*Journal of Information Hiding and Multimedia Signal Processing* ©2016 ISSN 2073-4212
**Ubiquitous International** Volume **7**, Number **4**, July **2016**

# Using Chaotic Maps to Construct Anonymous Multi-receiver Scheme Based on BAN Logic

Hongfeng Zhu
Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 China
zhuhongfeng1978@163.com

Dan Zhu
School of Foreign Languages
Shenyang Jianzhu University
No.9, HunNan East Street, HunNan District, Shenyang, P.C 110168 China
zhudan413@163.com

Yan Zhang
Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 China
1505733680@qq.com

Received June, 2015; revised September, 2015

Abstract. *Multi-receiver public key encryption is an essential cryptography paradigm, which enables flexible, on-demand, and low computing to transmit one message securely among the users by the to form over an insecure network. In this paper, we propose a novel Chaotic Maps-based Multi-Receiver scheme, named CMMR, aiming to require one ciphertext with non-interactive process for achieve authentication and the message transmission secretly. Compared with Multi-receiver Identity-Based Encryption (MRIBE), our proposed scheme mainly owns three merits: (1) One is to eliminate 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. (2) The other is that our scheme is based on chaotic maps, which is a high efficient cryptosystem and is firstly used to construct multi-receiver public key encryption. (3) The last merit is the most important: Unlike bilinear pairs cryptosystem that need many redundant algorithms to get anonymity, while our scheme can acquire privacy protection easily. Next, a novel idea of our CMMR 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:** Multi-receiver; Privacy Protection; Ban logic; Chaotic maps

1. **Introduction.** Multi-receiver encryption is one of the most important cryptographic primitive in 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 $n$ 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 $M_i(i = 1, ..., n)$ to $n$ receivers, a sender has to employ all receivers public key to encrypt message, afterwards sends the ciphertexts $(E_1, ..., E_n)$ 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 $(M_1 = \ldots = M_i \ldots = M_n)$ encryption communications. This setting of public key encryption is called as 1-to-n multi-receiver public key encryption system in the following documents [2-4]. Such as the signcryption mechanism proposed by Sun and Li [5] 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 [6-8]. Meanwhile in the field of multiple receivers, researchers also pursue identity privacy protection. In 2013, Wang [9] 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 [10] with complete anonymity that can achieve both the signers and the receivers anonymity. Motivated by the notion of multi-receiver [1] and identity-based which was presented by Shamir [11], Baek et al. [12] proposed a new multi-receiver identity-based encryption (MR-IBE) scheme in 2005. In this protocol, a sender encrypt a message to n 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 [13], 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. [14] 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 [15-17] to solve this anonymity problem. In the year of 2011, Qin et al. [18] 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 CMMR (Chaotic Maps-based Multi-Receiver). As a basic algorithm, chaotic maps [19, 20, 28, 29] 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 [12], 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 [9] and [10], 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 [21], then for every probabilistic polynomial oracle $A$ and all large enough $n$, we have that:

$$A^{G_n}(1^n) = 1]| < \varepsilon(n)$$

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

2.2. **Definition and hard problems of Chebyshev chaotic maps[22-25].** 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 $T_n(x) = \cos(ncos^{-1}(x))$.Chebyshev polynomial map $T_n : R \to R$ of degree $n$ is defined using the following recurrent relation:

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

The first few Chebyshev polynomials are:
$T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$,...... 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 [23] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. The enhanced Chebyshev polynomials are used in the proposed protocol:

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

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

**Definition 2.2.** *(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 2.3.** *(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 $\varepsilon$.*

**Definition 2.4.** *(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 2.5.** *(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 $\varepsilon$.*

3. **The Proposed CMMR Scheme.** In this section, we first present a novel Chaotic Maps-based Multi-Receiver scheme which is made up of three steps: Setup, encrypt and dencrypt.

3.1. **Notations.** The concrete notations used hereafter are shown in Table1.

