An Anonymous SignCryption Scheme Based on Multilinear Maps for Multi-Receiver

Zhengjun Jing*, Zhimin Yu, Haijuan Zang, Mingxia Chen

Department of Computer, Jiangsu University of Technology, Changzhou, Jiangsu, 213001, China

Abstract

Anonymous signcryption is an important cryptographic primitive, which is useful in protecting the privacy of a set of users who are connected through an ad-hoc network. In this paper, we construct a novel multi-receiver anonymous signcryption (MRASC) scheme based on Garg-Gentry-Halevi (GGH) framework which is a candidate of multi-linear maps from ideal lattice. In the MRASC scheme, a user instead of the group is able to signcrypt a message, and sends the signcryption to multiple receivers. Under the GGH graded decisional Diffie-Hellman (GDDH) assumption, the proposed ring signcryption scheme guarantees the anonymity, unforgeability and message confidentiality in the random oracle model. Compared with the existing MRASC schemes based on multilinear maps, our new scheme enjoys shorter public key length and higher efficiency.

Keywords: RING SIGNCRYPTION, MULTILINEAR MAPS, ANONYMOUS, MULTI-RECEIVER, PRIVACY AND TRUST.

1. Introduction

In 1997, Zheng introduced the term of signcryption which supports authentication and confidentiality simultaneously [1]. Due to the combination of functionality of signature and encryption in a single logical step, signcryption has a cost lower than signing and encrypting a message independently. After Bohen and Franklin proposed identity-based public key encryption from bilinear maps [2], more identity-based signcryption scheme have been proposed [3-4].

Anonymous signcryption or ring signcryption [5] is a cryptographic primitive in which the anonymous property of ring signature is required in addition to the authentication and confidentiality guaranteed by signcryption. Specifically, in a ring signcryption scheme, any user can choose a set of users who make up a ring that includes the user himself and signcrypt any message by using his private key and other users' public keys. Throughout the process, it is worth noting that there is no group manager, no setup procedure, no revocation procedure, no need to get any approval or assistance from other users in the ring. Because of these advantages, ring signcryption is useful to protect the sender's privacy during transferring trustworthy messages in ad-hoc network [6] and plays an important role in building e-commence where involves many partners, such as in cloud computing [7].

In order to demonstrate how to use ring signcryption, we consider the following scenario which was described by Sharmila *et al*. [8]. Suppose that in a cabinet there are multiple members. Now, a member of them wants to leak a very important and justice message regarding the President of the nation to the press. For the sake of his own interest, he intends to leak the secret in an anonymous way. However, for the press, the information will not be accepted unless it can be authenticated by one of the members of

the cabinet. Additionally, the information is so sensitive that it should not be leaked until the authorities in the press receives it. To solve the problems described in the above scene, constructing a ring signcryption scheme is an appropriate idea according to the definition of ring signcryption proposed by Huang *et al*. [5], because its anonymity can keep privacy of the cabinet member who sends the message while its authentication convinces the authorities in the press of the validity of the information. At the same time, the confidentiality of the ring signcryption keeps the information secure till the right authorities in the press receive them. However, the signcryption in [5,8-9] just consider that there is only one receiver. If the cabinet member wants to transfer the sensitive message to different press authorities simultaneously in order to avoid the problems described by Lal and Kushwanh [10], the multi-receiver ring signcryption should be adopted.

1.1. Related works

The notion of ring signature was first formally introduced by Rivest, Shamir and Tauman [11]. In a ring signature, any member in the ring can sign on behalf of the whole ring. As a result, the verifier is convinced that this signature is from a ring in which the signer is a member, but it is hard to know which member in the ring actually generated the signature. On the definition of security for ring signature, Bendery *et al*. [12] gave a widely accepted definition of both anonymity and unforgeability. Due to the unique anonymity and flexibility (such as, no managers, no setup procedure of the ring and no revocation procedure), the ring signature can be applied for a variety of purposes which have been suggested in previous works, for example, anonymous leakage of secrets [11] and anonymous authentication in Ad-hoc networks and wireless sensor networks [13-14].

With the motivation of ring signature, Huang *et al*. [5] proposed a first anonymous signcryption or ring signcryption scheme, in which a user can anonymously signcrypted a message on behalf of a group of users including himself. Subsequently, more efficient ID-based ring signcryption are reported, see for instance [15-17]. However, most of them have been proved to be insecure and then improved in [8,18].

When a message needs to be confidentially transmitted to multiple recipients, traditional encryption scheme is no longer valid. For the multi-receiver situation, Bellare *et al.* [19] and Baudron *et al.* [20] independently proposed the concept of multi-recipient public key encryption. In a multi-recipient public key encryption system, the sender can encrypt the same message for multiple receivers in a single ciphertext. Such properties of multi-recipient public key encryption can be applied for a variety of purposes, such as broadcasting encryption and multicast security protocols in wireless sensor network. After that, Duan and Cao [21] introduced the multi-receivers public encryption conception into signcryption and constructed the first ID-based multi-receiver signcryption. Recently, more improved schemes are proposed by Pang *et al*. [22], in which the receivers' identity anonymity is required and the fairness of decryption is considered.

