The Proposed MRCM Scheme

3.1 Notations

The concrete notations used hereafter are shown in Table 1.

3.2 MRCM Scheme

Figure 1 illustrates the MRCM scheme.

Setup. Simply speaking, for all the users $U_i(0 \leq i \leq n)$, their public keys are $(x, T_{k_i}(x))(0 \leq i \leq n)$ and the corresponding secret keys are $k_i(0 \leq i \leq n)$. And without loss of generality, we assume the user U_0 is

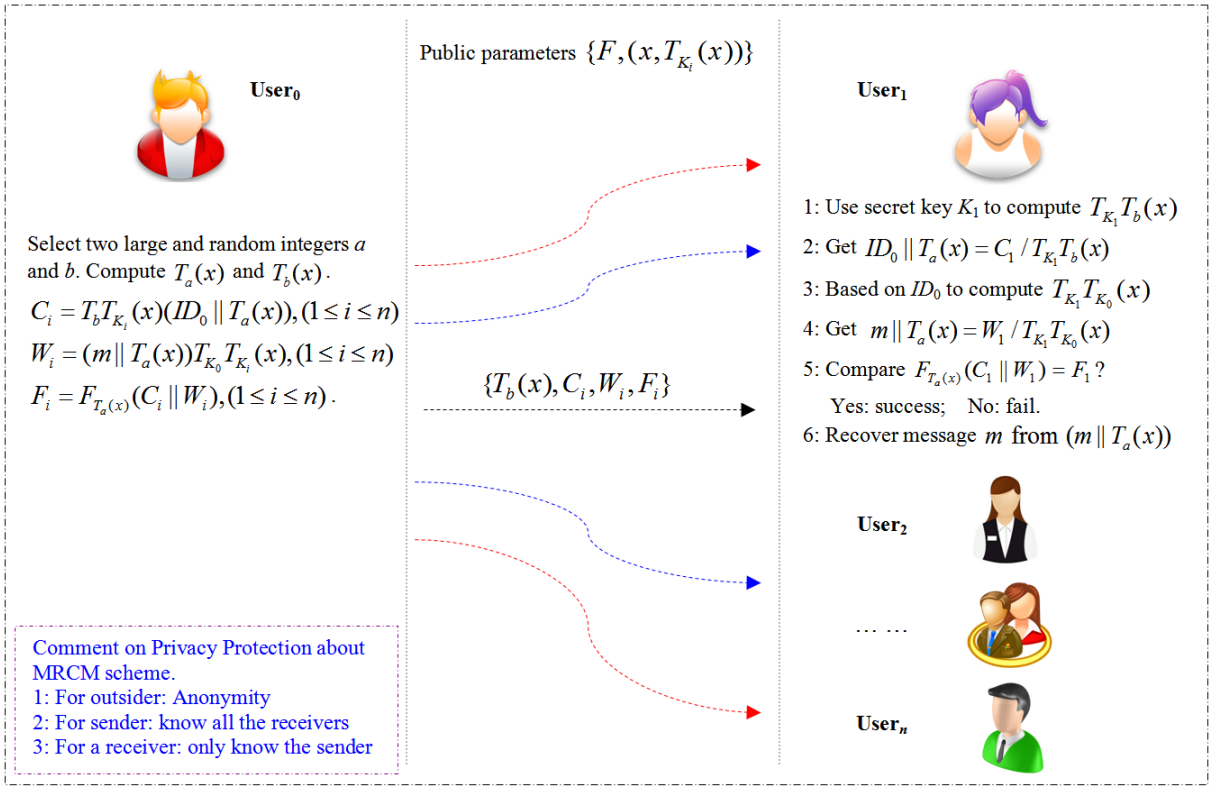

Figure 1: Chaotic maps-based multi-receiver with privacy protection scheme

the sender, and the users $U_i(1 \le i \le n)$ are the receivers. 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 a user U_0 wants to send the same message m to the users $U_i(1 \le i \le n)$, she chooses two large and random integers a and b. Next, U_0 computes $T_a(x)$, $T_b(x)$, $C_i = T_b T_{K_i}(x)(ID_0||T_a(x)), (1 \le i \le n)$, $W_i = (m||T_a(x))T_{K_0}T_{K_i}(x), (1 \le i \le n)$ and $F_i = F_{T_a(x)}(C_i||W_i), (1 \le i \le n)$. Finally, U_0 sends $\{T_b(x), C_i, W_i, F_i\}$ to the users $U_i(1 \le i \le n)$.