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 |

3.2. **CMMR Scheme.** Fig.1 illustrates the CMMR 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 the sender, and the users $U_i(1 \leq i \leq n)$ 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 $U_i(1 \leq i \leq n)$,she chooses two large and random integers $a$ and $b$.Next, $U_0$ computes $T_a(x), T_b(x)$, $C_i = T_bT_{K_i}(x)ID_0, (1 \leq i \leq n)$, $V_i = T_a(x)T_{K_0}T_{K_i}(x), (1 \leq i \leq n)$, $W = T_a(x)m$ and $F_i = F_{T_a(x)}(C_i||V_i||W), (1 \leq i \leq n)$.Finally, $U_0$ sends $T_b(x), C_i, V_i, W, F_i$ to the users $U_i(1 \leq i \leq n)$. **Decrypt.**
(1) Upon receiving $\{T_b(x), C_i, V_i, W, F_i\}$ 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 $ID_0 = C_i/T_{K_i}T_b(x)$.
(2) Based the senders identity $ID_0$, $U_i$ can get the public key $T_0(x)$
and compute $T_{K_i}T_{K_0}(x)$ for getting $T_a(x) = V_i/T_{K_i}T_{K_0}(x)$.This step is also authenticating the sender, if the sender is the sender, the last step any user can recover the right message,

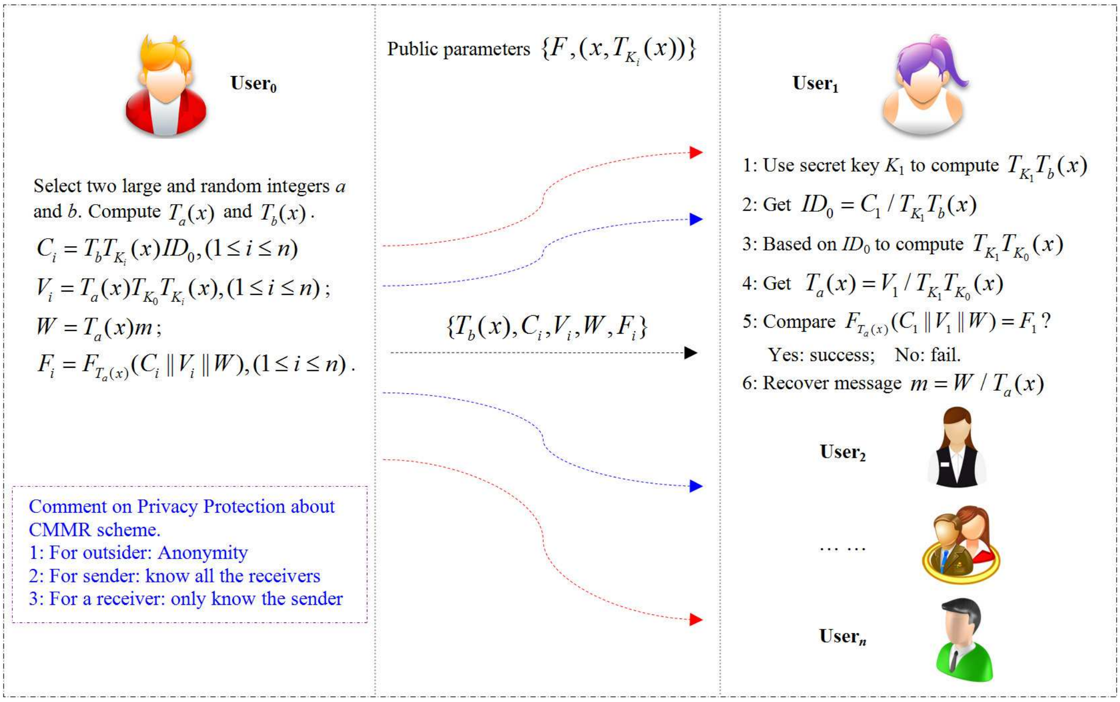


FIGURE 1. Chaotic maps-based multi-receiver with privacy protection scheme

if not, the recovered message will not be the plaintext.
(3)$U_i$ authenticates the message integrity $F_{T_a(x)}(C_1||V_1||W) = F_1$?.If yes, the ciphertext is valid. Otherwise, the ciphertext 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 $m = \frac{W}{V_i/T_{K_i}T_{K_0}(x)}$.