A multi-receiver anonymous signcryption (*MRASC*) combines the properties of ring signature and multi-receiver signcryption. Thus, it enables the sender to anonymously signcrypt any message to multiple receivers in a single ciphertext. Layl et al. [10] proposed the first *MRASC* scheme to solve the problems when the cabinet intends to send the sensitive message to different press authorities simultaneously in the above scenario. However, Wang et al. [23] showed that their scheme was insecure in resisting adaptive chosen ciphertext attack and made some improvements. Subsequently, Zhang and Xu [24] constructed in the standard model the first ID-based MRASC scheme which guaranteed the semantic security, unforgeability and signcrypter's identity ambiguity.

Here we want to point out that the security of the existing ring signcryption schemes, either for a single receiver or multiple receivers, depends on the hard assumption based on bilinear pairs, such as computational Diffie-Hellman assumption and decisional bilinear Diffie-Hellman problem. However, with the advent of quantum computer era, all the above schemes will no longer be secure, because the quantum algorithm designed can efficiently solve the classical problems in number theory (e.g. large integer factorization, discrete logarithm problem). Therefore, it is meaningful to choose a new hard assumption to design a secure alternative to the multi-receivers ring signcryption in the post-quantum era.

1.2. Our contribution

In this paper, we provide the first alternative to the multi-receiver anonymous signcryption based on the bilinear-pairs hard assumption. The new MRASC scheme is based on GGH's graded encoding system which is a candidate multi-linear map from ideal lattice, while its security can be reduced to the Grade Decisional Diffie-Hellman (GDDH) assumption of GGH framework. Although GDDH hard assumption cannot be directly reduced to the general lattice problem, such as SVP (shortest vector problem) or LWE (learning with error), there is still no effective

algorithm in polynomial time to solve this problem, including quantum algorithms. Under GDDH assumption, we give the formal security proof of the proposed scheme in terms of confidentiality, unforgeability and anonymity in the random model.

2. Preliminaries

2.1. Notations

For a positive integer k, $[k]$ denotes $\{1,\cdots k\}$. In this paper, we use $\Pr$ to denote the probability of an event, then the probability of two events occur simultaneously and conditional probability is denoted by $\Pr(a \wedge b)$ and $\Pr(a \mid b)$, respectively. For a set S, let $|S|$ denote the number of members in S.

2.2. Multilinear maps and graded encodings system

We now first recall the formal definition of generic k-leveled multilinear groups [25]. Assume that there is a group generator $\mathcal{G}(1^\lambda, k)$ which takes as input a security parameter λ and a positive integer k to indicate the number of allowed pairing operations. The group generator $\mathcal{G}(1^\lambda, k)$ outputs a sequence of group $\vec{G} = (G_1, \cdots, G_k)$ each of large prime order $p > 2^\lambda$. Let g_i be a canonical generator of G_i, and $g = g_1$. We assume that there exists a set of bilinear maps $\{e_{i,j} : G_i \times G_j \to G_{i+j} \mid i, j \geq 1, i + j \leq k\}$, which satisfies the relation: $e_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab}$.

In the past decade, how to achieve cryptographically useful multi-linear maps is an important open problem. Recently, Garg, Gentry and Halevi (GGH) [25] have proposed a candidate in *EUROCRYPT'* 2013. Abstractly, in GGH graded encoding system, the exponentiation g_i^α in multi-linear group family is viewed as an encoding of an element α on the i-level. At the same time, the GGH replaces the groups defined in BS with an encoding set associated with ideal lattice. Specifically, for a ring R, the GGH graded encoding system includes a system of sets $S = \{S_i^{\mathbf{a}} \subset \{0,1\}^* : i \in [0, n], \mathbf{a} \in R\}$, where $S_i^{(\mathbf{a})}$ consists of the i-level encodings of $\mathbf{a}$ and the sets $S_i = \bigcup_\alpha S_i^{(\mathbf{a})}$. The k-GGH framework includes several algorithms, which are instance generation, sampling, encodings at higher levels, re-randomization, zero-testing and extraction. the details about GGH framework can be referred to [25].

2.3. GDDH hard assumption

Now, we describe the hard assumption in GGH framework: Graded Decisional Diffie-Hellman problem (GDDH), which is the basis of the security of our scheme in this paper.

Definition 1. (**GDDH**). On parameters λ, n, q, k, a challenger runs $\mathrm{InstGen}(1^\lambda, 1^k)$ to get the public parameters $(params, \mathbf{p}_{zt})$ of the GGH graded encoding system, and it calls $\mathrm{samp}()$ several times to pick the random $\mathbf{e}_0, \cdots \mathbf{e}_k$. Then, given $params$, $\mathbf{p}_{zt}$, $\text{re-enc}(1, \mathbf{e}_0), \cdots, \text{re-enc}(1, \mathbf{e}_k)$ and a random level-k encoding $\mathbf{u} \leftarrow \text{re-enc}(k, \mathrm{samp}())$, the goal of the k-GDDH is to distinguish between the level-k encoding $\text{re-enc}(k, \prod_{i \in [0,k]} \mathbf{e}_i)$ and the random encoding $\mathbf{u}$.

2.4. The model of MRASC

Here, we describe the mode of anonymous signcryption scheme for multi-receivers, which includes the general definition and its security model. Note that in the mode the public key of a user (either the senders or receivers) represents himself.

An anonymous signcryption scheme for multi-receivers consists of three polynomial-time algorithms: **Setup**, **SignCrypt** and **Unsigncrypt**.