Decrypt.

1) Upon receiving $\{T_b(x), C_i, W_i, F_i\}$ from the sender, firstly, any user can recover the identity of the sender by using secret key K_i to compute $T_{K_i}T_b(x)$ and get $ID_0||T_a(x) = C_1/T_{K_1}T_b(x)$.
2) Based the sender's identity ID_0, U_i can get the public key $T_0(x)$ and compute $T_{K_i}T_{K_0}(x)$ for getting $m||T_a(x) = W_1/T_{K_1}T_{K_0}(x)$. This step is also authenticating the sender, if the sender is the "sender", the last step any user can recover the right message, if not, the recovered message will not be the plaintext.
3) U_i authenticates the message integrity $F_{T_a(x)}(C_1||W_1) = F_1$?. If yes, the cipher-text is valid. Otherwise, the cipher-text is invalid or has been damaged during transmission.
4) Finally, based on their secret key K_i, any user in the group can recover the message $m = \frac{W_i}{T_{K_i}T_{K_0}(x)} - T_a(x) = \frac{W_i}{T_{K_i}T_{K_0}(x)} - (\frac{C_i}{T_{K_i}T_b(x)} - ID_0)$.

3.3 Consistency

Let $\{T_b(x), C_i, W_i, F_i\}$ be a valid ciphertext, for any user U_i, we have

$$\begin{aligned} & \frac{W_i}{T_{K_i}T_{K_0}(x)} - (\frac{C_i}{T_{K_i}T_b(x)} - ID_0) \\ = & \frac{W_i}{T_{K_i}T_{K_0}(x)} - (ID_0||T_a(x) - ID_0) \\ = & \frac{W_i}{T_{K_i}T_{K_0}(x)} - T_a(x) \\ = & m||T_a(x) - T_a(x) \\ = & m. \end{aligned}$$

4 Security Consideration

4.1 Security Analysis for Security Requirements and the Comparisons

There are many security requirements about protocol type. Because our proposed scheme is multi-receiver type with one message without exchanging process, there are

Table 2: Definition and the reasons why we do not discuss

Attack Type	Security Requirements	Definition	Reasons why we do not discuss
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
	Losing 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

many security requirements no need to discuss (see Table 2).

Next, from the Table 3, we can see that the proposed scheme can provide known secure session key agreement, impersonation attack and so on.
Some other security attributes:

1) The security of one ciphertext with some authentications.

Theorem 2. *Our proposed scheme is one ciphertext security 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: each message must mix with a large random nonce and any public key cannot be used to encrypt secret message directly. Therefore, we construct $W_i = (m||T_a(x))T_{K_0}T_{K_i}(x)$, $(1 \leq i \leq n)$ to covered the secret message m. The encrypted message W_i is generated from a which is different in each session and is only known by the sender U_0. Any receiver can decrypt W_i using his/her own secret key, but the decrypted process is completely different: The middle process value $T_{K_0}T_{K_i}(x)$ only can be computed by the corresponding receiver which is secure under the CMBDLP and CMBDHP assumptions, and furthermore getting the $m = m||T_a(x) - T_a(x)$. 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 one ciphertext security. □

2) The security of privacy protection.

Theorem 3. *Our proposed scheme is privacy protection partly under the CMBDLP and CMBDHP assumptions.*

Proof. We divide the participants into three characters: the sender, the receivers and the outsiders (including attacker, any curious nodes and so on). The sender's identity is anonymity for outsiders because ID_0 is covered by $C_i = T_bT_{K_i}(x)(ID_0||T_a(x)), (1 \leq i \leq n)$, and then only the legal receivers can use his/her secret key to recover the ID_0. Due to PKC-based about our scheme, the ID_0 must be emerged to the legal receivers, or they cannot know the public key of the sender. The sender must know the receiver's identity because our scheme is adopted PKC and chaotic maps. All the receivers cannot know the others receivers because they only recover the corresponding C_i using their own secret key.