3.3. **Consistency.** Let $\{T_b(x), C_i, V_i, W, F_i\}$ be a valid ciphertext, for any user $U_i$, we have

$$\frac{W}{V_i/T_{K_i}T_{K_0}(x)} = \frac{W}{V_i/T_{K_0}T_{K_i}(x)} = \frac{W}{T_a(x)} = m$$

3.4. **Discuss privacy protection.** Privacy protection can be classified into two types:
(1) One is anonymity, which ensures that a user may use a resource or service without disclosing the users identity completely.
(2) The other is ID hiding, which usually means that a user may use a resource or service without disclosing the users identity during the protocol interaction, which is a kind of privacy protection partly. A pseudonym is an identifier of a subject other than one of the subjects real names. ID hiding usually uses pseudonym to realize.
The privacy protection of our CMMR scheme belongs to the ID hiding, anyway, we must emphasize three points:
(1) Any outsider cannot get any ID information (sender or receivers) about our proposed scheme.
(2) Only the sender knows the ID information of all receivers.
(3) Any receiver cannot get any other receivers ID information.

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

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

| Attack Type | Security Requirements | 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 known secure session key agreement, impersonation attack and so on.

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 |

Some other security attributes (1) The security of one ciphertext with some authentications

**Theorem 4.1.** *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 $V_i = T_a(x)T_{K_0}T_{K_i}(x), (1 \leq i \leq n)$ 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 $U_0$.Any receiver can decrypt $W$ 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 $m = W/T_a(x)$.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 one ciphertext security.
(2) The security of privacy protection

**Theorem 4.2.** *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). We sum up the privacy protection of our scheme in the Table 4. The senders identity is anonymity for outsiders because $ID_0$ is covered by $C_i = T_bT_{K_i}(x)ID_0, (1 \leq i \leq n)$,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 receiverss identity because our scheme is adopted PKC and chaotic maps. All the reveivers cannot know the others receviers because they only revover the corresponding $C_i$ using their own secret key.
we construct $C_i = T_bT_{K_i}(x)ID_0, (1 \leq i \leq n)$ to covered the senders 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 $ID_0 = C_1/T_{K_1}T_b(x)$.Additionally, since the values $b$ of the random elements is very large, attackers cannot directly guess the values $a$ of the random elements is very large, attackers cannot directly guess the values $T_b(x)$.Therefore, the proposed scheme provides privacy protection.

Table 4. Privacy protection comparisons

| Security attributes | | [31] 2009 | [32] 2010 | [33] 2013 | Ours |
|---|---|---|---|---|---|
| Sender anonymity | 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 |

4.2. **Security proof based on the BAN logic [30].** 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.

**Remark 4.1.** $(X)_Y$ *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.*

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 $X$. |
| $P \triangleleft X$ | 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 $K$. |
| $P \xleftrightarrow{K} Q$ | 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 6. Logical postulates of the BAN logic

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

According to analytic procedures of BAN logic and the requirement of multi-receiver scheme, our CMMR scheme should satisfy the following goals in Table 7:

TABLE 7. Goals of the proposed scheme

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

First of all, we transform the process of our protocol to the following idealized form.
$(U_0 \to U_i)C : U_i \triangleleft T_b(x), T_bT_{K_i}(x)ID_0, T_a(x)T_{K_0}T_{K_i}(x), T_a(x)m, (C_i||V_i||W)_{T_a(x)}$;
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 8.

ased 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:

TABLE 8. Assumptions about the initial state of our protocol

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

$S_1 : U_i| \equiv U_0| \sim C$ Based on the initial assumptions $P_3, P_4$,and relating with $R_2$,we could get: $S_2 : U_i| \equiv \#C$
Combine $S_1, S_2, P_3, P_4, P_5, P_6, R_3$ and attributes of chaotic maps, we could get: $S_3 : U_i| \equiv \#ID_0, T_a(x), T_b(x)$
Based on $R_5$,we take apart $S_3$ and get: $S_4 : U_i| \equiv \#T_b(x)$, $S_5 : U_i| \equiv \#T_a(x)$
Combine $S_3, S_4$ and attributes of chaotic maps, we can get the fresh and privacy protection about senders identity. Combine $S_5$ and attributes of chaotic maps, we can get the message $m$ for all the $U_i(1 \leq i \leq n)$.
Combine:
Because the 1-to-n parties($U_0$ and $U_i(1 \leq i \leq n)$) communicate each other just now, they confirm the other is on-line. Moreover, since the $U_i(1 \leq i \leq n)$ can get $ID_0$ from the $T_bT_{K_i}(x)ID_0$ with his own secret key, and based on $S_5, R_4$ with chaotic maps problems, we could get:
Goal 1. $U_0| \equiv (U_0U_i)$; Goal 2. $U_0| \equiv U_i| \equiv (U_0U_i)$;
Goal 3. $U_i| \equiv (U_iU_0)$; Goal 4. $U_i| \equiv U_0| \equiv (U_iU_0)$;
According to (Goal 1 Goal 4), we know that both sender $U_0$ and receivers $U_i(1 \leq i \leq n)$ believe that the $U_i(1 \leq i \leq n)$ can authenticate $U_0$ and recover the message based on the fresh nonces $a$, $b$ and the $(pk_i, sk_i)(0 \leq i \leq n)$.

## 5. **Efficiency Analysis.**

5.1. **The comparisons among different algorithms.** Compared to RSA , ECC and Bilinear map, Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. 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 [27]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. According to the results in [34], 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.
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 9). 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 [26, 28, 29]. 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 $E_{T_aT_b(x)}(messages)$ 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 CMMR scheme and the related literatures.** In this section, we make a comparison between the CMMR and other multi-receiver scheme to judge its function and competence. From Table 9, we can conclude that our scheme is more efficient than the others.

Table 9. Comparisons between our proposed scheme and the related literatures

| **Phase** | Some property | [31] 2009 | [32] 2010 | [33] 2013 | **Ours** |
|---|---|---|---|---|---|
| **Encrypt** | Number of parameters | $n$+9 | 13 | 10 | 2 |
| | Computation Complexity | $(n+1)T_a+(n+3)T_m+T_e+2T_h$ | $T_p+(m+n+1)T_m+(2m+n+3)T_e+2T_h$ | $T_p+2T_a+6T_m+T_e+2T_h$ | $nT_f+2nT_c+(2n+1)T_{mo}$ |
| | 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 | $3T_p+2T_a+(3n+3)T_m+2T_e+(n+1)T_h$ | $(m+5)T_p+T_a+(m+\|M\|+2)T_m+2T_h$ | $2T_p+T_a+T_m+T_h$ | $T_f+2T_c+2T_{mo}$ |
| | 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 | $3T_p+2T_a+(3n+3)T_m+2T_e+(n+1)T_h$ | $(m+5)T_p+T_a+(m+\|M\|+2)T_m+2T_h$ | $2T_p+nT_a+(n-1)T_m+2T_h$ | $T_{mo}$ |
| **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 [23].
$T_f$: 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 [31–33] 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.

6. **Conclusion.** In this paper, we propose CMMR, 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 standtard model and high-efficiency) with respect to a traditional multi-receiver protocols. Compared with the related works, our CMMR scheme is not the trade off between security and efficiency, but is comprehensively improved scheme.

## REFERENCES


[1] J. Baek, S. N. Reihaneh, and S. Willy,Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption *Lecture Notes in Computer Science*, vol.3386, pp.380-397, 2005.