$Setup(\lambda, N, L)$. The algorithm takes as input the security parameter λ, the number of senders N and the number of receivers L, and outputs the public-private key pairs (spk_i, ssk_i), $i \in [N]$ for the senders and (rpk_j, rsk_j), $j \in [L]$ for the receivers. Since the users in this system must share some public parameters derived from λ, we can divide the **Setup** algorithm into two sub-algorithms: $\text{Setup-params}(1^\lambda)$ which generates a set of public parameters PP which are used in all algorithms; $\text{Setup-Keys}(PP)$ which generates key pairs based on the public parameters.

$SignCrypt(M, ssk_i, W, Q)$. Given a message $M \in \{0,1\}^l$, a set of senders' public keys $W = \{spk_1, \cdots, spk_N\}$ and a set of receivers' public keys $Q = \{rpk_1, \cdots, rpk_L\}$, a user in the set W can run $c \leftarrow SignCrypt(M, ssk_i, W, Q)$ and send the ciphertext c to L receivers anonymously, where ssk_i is the corresponding private key.

$UnSignCrypt(c, rsk_i, W, Q)$. When receiving a ciphertext c, any member in the set Q can run the algorithm $UnSignCrypt(c, rsk_i, W, Q)$ to obtain the corresponding plaintext message M, where rsk_i is his private key. If unsigncryption is unsuccessful, it outputs the symbol $\perp$.

For correctness, it is required that for $(PP, \{spk_i, ssk_i\}, \{rpk_j, rsk_j\}) \leftarrow Setup(\lambda, N, L)$, $i \in [N]$, $j \in [L]$ any message $M \in \{0,1\}^l$ and a signcryption $c \leftarrow SignCrypt(M, ssk_i, W, Q)$, any receiver in the set Q obtains the message M by running $UnSignCrypt(c, rsk_i, W, Q)$ with his private key rsk_i.

For a secure ring (or anonymous) signcryption scheme Φ with N ring members and L receivers, it must guarantee the signcrypter identity's anonymity, message confidentiality and unforgeability.

Definition 2. (**Anonymity**) An *MRASC* scheme Φ is unconditionally anonymous if for any group of N members with the corresponding public keys $W = \{spk_1, \cdots, spk_N\}$, the probability of any adver-

sary to identify the actual signcrypter is not more than random guess's. In other words, the adversary outputs the actual signcrypter with probability $1/N$ if he is not a member of W, and with probability $1/(N\text{-}1)$ if he is the member of W.

Definition 3. (**Message Confidentiality**) A MRASC scheme Φ is secure under IND-CPA (Indistinguishability under Chosen Plaintext Attack) model if all PPT adversaries have at most a negligible advantage in λ in the following security game between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$, where the advantage of an adversary is defined as $Adv_{\mathcal{A}}^{ind\text{-}cpa} = \left|\Pr[b^*=b]\text{-}\frac{1}{2}\right|$.

Setup. The challenger $\mathcal{B}$ calls $Setup(\lambda, N, L)$ and generates the public-private pairs $\{(spk_1, ssk_1), \cdots (spk_N, ssk_N)\}$ for the senders and the public-private pairs $\{(rpk_1, rsk_1), \cdots (rpk_L, rsk_L)\}$ for recipients.

Let $PP = \{W = \{spk_1, \cdots, spk_N\}, Q = \{rpk_1, \cdots, rpk_L\}\}$ be the public parameter. $\mathcal{B}$ keeps the users' private keys secure and sends the public parameter to adversary.

Signcryption Queries. The adversary $\mathcal{A}$ randomly chooses a message $M \in \{0,1\}^l$ and sends to $\mathcal{B}$. When getting the signcrypt query, the challenger $\mathcal{B}$ randomly chooses a user whose public key $spk_i \in W$ and computes a ciphertext $c \leftarrow SignCrypt(M, ssk_i, W, Q)$ where ssk_i is the chosen user's private key. $\mathcal{B}$ returns the ciphertext c to $\mathcal{A}$.

Challenge. After finite queries, the adversary wants to challenge. $\mathcal{A}$ chooses two messages M_0, M_1 with the same length and sends them to challenger $\mathcal{B}$. After receiving them, $\mathcal{B}$ first flips a coin to choose a bit $b \in \{0,1\}$, then calls $SignCrypt(M_b, ssk_i, W, Q)$ to generate a ciphertext c^* where ssk_i is the private key of a sender chosen randomly from W. Finally, $\mathcal{B}$ sends c^* to the adversary.

Guess. The adversary outputs a guess b^* and wins if $b^* = b$.

Definition 4. (**Existential Unforgeability**) A *MRASC* scheme is existentially unforgeable with respect to selective chosen-message attack and fixed-ring attack if no polynomially bounded adversary wins the following game with a non-negligible advantage.

Init. The forger $\mathcal{F}$ gives the challenger the forgery message M^*. The message M^* cannot be queried during the signcryption query phase.

Setup. The challenger $\mathcal{B}$ calls $Setup(\lambda, N, L)$ and generates the public-private pairs $\{(spk_1, ssk_1), \cdots (spk_N, ssk_N)\}$ for the senders and the public-private pairs $\{(rpk_1, rsk_1), \cdots (rpk_L, rsk_L)\}$ for recipients.

Let $PP = \{W = \{spk_1, \cdots, spk_N\}, Q = \{rpk_1, \cdots, rpk_L\}\}$ be the public parameter. $\mathcal{B}$ keeps the users' private keys secure and sends the public parameter to adversary.