Table 3: Definition and simplified proof

Attack Type	Security Requirements	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

We construct $C_i = T_b T_{K_i}(x)(ID_0||T_a(x)), (1 \leq i \leq n)$ to covered the sender's identity. The encrypted message C_i is generated from b which is different in each session and is only known by the sender U_0. Any receiver can decrypt C_i using $T_b(x)$ and his/her own secret key, but the decrypted process is completely different: the middle process value $T_{K_i}T_b(x)$ only can be computed by the corresponding receiver which is secure under the CMBDLP and CMBDHP assumptions, and furthermore getting the $ID_0||T_a(x) = C_i/T_{K_i}T_b(x)$, you can get ID_0 and $T_a(x)$ in the same time. Additionally, since the values b of the random elements is very large, attackers cannot directly guess the values a of the random elements to generate $T_b(x)$. Therefore, the proposed scheme provides privacy protection.

The privacy protection of our MRCM scheme belongs to the ID hiding(a user may use a resource or service without disclosing the user's identity during the protocol interaction), anyway, we must emphasize three points:

a. Any outsider cannot get any ID information (sender or receivers) about our proposed scheme.

b. Only the sender knows the ID information of all receivers.

c. Any receiver cannot get any other receiver's ID information. We sum up the privacy protection of our scheme in the Table 4.

□

4.2 Security Proof Based on the BAN Logic

For convenience, we first give the description of some notations (Table 5) used in the BAN logic analysis and define some main logical postulates (Table 6) of BAN logic [3].

Remark 1. *$(X)_K$ means that the formula X is hash function with the key K. But in our scheme, we redefine $(X)_K$: 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 multi-receiver scheme, our MRCM scheme should satisfy the following goals in Table 7.

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

$$(U_0 \to U_i)C : U_i \lhd T_b(x), T_b T_{K_i}(x)(ID_0||T_a(x)),$$

$$(m||T_a(x))T_{K_0}T_{K_i}(x), (C_i||W_i)_{T_a(x)};$$

According to the description of our protocol, we could make the following assumptions about the initial state,

Table 4: Privacy protection comparisons

Security attributes		[19] 2009	[31] 2010	[16] 2013	Ours
Missing encrypted identity attacks	For outsiders	No	Yes	Yes	Yes
	For receivers	No	No	No	No
Receiver anonymity	For outsiders	No	No	Yes	Yes
	For other receivers	No	No	No	Yes
	For the sender	No	No	No	No

Table 5: 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_K	The formula X is encrypted under the key K.
$(X)_K$	The formula X is hash function with the key K. If there is no K, and that means is no key input.
$P\overset{K}{\longleftrightarrow}Q$	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.
$\overset{K}{\longrightarrow}P$	The public key of P, and the secret key is described by K^{-1}.

Table 6: Logical postulates of the BAN logic

Symbol	Definition
$\frac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q,P\{X\}_K}{P\mid\equiv Q\mid\sim X}$	The message-meaning rule (R_1)
$\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$	The freshness-conjunction rule (R_2)
$\frac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$	The nonce-verification rule (R_3)
$\frac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$	The jurisdiction rule (R_4)
$\frac{P\mid\equiv Q\mid\equiv(X,Y)}{P\mid\equiv Q\mid\equiv X}$	The belief rules (R_5)
Remark 3: Molecule can deduce denominator for above formulas.	