[2] 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.

[3] E. Ekrem, and S. Ulukus, Multi-Receiver Wiretap Channel with Public and Confidential Messages . *IEEE Transactions on Information Theory.* vol.59, no.4, 2165-2177, 2013.

[4] J. G. Minonzio, M. Talman,t and L. Pascal, Multiemitters and multireceivers probe for long cortical bone assessment . *Journal of the Acoustical Society of America.* vol.127, no.3, pp.2032-2035, 2010.

[5] Y. X. Sun and 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.

[6] E. J. Yoon, K. Y. Yoo, J. W. Hong, S. Y. Yoon, D. 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.

[7] S. Canard, J. Traore, Anonymous Service Using Smart Cards and Cryptography .*IFIP International Federation for Information Processing.* vol.153, pp.83-98, 2004.

[8] C. H. Lee, X. Deng and H. F. Zhu, Design and Security Analysis of Anonymous Group Identification Protocols . *Lecture Notes in Computer Science.* vol.2274, pp.188-198, 2002.

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

[10] L. J. Pang, H. X. Li, L. Gao, and Y. M. Wang, Completely Anonymous Multi-Recipient Signcryption Scheme with Public Verification .*PLoS ONE.* vol.8, no.5, pp.1-10, 2013.

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

[12] J. S. Baek, R. Safavi-Naini and S. Willy, Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption . *Lecture Notes in Computer Science.* vol.3386, pp.380-397, 2005.

[13] D. Boneh, M. Franklin, Identity-Based Encryption from the Weil Pairing . *SIAM Journal on Computing.* vol.32, no.3, pp.586-615, 2003.

[14] C. I. 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.

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

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

[17] J. H. Zhang and J. Mao, An improved anonymous multi-receiver identity-based encryption scheme .*Int. J. Commun. Syst.* 2015; 28:645658.

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

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

[20] 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.

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

[22] X. Wang, and J. Zhao, An improved key agreement protocol based on chaos, *Commun. Nonlinear Sci. Numer. Simul*, vol. 15, pp. 4052-4057, 2010.

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

[24] L. R. Devaney, An Introduction to Chaotic Dynamical System,*Cummings Publishing Company Inc.*, The Benjammin, Menlo Park, 1986.

[25] J. C. Jiang, Y. H. Peng, Chaos of the Chebyshev polynomials, *Nat. Sci. J. Xiangtan Univ*, vol. 19, no. 3, pp. 3739, 1996.

[26] J. H. Yang, T. J. Cao, Provably secure three-party password authenticated key exchange protocol in the standard model. *J. Syst. Softw.* 85, 340350 (2012)

[27] L. Kocarev, and S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, pp. 5354, 2011.

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

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

[30] M. Burrows, M. Abadi, and R. Needham, A logic of authentication. *ACM Trans. Comput. Syst.* 8, 1836 (1990).

[31] S. Sharmila, S. Sree, R. Srinivasan, C Pandu, An efficient identity-based signcryption scheme for multiple receivers.*Proc. the Advances in Information and Computer Security 4th International Workshop on Security.* Toyama, Japan: 7188. (2009), $doi: 10.1007/978-3-642-04846-3_6$.

[32] B. Zhang, Q. Xu An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. *Proc. of the AST/UCMA/ISA/CAN conferences.* Miyazaki, Japan: pp. 1527, 2010, $doi: 10.1007/978-3-642-13577-4_2$.

[33] L. Pang, H. Li, L. Gao, Y. Wang, Completely Anonymous Multi-Recipient Signcryption Scheme with Public Verification. *PLoS ONE 8(5)*: e63562. doi:10.1371/journal.pone.0063562, 2013.

[34] P. Barreto, B. Lynn, M. Scott, On the selection of pairing-friendly groups, *In: Selected Areas in Cryptography, In: LNCS*, vol. 3006, Springer-Verlag, 2004, pp. 1725.