Signcryption Queries. The forger $\mathcal{F}$ performs a polynomially bounded signcryption queries of same type as in message confidentiality game.

Forgery. The forger $\mathcal{F}$ outputs a ring signcryption c^* for the receivers $Q = \{rpk_1, \cdots, rpk_L\}$. We say the forger $\mathcal{F}$ wins the game if: (1) if the c^* is a valid ciphertext under the group senders $W = \{spk_1, \cdots, spk_n\}$ such that the result of $UnSignCrypt(c, rsk_i, W, Q)$ is M^*, where the rsk_i is a private key of any receiver in Q, and (2) M^* is not queried during the *Signcryption* oracle.

3. Our MRASC scheme based on GGH system

According to the definition of MRASC in section 2, the proposed scheme based on GGH consists of the following three polynomial time algorithms.

Setup. Given the security parameter λ, the number of senders N and the number of recipients L, the algorithm initializes the system from three parts.

(a) Call $\text{InstGen}(\lambda, k = N + L)$ to obtain a GGH instance parameters $params = \{n, q, \mathbf{y}, \{\mathbf{x}_i\}_i, s\}$, $\mathbf{p}_{zt}$, $i \in [k]$

(b) Choose a hash function $H : \{0,1\}^{\lambda} \to \{0,1\}^l$ and another hash function h which has an availability that maps messages $M \in \{0,1\}^l$ to the random level-0 encodings of GGH's system. These two hash functions can be viewed as a random oracle, respectively. In practice, for the hash function h, given a message M whose length is l, it firstly chooses random encodings $\mathbf{b}_{j,v} \leftarrow \text{samp}()$, where $j \in [2l]$ and $v \in \{0,1\}$. Then, it generates the corresponding level-0 encoding $\mathbf{a} = \sum_{i \in [l]} \mathbf{b}_{m[i]}$ where $M[i]$ are the bits of M.

(c) Pick a random element α_i which is the result of a fresh call to samp() and generates the level-one encoding $\mathbf{A}_i = \text{re-enc}(\alpha_i)$, $1 \le i \le k$. Without loss of generality, in this paper $U_{i \in [N]}$ denotes the sender and $U_{j \in [N+1,k]}$ the recipients. So, the public-private key set of the senders is $\{(\mathbf{a}_1, \mathbf{A}_1), \cdots, (\mathbf{a}_N, \mathbf{A}_N)\}$ while the public-private key set of the recipients is $\{(\mathbf{a}_{N+1}, \mathbf{A}_{N+1}), \cdots, (\mathbf{a}_{N+L}, \mathbf{A}_{N+L})\}$.

Finally, this algorithm outputs the public parameters $PP = \{params, \mathbf{p}_{zt}, h, H, PK\}$, where $PK = \{\mathbf{A}_1, \cdots \mathbf{A}_k\}$.

Signcrypt. Given the public parameter PP and a message $M \in \{0,1\}^l$, the sender $U_{i \in [N]}$ signcrypts the message M as follows.

(*a*) Select randomly an element $\mathbf{r} = \text{samp}()$ and generate the level-1 encoding $\mathbf{A}_r = \text{re-enc}(1, \mathbf{r})$.

(*b*) Compute $\mathbf{s}_0 = h(M) \cdot ssk_i \cdot \mathbf{A}_r$ where ssk_i is the private key of U_i whose public key is in the set W. Then, generate $\mathbf{s}_1 = \prod_{j \neq i} spk_j, j \in [N]$, $\mathbf{s}_2 = \text{re-enc}\ (2, \mathbf{s}_0)$.

(*c*) Compute $\mathbf{c}_1 = \text{re-enc}(N+1, \mathbf{s}_1 \cdot \mathbf{s}_2)$.

(*d*) Compute $\mathbf{s}_2 = \text{re-enc}(N, \mathbf{s}_0 \cdot \mathbf{s}_1)$ and $\mathbf{s}_4 = \text{re-enc}(L, \prod_{j \in [L]} rpk_j)$, then generate $\mathbf{c}_2 = H(\text{ext}(\mathbf{p}_{zt}, \mathbf{s}_3 \cdot \mathbf{s}_4))) \otimes M$ where the notation $\otimes$ denotes bitwise XOR operate.

(*e*) Let $\mathbf{c}_3 = \mathbf{A}_r$ and output a ciphertext $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$.

Unsigncrypt. After receiving a ciphertext $\mathbf{c}$, any legitimate recipient $U_{j \in [L]}$ can decrypt the ciphertext as followings.

(a) Parse the ciphertext $\mathbf{c}$ to the form $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, and compute the level-$(L-1)$ encoding $\mathbf{c}' = rsk_j \cdot \prod_i rpk_i$, where $N+1 \le i \le N+L, i \neq j$ and rsk_j is the private key of a receiver $U_{j \in [L]}$.

(b) Compute $\mathbf{c}'' = \mathbf{c}_1 \cdot \mathbf{c}'$ and obtain $M = H(\text{ext}(k, \mathbf{c}'')) \otimes \mathbf{c}_2$.

(c) Compute $\mathbf{c}''' = h(M) \cdot \mathbf{c}_3 \cdot \prod_{i \in [N]} spk_i$.

If the result of the algorithm $\text{isZero}(\mathbf{p}_{zt}, (\mathbf{c}''' - \mathbf{c}_1) \cdot \mathbf{y}^{L-1})$ is 1, it outputs the plaintext M, and the recipient U_j accept the message M. Otherwise, the recipient does not think that the ciphertext $\mathbf{c}$ is sent by an honest sender, and outputs $\perp$.