Table 7: Goals of the proposed scheme

Goals
Goal 1. $U_0\mid\equiv(U_0\overset{m}{\longleftrightarrow}U_i)$; Goal 2. $U_0\mid\equiv U_i\mid\equiv(U_0\overset{m}{\longleftrightarrow}U_i)$;
Goal 3. $U_i\mid\equiv(U_i\overset{m}{\longleftrightarrow}U_0)$; Goal 4. $U_i\mid\equiv U_0\mid\equiv(U_i\overset{m}{\longleftrightarrow}U_0)$;
Where U_0 means the sender, $U_i(1\leq i\leq n)$ means the $n-receiver$, and m means the messages.

Table 8: Assumptions about the initial state of our protocol

Initial states	
$P_1 : U_0\| \equiv \xrightarrow{T_{K_i}(x)} U_i$	$P_2 : U_i\| \equiv \xrightarrow{T_{K_0}(x)} U_0$
$P_3 : U_0\| \equiv \#(a)$	$P_4 : U_0\| \equiv \#(b)$
$P_5 : U_0\| \equiv U_0 \xleftrightarrow{T_{K_0}T_{K_i}(x)} U_i$	$P_6 : U_i\| \equiv U_i \xleftrightarrow{T_{K_i}T_{K_0}(x)} U_0$

which will be used in the analysis of our protocol in Table 8.

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:

$$S_1 : U_i\| \equiv U_0\| \sim C_i.$$

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

$$S_2 : U_i\| \equiv \sharp C_i.$$

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

$$S_3 : U_i\| \equiv \sharp ID_0, T_a(x), T_b(x).$$

Based on R_5, we take apart S_3 and get:

$$S_4 : U_i\| \equiv \sharp T_b(x), S_5 : U_i\| \equiv \sharp T_a(x).$$

Combine S_3, S_4 and attributes of chaotic maps, we can get the fresh and privacy protection about sender's identity. Combine S_5 and attributes of chaotic maps, we can get the message m for all the $U_i(1 \le i \le n)$.

Combine 1. *Because the 1-to-n parties (U_0 and $U_i(1 \le i \le n)$) communicate each other just now, they confirm the other is on-line. Moreover, since the $U_i(1 \le i \le n)$ can get ID_0 and $T_a(x)$ from the $T_bT_{K_i}(x)(ID_0||T_a(x))$ with his own secret key, and based on S_5, R_4 with chaotic maps problems, we could get:*

Goal 1. $U_0\| \equiv (U_0 \xleftrightarrow{m} U_i)$;

Goal 2. $U_0\| \equiv U_i\| \equiv (U_0 \xleftrightarrow{m} U_i)$;

Goal 3. $U_i\| \equiv (U_i \xleftrightarrow{m} U_0)$;

Goal 4. $U_i\| \equiv U_0\| \equiv (U_i \xleftrightarrow{m} U_0)$;

According to (Goal 1 $\sim$ Goal 4), we know that both sender U_0 and receivers $U_i(1 \le i \le n)$ believe that the $U_i(1 \le i \le n)$ can authenticate U_0 and recover the message based on the fresh nonces a, b and the $(pk_i, sk_i)(0 \le i \le n)$.

5 Efficiency Analysis

5.1 The Comparisons among Different Algorithms

Compared to RSA[1], ECC[2] and Bilinear map[3], Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. Chaotic maps encryption algorithm: As a special form of motion, Chaos means that in a certain nonlinear system can appear similar to the behavior of random phenomena without needing any random factors. Chaotic system has the characteristics of certainty, boundness, sensibility to initial parameters and unpredictability, etc. Chaotic maps encryption algorithm utilizes the unique semi-group mature of Chebyshev chaotic maps, based on two difficult problems-the chaotic maps discrete logarithm problem and the chaotic maps Diffie-Hellman problem, puts forward a kind of encryption algorithm. Compared with ECC encryption algorithm, Chaotic maps encryption algorithm avoids scalar multiplication and modular exponentiation computation, effectively improves the efficiency. However, Wang [27] 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 [11]. Moreover, the computational cost of XOR operation could be ignored when compared with other

[1] **RSA encryption algorithm:** RSA encryption algorithm is a kind of algorithm based on big integer factorization, its public keys and secret keys are the function of two large prime numbers (Which large prime numbers are more than 100 digits of decimal.). RSA encryption algorithm, as the first algorithm which can be used to encryption and digital signature, is easily to understand and operate.

[2] **ECC encryption algorithm:** ECC encryption algorithm is a kind of public-key cryptosystem algorithm, its mathematical theory is that using the rational points on the Elliptic curve constitutes Abel additive group, and utilizes the computational difficulty of discrete logarithm.

[3] **Bilinear map:** In mathematics a pairing function is a process to uniquely encode two natural numbers into a single natural number. In mathematics, a bilinear map is a function combining elements of two vector spaces to yield an element of a third vector space. It is called bilinear because it is linear in each of its arguments.

operations. According to the results in [2], 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 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 9 given the comparison for RSA, ECC and Chaotic maps.

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 (see the Table 10). 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 $ChaoticMaps-BasedDiffie-Hellman(CDH)problem$ to get the same session key to encrypting/decrypting messages transferred between user and server [9, 28, 29]. But our proposed scheme only uses $CDHproblem$ to get temporary key for attaching messages to it, which can make our scheme more efficient, and the users's privacy information is protected. In other words, we change the usage of chaotic maps from the form $E_{T_aT_b(x)}(messages)$ to another form $T_aT_b(x) \cdot (messages)$, obviously, the latter is much more efficient than the former.

5.3 The Comparisons among Our MRCM Scheme and the Related Literatures

In this section, we make a comparison between the MRCM and other multi-receiver scheme to judge its function and competence. From Table 10, we can conclude that our scheme is more efficient than the others.

6 Conclusion

In this paper, we propose MRCM, a novel scheme towards building a PKC-based scheme for a sender sending only one encrypted message with some authentication information to multi-receiver, and at the same time, achieving privacy protection. The core idea we have followed is that the most existing multi-receiver schemes are bilinear pairing-based, 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 standard model and high-efficiency) with respect to a traditional multi-receiver protocols. Compared with the related works, our MRCM scheme is not the trade off between security and efficiency, but is comprehensively improved scheme.

Acknowledgments

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

References

[1] J. Baek, R. Safavinaini and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," *Lecture Notes in Computer Science*, vol. 3386, pp. 380–397, Springer, 2005.

[2] P. S. L. M. Barreto, B. Lynn and M. Scott, "On the selection of pairing-friendly groups," in *Selected Areas in Cryptography*, LNCS 3006, pp. 17–25, Springer-Verlag, 2004.

[3] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, pp. 18–36, 1990.

[4] H. L. Chan, X. Deng, H. Zhu, "Design and security analysis of anonymous group identification protocols," *Lecture Notes in Computer Science*, vol. 2274, pp. 188–198, Springer, 2002.

[5] B. Dan, M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[6] R. L. Devaney, J. P. Eckmann, "An introduction to chaotic dynamical systems," *Mathematical Gazette*, vol. 19, no. 2, pp. 204–205, 1990.

[7] E. Ekrem, S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2165–2177, 2013.

[8] C. Fan, L. Y. Huang and P. H. Ho, "Anonymous multi receiver identity-based encryption," *IEEE Transactions on Computers*, vol. 59, no. 9, pp. 1239–1249, 2010.

[9] C. Guo, C. C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 1433–1440, 2013.

Table 9: Comparison for RSA, ECC and Chaotic maps

	RSA encryption algorithm	ECC encryption algorithm	Chaotic maps encryption algorithm
Items	Differences		
Mathematical basis	Large prime number	Elliptic curve	Chebyshev polynomial
Difficult problem assumptions	large prime factorization problem	Discrete logarithm calculation problem on the elliptic curve	Chaotic maps discrete logarithm problem, Chaotic maps Diffie-Hellman problem
Operation Cost	√ √	√ √ √	√ √ √
Operation Speed	√	√ √	√ √ √
Security Level	√	√ √ √	√ √ √
Normal √	Good √ √	Excellent √ √ √	