4. Analysis of the scheme

In this section, we analyze the proposed multi-receivers anonymous signcryption scheme based on GGH framework in terms of correctness, security and performance.

4.1. Correctness

According to the GGH's framework and the procedure of signcryption, we know that $\mathbf{s}_1 \cdot \mathbf{s}_2$ is a level-k encoding of $h(M) \cdot \mathbf{r} \cdot \prod_{i \in [k]} \mathbf{a}_i$, and that $\mathbf{c}_1 = h(M) \cdot \mathbf{A}_r \cdot \prod_{i \in [N]} spk_i$ is a level-$(N+1)$ encoding of $h(M) \cdot \mathbf{r} \cdot \prod_{i \in [N]} \mathbf{a}_i$. Since $\mathbf{c}' = rsk_j \cdot \prod_i rpk_i$ is a level-$(L\text{-}1)$ encoding of $\prod_j \mathbf{a}_j$, $N+1 \le j \le N+L$, $\mathbf{c}_1 \cdot \mathbf{c}'$ is a level-k encoding of $h(M) \cdot \mathbf{r} \cdot \prod_{i \in [k]} \mathbf{a}_i$. Thus,

$$
\begin{aligned}
&H(\text{ext}(k, \mathbf{c}'')) \otimes \mathbf{c}_2 = H(\text{ext}(k, \mathbf{c}_1 \cdot \mathbf{c}')) \otimes \mathbf{c}_2 \\
&= H(\text{ext}(k, \mathbf{c}_1 \cdot \mathbf{c}')) \otimes H(\text{ext}(k, \mathbf{s}_1 \cdot \mathbf{s}_2)) \otimes M \\
&= H(\text{ext}(k, \text{re-enc}(\ k, h(M) \cdot \mathbf{r} \cdot \prod_{i \in [k]} \mathbf{a}_i))) \otimes \\
&\quad H(\text{ext}(k, \text{re-enc}(\ h(M) \cdot \mathbf{r} \cdot \prod_{i \in [k]} \mathbf{a}_i))) \otimes M \\
&= M
\end{aligned}
$$

The establishment of the last equation is due to the properties of the **Extraction** algorithm in GGH's system. Furthermore, when obtaining the message M, the encoding $\mathbf{c}'''$ can be computed immediately, which is also a level-$(N+1)$ encoding of $h(M) \cdot \mathbf{r} \cdot \prod_{i \in [N]} \mathbf{a}_i$. So the receiver $U_{j \in [L]}$ can finish authentication by using the "zero-testing" algorithm $\text{isZero}(\mathbf{p}_{zt}, (\mathbf{c}''' - \mathbf{c}_1) \cdot \mathbf{y}^{L-1})$.

4.2. Security analysis

According to the security model described in section 3, we prove the security of the proposed *MRASC* scheme based on GGH in random oracle model, which could be reduced to the *GDDH* problem.

Theorem 1. The proposed MRASC scheme based on GGH graded encoding system satisfies the unconditional anonymous.

Proof. To prove our scheme satisfies the anonymous, we show that the distribution of signcryption produced by anyone in the group $W = \{spk_1, \cdots, spk_N\}$ is indistinguishable. Without loss of generality, we choose two senders $U_b, b \in \{0,1\}$, whose public-private keys are $\{spk_1, ssk_1\}$ and $\{spk_2, ssk_2\}$ respectively.

For a message M, the sender U_b randomly picks a level-0 encoding $\mathbf{r} = \text{samp}()$ and computes the corresponding ciphertext $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*, \mathbf{c}_3^*)$ by calling thealgorithm $\text{signcrypt}(m, ssk_b, W, Q)$, where $b \in \{0,1\}$, $W = \{spk_1, \cdots, spk_N\}$, $Q = \{rpk_1, \cdots rpk_L\}$, According to the procedure of signcryption, each valid signcryption $\mathbf{c}^*$ can be parsed to three random encodings. Therefore, we need to analyze the distribution of the signcryption. According to the procedure of signcryption, we know that, regardless of $\mathbf{c}^*$ sent by the user U_0 or the user U_1, the distribution of a valid signcryption on message m about the groups W and Q is the same, such that $\mathbf{c}_1^*$ is a level-$(N+1)$ encoding of $h(M) \cdot r \cdot \prod_{i \in [N]} \mathbf{a}_i$, $\mathbf{c}_2^*$ is a level-k encoding of $h(M) \cdot \mathbf{r} \cdot \prod_{i \in [k]} \mathbf{a}_i$, and $\mathbf{c}_3^*$ is a level-1 encoding of $\mathbf{r}$. That is, for the same message, in our scheme the distribution of the signcryption from the different members in the group W is indistinguishable.

Theorem 2. If the GDDH assumption holds then proposed MRASC scheme based on GGH graded encoding system is IND-CPA secure.