Table 10: Comparisons between our proposed scheme and the related literatures

Phase	Some property	[19] 2009	[31] 2010	[16] 2013	Ours
Encrypt	Number of parameters	$n+9$	13	10	2
	Computation Complexity	$(n+1)T_a + (n+3)T_m + T_e + 2T_h$	$T_p + (m+n+1)T_m + (2m+n+3)T_e + 2T_h$	$T_p + 2T_a + 6T_m + T_e + 2T_h$	$nT_f + 2nT_c + 2nT_{mo}$
	Ciphertext length	$3\|G_1\| + \|M\| + n\|ID\|$	$(m+n+2)\|G_1\| + \|M\| + m\|ID\|$	$(n+4)\|G_1\| + \|M\|$	$(2n+1)\|G_2\| + n\|F\|$
Decrypt	Ciphertext validity or integrity	$3T_p + 2T_a + (3n+3)T_m + 2T_e + (n+1)T_h$	$(m+5)T_p + T_a + (m+\|M\|+2)T_m + 2T_h$	$2T_p + T_a + T_m + T_h$	T_f
	Authorized or not	$3T_p + 2T_a + (3n+3)T_m + 2T_e + (n+1)T_h$	$(m+5)T_p + T_a + (m+\|M\|+2)T_m + 2T_h$	$2T_p + T_a + T_m + T_h$	No need
	Decryption	$3T_p + 2T_a + (3n+3)T_m + 2T_e + (n+1)T_h$	$(m+5)T_p + T_a + (m+\|M\|+2)T_m + 2T_h$	$2T_p + nT_a + (n-1)T_m + 2T_h$	$2T_c + 2T_{mo}$
Model		Random Oracle	Random Oracle	Random Oracle	Standard Model

T_p: Time for bilinear pair operation
T_a: Time for addition operation
T_m: Time for a point scalar multiplication operation
T_{mo}: Time for integer multiplication operation in the field
T_e: Time for exponentiation operation
T_h: Time for Hash operation
T_s: Time for symmetric encryption algorithm
T_c: The time for executing the $T_n(x)$ mod p in Chebyshev polynomial using the algorithm in literature [33].
T_f: Time for pseudo-random function

$|G_1|$: The length of the elements in G_1; $|G_2|$: The length of the elements in G_2; $|ID|$: the length of ID;
Let G_1 be an additive group and G_2 be a multiplicative group with the same prime order q;
$|M|$: The length of the plaintext M; $|F|$: the length of the output of pseudo-random function.
m: The number of signers/sender (m=1 in schemes [16, 19, 31] and our scheme); n: the number of receivers.

Random Oracle: A random oracle is a random mathematical function, that is, a function mapping each possible query to a (fixed) random response from its output domain, for example, regarding hash function as a real random mathematical function in the practical application.
Standard Model: The standard model is the model of computation in which the adversary is only limited by the amount of time and computational power available, without using a random mathematical function.

[10] J. C. Jiang, Y. H. Peng, "Chaos of the Chebyshev polynomials," *Natural Science Journal of Xiangtan University*, vol. 19, no. 3, pp. 37–39, 1996.

[11] L. Kocarev, S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*, pp. 53–54, 2011.

[12] C. C. Lee, D. C. Lou, C. T. Li, C. W. Hsu, "An extended chaotic-maps-based protocol with key agreement for multi server environments," *Nonlinear Dynamics*, vol. 76, no. 1, pp. 853–866, 2014.

[13] H. Li, L. Pang, "Cryptanalysis of Wang et al.'s improved anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 8, no. 1, pp. 8–11, 2014.

[14] J. Minonzio, M. Talmant and P. Laugier, "Multi-emitters and multi-receivers probe for long cortical bone assessment," *Journal of the Acoustical Society of America*, vol. 127, no. 3, pp. 2032–2035, 2010.

[15] PR Newswire, "Ticketmaster Launches New, Innovative CAPTCHA Solutions, Making The Fan Experience Better," *PR Newswire*, US, 2013. (`http://www.prnewswire.com/news-releases/ticketmaster-launches-new-innovative-captcha-solutions-making-the-fan-experience-better-189000181.html`)

[16] L. Pang, H. Li, L. Gao, Y. Wang, "Completely anonymous multi-recipient signcryption scheme with public verification," *PLoS ONE* vol. 8, no. 5, 2013.