Proof. Assume that there exists a PPT adversary $\mathcal{A}$ that breaks the proposed *MRASC* scheme in the *IND-CPA* secure game with an advantage δ for the number of senders N, the number of recipients L and security parameter λ, then we can construct an algorithm $\mathcal{B}$ to solve the level-k GDDH problem for security parameter λ with probability $\delta/2$, where $k = N+L$. The algorithm $\mathcal{B}$ takes as input a GDDH instance $\Psi = \{params, \mathbf{p}_{zt}, \mathbf{A}_0 = \text{re-enc}(1, \mathbf{a}_0), \cdots, \mathbf{A}_k = \text{re-enc}(1, \mathbf{a}_k), \mathbf{T}\}$,

where $\mathbf{a}_i$=samp(), $0 \le i \le k$, and $\mathbf{T}$ is a level-k encoding of the product $\prod_{i=0}^{k} \mathbf{a}_i$ or a level-k encoding of a random element.

Let $\mathbf{T}_0 = \text{re-enc}(k, \prod_{i=0}^{k} \mathbf{a}_i)$ and $\mathbf{T}_1 = \text{re-enc}(k, \text{samp}(\cdot))$, then the goal of algorithm $\mathcal{B}$ is to determine whether the value of $\mathbf{T}$ is $\mathbf{T}_0$ or $\mathbf{T}_1$. The algorithm $\mathcal{B}$ plays the role of challenger in the game.

Setup. The challenger prepares a simulated attack environment for $\mathcal{A}$ as follows:

(1) Let the public key of each sender be $\{spk_1 = \mathbf{A}_1, \cdots, spk_N = \mathbf{A}_N\}$, and let the public key of each receiver be $\{rpk_1 = \mathbf{A}_{N+1}, \cdots, rpk_L = \mathbf{A}_{N+L}\}$

(2) Pick random encodings $\mathbf{b}_{j,v} \leftarrow \text{samp}()$, where $j \in [2l]$ and $v \in \{0,1\}$.

(3) Choose a hash function $H : \{0,1\}^{\lambda} \to \{0,1\}^{l}$.

(4) Maintain a list T which is initialized to be empty and store the sequences of massage-hash value.

(5) Publish the public parameter

$$PP = \{params, \mathbf{p}_{zt}, H, W = \{spk_1, \cdots, spk_N\}, Q = \{rpk_1, \cdots, rpk_N\}\}.$$

Random-Oracle Hash Queries. $\mathcal{A}$ may query the random oracle h adaptively. (We assume that the queries are unique, otherwise the challenger simply returns the same output on the same input.) When the adversary makes hash query for any message $M \in \{0,1\}^{l}$, the challenger $\mathcal{B}$ generates the corresponding level-0 encoding $h(M) = \sum_{i \in [l]} \mathbf{b}_{m[i]}$ where $M[i]$ are the bits of M. Then, it saves $(M_i, h(M_i))$ in list T and returns $h(M)$ to $\mathcal{A}$.

Signcryption Queries. When the adversary makes signcryption queries for messages $M \in \{0,1\}^{l}$, a group of senders $W = \{spk_1, \cdots, spk_N\}$ and a receiver list $Q = \{rpk_1, \cdots, rpk_N\}$, $\mathcal{B}$ firstly obtains the corresponding hash value $h(M)$ by looking up the list. (We assume that f has made the hash queries before signcryption queries.) Then, the challenger computes $\mathbf{c}_1 = \text{re-enc}\ (N+1, h(M) \cdot \mathbf{A}_0 \cdot \prod_{i \in [N]} spk_i)$, $\mathbf{c}_2 = H(\text{ext}(h(M) \cdot \mathbf{T})) \otimes M$ and $\mathbf{c}_3 = \mathbf{A}_0$. Finally, it returns the ciphertext $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ to $\mathcal{A}$.

Challenge. The adversary $\mathcal{A}$ chooses two messages M_0, M_1 with the same length and sends them to $\mathcal{B}$. After receiving them, $\mathcal{B}$ first randomly chooses a bit $b \in \{0,1\}$ and compute the signcryption $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*, \mathbf{c}_3^*)$ of m_b just as the procedure of signcryption queries do, in which

$\mathbf{c}_1^* = \text{re-enc}\ (N+1, h(M_b) \cdot \mathbf{A}_0 \cdot \prod_{i \in [N]} spk_i)$,

$\mathbf{c}_2^* = H(\text{ext}(h(M_b) \cdot \mathbf{T})) \otimes M_b$ and $\mathbf{c}_3^* = \mathbf{A}_0$.

Finally, the challenge ciphertext $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*, \mathbf{c}_3^*)$ is returned to $\mathcal{A}$.

If $\mathbf{T} = \mathbf{T}_0$, $\mathbf{T}$ is a level-k encoding of $\mathbf{a}_0 \cdot \prod_{i \in [N]} \mathbf{a}_i$. At this point, the challenge ciphertext $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*, \mathbf{c}_3^*)$ is a valid signcryption of M_b. Otherwise, if $\mathbf{T} = \mathbf{T}_1$, $\mathbf{T}$=re-enc$(k, \text{samp}(\cdot))$ is a level-k encoding of a random element. As the randomness of the algorithm ext(), the challenge ciphertext sent to $\mathcal{A}$ can not disclose any information about b.

Guess. After receiving b^* guessed by the adversary $\mathcal{A}$, the algorithm $\mathcal{B}$ determines the GDDH instance Ψ in the following way: if $b^* = b$, it outputs $(\mathbf{A}_0, \cdots, \mathbf{A}_N, \cdots, \mathbf{A}_k, \mathbf{T}_0)$; otherwise, it outputs $(\mathbf{A}_0, \cdots, \mathbf{A}_N, \cdots, \mathbf{A}_k, \mathbf{T}_1)$.