[17] H. Qin, Y. Dai and Z. Wang, "Identity-based multi-receiver threshold signcryption scheme," *Security and Communication Networks*, vol. 4, no. 11, pp. 1331–1337, 2011.

[18] K. R. Santosh, C. Narasimham, and P. Shetty, "Cryptanalysis of multi-prime RSA with two decryption exponents," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 40–44, 2016.

[19] S. S. D. Selvi, S. S. Vivek, R. Srinivasan, C. P. Rangan, "An efficient identity-based signcryption scheme for multiple receivers," in *Proceedings of the 4th International Workshop on Security*, pp. 71–88, 2009.

[20] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Lecture Notes in Computer Science*, vol. 196, pp. 47–53, Springer, 1985.

[21] Z. Shen, H. Yu, Y. Hu and C. Shen, "Joint symbol detection for multi-receiver without signal synchronization and array alignment," *IEEE Communications Letters*, vol. 18, no. 10, pp. 1755–1758, 2014.

[22] Y. X. Sun, H. Li, "Efficient signcryption between TPKC and IDPKC and its multi-receiver construction," *Science in China. Series F: Information Sciences*, vol. 53, no. 3, pp. 557–566, 2010.

[23] Z. Tan, "A chaotic maps-based authenticated key agreement protocol with strong anonymity," *Nonlinear Dynamics*, vol. 72, pp. 311–320, 2013.

[24] H. Wang, "Anonymous multi-receiver remote data retrieval for pay-TV in public clouds," *IET Information Security*, vol. 9, no. 2, pp. 108–118, 2015.

[25] H. Wang, H. Zhang, J. Li and X. U. Chen, "A(3,3) visual cryptography scheme for authentication," *Journal of Shenyang Normal University(Natural Science Edition)*, vol. 31, no. 3, pp. 397–400, 2013.

[26] H. Wang, Y. Zhang, H. Xiong and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 6, no. 1, pp. 20–27, 2012.

[27] X. Wang, J. Zhao, "An improved key agreement protocol based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, pp. 4052–4057, 2010.

[28] Q. Xie, J. Zhao, X. Yu, "Chaotic maps-based three-party password-authenticated key agreement scheme," *Nonlinear Dynamics*, vol. 74, pp. 1021–1027, 2013.

[29] J. H. Yang, T. J. Cao, "Provably secure three-party password authenticated key exchange protocol in the standard model," *Journal of Systems and Software*, vol. 85, pp. 340–350, 2012.

[30] E. J. Yoon, K. Y. Yoo, J. W. Hong, S. Y. Yoon, D. I. Park and M. J. Choi, "An efficient and secure anonymous authentication scheme for mobile satellite communication systems," *Eurasip Journal on Wireless Communications and Networking*, vol. 10, pp. 1687–1695, 2011.

[31] B. Zhang, Q. Xu, "An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model," in *Proceedings of the AST/UCMA/ISA/CAN Conferences*, pp. 15–27, 2010.

[32] J. Zhang, J. Mao, "An improved anonymous multi-receiver identity-based encryption scheme," *International Journal of Communication Systems*, vol. 28, pp. 645–658, 2015.

[33] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos Solitons Fractals*, vol. 37, no. 3, pp. 669–674, 2008.

Yang Sun obtained his master degree in Information Science and Engineering from Northeastern University. Yang Sun is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a department head of network engineering. He has research interests in wireless networks, mobile computing, cloud computing, social networks and network security. Yang Sun had published more than 15 international journal and international conference papers on the above research fields.

Hongfeng Zhu obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Dr. Zhu had published more than 50 international journal papers (SCI or EI journals) on the above research

fields.

Xueshuai Feng graduated with a Bachelor of Engineering from Shenyang Normal University in 2015. In his college, after completing the learning task, he interests in exploring his professional knowledge. During graduate, under the guidance of his master instructor, he researches IoT security theory and technology.