We analysis the advantage of $\mathcal{B}$. For the challenge signcryption ciphertext $\mathbf{c}^*$, there are two cases to be discussed. As in the poof of Theorem 1 in [26], we can conclude that if the adversary $\mathcal{A}$ can break the proposed *MRASC* scheme for N ring members and L receivers with non-negligible advantage δ, the PPT algorithm $\mathcal{B}$ can succeed to distinguish the k-GDDH instance with advantage $\frac{\delta}{2}$, where $k = N + L$.

Theorem 3. Under the GDDH assumption, the proposed MRASC scheme based on GGH graded encoding system is extensively unforgeable against selective chosen message attack in random model.

Proof. Under the selective chosen message attack model, assume that there is a probabilistic polynomial-time forger for the proposed scheme with an advantage δ, then we can construct an efficient algorithm $\mathcal{B}$ to solve the GDDH problem by calling the forger as a subroutine. The algorithm $\mathcal{B}$ takes as input a GDDH instance, which is the same as the one in the above Theorem 2.

Init. The forger outputs the forgery message $M^* \in \{0,1\}^{l}$.

Setup. In order to prepare a simulated attack environment for the forger $\mathcal{F}$, the algorithm $\mathcal{B}$ sets the public parameters using Setup algorithm described in the theorem 2.

Queries. The forger can make a polynomially bounded number of queries including the hash queries and signcryption queries. $\mathcal{B}$ answers these queries in the same way as that of the theorem 2.

Forgery. The forger give a signcryption ciphertext $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*, \mathbf{c}_3^*)$ on message M^* for the senders' set W and the receivers' set Q.

When receiving $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*, \mathbf{c}_3^*)$, the challenger $\mathcal{B}$ should verify the validation through two step: (1) Validate $\mathbf{c}_1^*$ by using the algorithm Signcrypt in the proposed scheme; (2) determine whether the result of $\text{H}(\text{ext}(\mathbf{p}_{zt}, \text{h}(M^*) \cdot \mathbf{T})) \oplus M^*$ is equal to $\mathbf{c}_2^*$. If both conditions are satisfied, $\mathcal{B}$ thinks that the ciphertext $\mathbf{c}^*$ is valid. According to the assumption that the forger can forge successfully with a non-negligible advantage δ, then after a polynomially bounded number of

queries, the challenger can determine whether $\mathbf{T}$ is $\mathbf{T}_0$ or $\mathbf{T}_1$ with an overwhelming probability.

4.3. Performance analysis

In the above anonymous (or ring) signcryption scheme for multi-receiver based on GGH's system, the length of ring is N while the number of receivers is L. To signcrypt a message $M \in \{0,1\}^l$, it only needs $k+l+2$ n-degree polynomial modular multiplication in quotient ring R_q, where $k = N + L$. Furthermore, the cost of unsigncrypt is the same as that of signcryption. In the table 1, we compare the new signcryption scheme with previous GGH-based *MRASC* scheme proposed by Yu *et al.*[27] in terms of the system public parameters length, public-private key size of each user in the ring, ciphertext length, signcryption cost and the level number of hard assumption.

Table 1. Comparison of GGH-based MRASC

Schemes	Key-size	Signcryption cost	Level numbe
Yu's	$4n\log_2 q$	$(2N + L + 2)\cdot T_s$	$k = 2N + L - 2$
Ours	$2n\log_2 q$	$(N + L + 2)\cdot T_s$	$k = N + L$

Table 1 shows that our scheme is more efficient because of the lower cost, where T_s denotes the time cost to run once n-degree polynomial modular multiplication in quotient ring R_q. Furthermore, since the approximate setting in GGH system is suggested: $n = O(k\lambda^2)$, $q = 2^{n/\lambda}$ and $m = O(n^2)$, the system parameters length, the public-private key size and the length of ciphertext in proposed scheme are smaller than that of Yu's scheme, which are $mn\log_2 q = k^4\lambda^7$ bits, $2n\log_2 q = O(k^2\lambda^2)$ bits and $2n\log_2 q + l = O(k^2\lambda^3)$ bits, respectively.

5. Conclusions

A secure MRASC scheme enables the sender to anonymously signcrypt any message in a single ciphertext and send it to multiple receivers. This important cryptographic primitive can be used to protect privacy and authenticity of a collection of users in an ad-hoc network. With the invention of GGH graded coding system as a candidate of multilinear maps, to design more common cryptographic primitives based on multi-linear maps becomes a hot research topic. In this paper, we construct a novel MRASC scheme based on GGH's framework and prove its security in terms of anonymity, message confidentiality and unforgeability.

Finally, we would like to point out that our scheme based on the GGH's framework seems to have higher efficiency because both the signcryption and unsigncryption only involve the polynomial modular addition and multiplication in polynomial ring. However, compared with the best results of the number theoretic schemes, the size of public keys of the proposed scheme is too large to be applicable, which is similar to the schemes based on lattice. Recently, Langlois *et al*. [28] improved the GGH construction in terms of the bit size of public parameters. How to take advantage of these improvements to reduce the length of the key in the MRASC scheme is our future research work.

Acknowledgements

This work is supported by the the National Natural Science Foundation of China (No. 61374180, 61401226), the Research Foundation for Humanities and Social Sciences of Ministry of Education, China (14YJAZH023), the Research Fund for the Graduate Innovation Program of Jiangsu Province (No. CXZZ13_0493), the Innovation and Research Joint Funding of Jiangsu Province (No. BY2014038-03) and the Natural Science Foundation of Universities of Jiangsu province (No. 13KJB520005).

References

1. Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). Proceedings of Conference "CRYPTO-1997". California, 1997, pp.165-179.
2. D. Boneh, M. Franklin, Identity based encryption from the Weil pairing. Proceedings of Conference CRYPTO-2001", California, 2001, pp. 213-229.
3. L. Chen, J. Malone-Lee, Improved identity-based signcryption, Proceedings of Conference "PKC-2005", Les Diablerets, 2005, 366-379.
4. P. Barreto, B. Libert, N. McCullagh, et al., Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, Proceedings of Conference "ASIACRYPT-2005". Chennai, 2005, pp. 515-532.
5. H. Xinyi, W. Susilo, M. Yi, et al. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world, Proceedings of Conference "AINA-2005",Taibei, 2005, pp. 649-654.
6. F. Li, Y. Hu, C. Zhang, An identity-based signcryption scheme for multi-domain Ad Hoc networks, Proceedings of Conference "ACNS-2007", Zhuhai, 2007, pp. 373-384.
7. S. Li, Zhang F, Chen H. Scheme on user identity attribute preserving based on ring signcryption for cloud computing. Journal on Communications, 2014, 35(9):99-112.

8. S. Sharmila Deva Selvi, S. Sree Vivek, C. Pandu Rangan, On the security of identity based ring signcryption schemes, Proceedings of Conference "ISC-2009", Pisa, 2009, pp. 310-325.
9. F. Li, S. Masaaki, T. Tsuyoshi, Analysis and improvement of authenticatable ring signcryption scheme. Journal of Shanghai Jiaotong University (Science), 2008. 13(6): pp. 679-683.
10. S. Lal, P. Kushwah Anonymous ID-based signcryption scheme for multiple receivers, IACR, http://eprint.iacr.org/2009/345.pdf.
11. R. Rivest, A. Shamir, Y. Tauman, How to leak a secret: theory and applications of ring signatures, Proceedings of Conference "ASIACRYPT 2001", Gold Coast, 2001, pp.552-565.
12. A. Bender, J. Katz, R. Morselli, Ring signatures: stronger definitions, and constructions without random oracles, Proceedings of Conference "TCC 2006", New York, 2006, pp.60-79.
13. Y. Dodis, A. Kiayias, A. Nicolosi, et al., Anonymous identification in Ad Hoc groups, Proceedings of Conference "EUROCRYPT 2004", Interlaken, 2004, pp.609-626.
14. F. Xiao, J. Liao, G. Zeng, Threshold ring signature for wireless sensor networks, Journal on Communications, 2012, 34(3), 75-81.
15. Y. Yu, F. Li, C. Xu, An efficient identity-based anonymous signcryption scheme. Wuhan University Journal of Natural Sciences 2008; 13(6): 670-674.
16. L. Zhu, F. Zhang. Efficient ID–based ring signature and ring signcryption schemes. Proceedings of Conference "CIS'08", Suzhou, 2008, pp. 303-307.
17. Z. Zhao, T. Yu, X. Ren, Efficient identity-based ring signcryption scheme in the standard model. Journal of Information & Computational Science, 2013, 10(5): pp.1471-1478.
18. M. Zhang, Y. Zhong, P. Li, Analysis and enhance of anonymous signcryption model. IACR, http://eprint.iacr.org/ 2009/194.pdf.
19. M. Bellare, A. Boldyreva,S. Micali, Public-key encryption in a multi-user setting: security proofs and improvements, Proceedings of Conference "EUROCRYPT-2000", Bruges, 2000, pp. 259-274.
20. O. Baudron, D. Pointcheval,J. Stern, Extended notions of security for multicast public key cryptosystems, Proceedings of Conference "ICALP 2000", Geneva, 2000, pp. 499-511.
21. S. Duan, Z. Cao, Efficient and provably secure multi-receiver identity-based signcryption, Proceedings of Conference "ACISP-2006", Melbourne, 2006, pp.195-206.
22. L. Pang, L. Gao, Q. Pei, Fair and anonymous ID-based multi-receiver signcryption. Journal on Communications, 2013, 34(8): 161-168.
23. X. Wang, J. Shu, W. Zheng, et al., New multi-receiver Id-based ring signcryption scheme, Proceedings of Conference "ICEE 2012", Shanghai, 2012, pp. 2251-2257.
24. B. Zhang, Q. Xu, An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model, Proceedings of Conference "AST- 2010", Miyazaki, 2010, pp. 15-27.
25. S. Garg, C. Gentry,S. Halevi, Candidate multilinear maps from ideal lattices, Proceedings of Conference "EUROCRYPT-2013", Athens, 2013, pp.1-17.
26. J. Zhengjun, J. Guoping, G. Chunsheng. A Verifiable Multi-recipient Encryption Scheme from Multilinear Maps. Proceedings of Conference "3PGCIC-2014", Guangdong, 2014, pp.151-156.
27. Y. Zhimin, J. Zhengjun. Ring signcryption broadcasting scheme based on multilinear maps. Computer Science, 2015, 42(2):106-110.
28. A. Langlois, D. Stehlé, R. Steinfeld, GGHLite: more efficient multilinear maps from ideal lattices, Proceedings of Conference "EUROCRYPT-2014" Copenhagen, 2014, pp. 239-256.