# Ring Signature Scheme from Multilinear Maps in the Standard Model

Hong-zhang Han(✉)

Department of Computer Engineering, Jiangsu University of Technology, Changzhou, China
hhz@jsut.edu.cn

**Abstract.** A novel ring signature is constructed based on Garg-Gentry-Halevi (GGH) graded encoding system which is a candidate multilinear maps from ideal lattice, and we prove its security in standard model. Under the GGH graded decisional Diffie-Hellman (GDDH) assumption, the proposed ring signature guarantees the anonymity of signer. At the same time, the ring signature is the existentially unforgeable against adaptive chosen message attack under the GGH graded computational Diffie-Hellman (GCDH) assumption.

**Keywords:** Multilinear map · Ring signature · Anonymous · Unforgeability

## 1 Introduction

The notion of ring signature was first formally introduced by Rivest et al. in 2001 [1]. 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. [2] pointed out that the definition of security was too weak in [1], and gave a strongest definitions of both anonymity and unforgeability depending on the security strength for ring signature. Due to this 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, anonymously leaking secrets [3] and anonymous authentication in Ad-hoc networks and wireless sensor networks [4–6].

With the introduction of the concept of ring signature, a large of ring signature scheme and its variants have been constructed based on intractability of the discrete logarithm or large integer factorization, such as the standard ring signature schemes [1–6], identity-based ring signature schemes [7], linkable ring signature schemes [8] and so on. With the advent of quantum computer era, all the above schemes will no longer be secure, because the quantum algorithm designed by Shorn can efficiently solve the classical problems in number theory. (e.g. large integer factorization, discrete logarithm problem.) In order to design a post-quantum secure ring signature, there are a few of ring signature schemes with security based on standard lattice problems which is considered infeasible even under the quantum computer [9–12]. As most of them made


J. Wan et al. (Eds.): CloudComp 2016, SPNCE 2016, LNICST 197, pp. 133–144, 2018.
https://doi.org/10.1007/978-3-319-69605-8_13

use of the hash-and-sign method based on the (Gentry-Peikert-Vaikuntanathan) GPV strong trapdoors [13], a hidden structure was added to the underlying lattice, which was considered an important price to pay from a theoretical point of view [14]. Recently, Melchor et al. [15] presented an efficient ring signature by means of adapting Lyubashevsky's signature from ideal lattice, in which the strongest security defined in [2] was achieved by using a weak trapdoor as Lyubashevsky's signature [16]. However, the proof of its security was in the oracle model.

In this paper, we construct a new ring signature based on GGH's graded encoding system which is an candidate multilinear maps from ideal lattice [17]. Our main contribution from a theoretical point of view is that the proposed ring signature scheme is the first one to be based on multilinear maps and no ring signature was until now based on it. Under the graded decisional Diffie-Hellman (GDDH) assumption and grade computational Diffie-Hellman (GCDH) assumption, the new ring signature scheme guarantees the anonymity of signer even if the secret key of the signer is exposed and holds the existential unforgeability against adaptive chosen message attack in the standard model, respectively.

The rest of this paper is organized as follows. In Sect. 2, we introduce the background about multilinear maps and the algorithms in the GGH framework, full domain hash from multilinear maps and the definition of ring signature and its security model. In Sect. 3, the new ring signature scheme based on multilinear maps is described in details, and Sect. 4 proves its security including the anonymity and unforgeability. Finally, in Sect. 5, we summarize this paper.

## 2 Preliminaries

### 2.1 Notation

We use $\mathbb{Z}$ to denote the set of integer, and $R = \mathbb{Z}[X]/(X^n + 1)$ denote the integer polynomial ring where $U_{i\in[N]}$ is a power of 2. For a large prime $q \in \mathbb{Z}$, $R_q = Z_q[X]/X^n + 1 = R/qR$ denotes the quotient ring of integer polynomial mod $q$. Let $I$ denote an ideal of ring $R$, then $R/I$ denotes a quotient ring generated by the ideal $I$ while $\{e + I : e \in R\}$ denotes the representative of coset of the quotient ring $R/I$. By convention, we use bold letters for vectors (e.g. a or $A$). In addition, for a positive integer $k$, $[k]$ denotes $\{1, \cdots k\}$.

### 2.2 Multilinear Maps and the GGH Graded Encoding System

Boneh and Silverberg (BS) first proposed the concept of multilinear maps and described many cryptographic applications in 2003 [18]. For the groups $G_1$ and $G_2$ which have the same prime order, the definition of BS is that if a map $e : G_1^n \to G_2$ is an n-multilinear maps it should satisfy the following properties:

(1) If $a_1, \ldots, a_n \in \mathbb{Z}$ and $x_1, \ldots, x_n \in G_1$, then $e(x_1^{a_1}, \ldots, x_n^{a_n}) = e(x_1, \ldots, x_n)^{\Pi_{i\in[n]}a_i}$;
(2) The map $e$ is non-degenerate. In other words, if $g \in G_1$ is a generator of $G_1$, then $e(g, \ldots, g)$ is a generator of $G_2$.

Although several efficient cryptographic primitives were constructed based on the concept of multilinear maps, Boneh and Silverberg also pointed out that to instantiate this kind of multilinear maps on Weil pair or Tate pair was infeasible. In the past decade, how to achieve cryptographically useful multilinear maps is an important open problem. Recently, Garg, Gentry and Halevi (GGH) give a candidate in EUROCRYPT' 2013 [17]. They construct an approximate multilinear maps from ideal lattice, which is also known as GGH graded coding system. In a $k$-level GGH candidate, as long as $i+j \leq k$, the encodings on $i$-level and encodings on $j$-level can make multiplication to obtain the encoding on $i+j$-level. Of course, the product should be smaller than the modulus $q$. By multiplication in an iterative manner, the encodings on $k$-level can be obtained. This approach is different from the BS view of multilinear maps where a $k$-linear maps should allow the simultaneous multiplication of $k$ source group elements into one target group element. Here, we briefly describe the GGH framework as follows, and the details can be referred to [17].

Abstractly, in GGH graded encoding system, the exponentiation *samp* in multilinear groups family is viewed as an encoding of an element $\alpha$ 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 as follow:

**Instance generation:** InstGen $(1^\lambda, 1^k)$. The instance-generation procedure takes as input the security parameter $\lambda$ and an integer $B_j = re{-}enc(1, \beta_j)$ that denotes the level number, and outputs parameters $(\text{params}, \mathbf{p}_{zt})$ where $params = \{n, m, q, \mathbf{y}, \{\mathbf{x}_i\}_i, s\}$ is the public parameters of the GGH $k$-graded encoding system as above, and $\mathbf{p}_{zt}$ is a $k$-level "zero-testing parameter". To ensure the security of graded encoding system, the parameters related to params is chosen carefully. Generally, for a quotient ring $R_q$, the approximate setting is $n = \tilde{\mathrm{O}}(k\lambda^2)$, $q = 2^{n/\lambda}$ and $m = \mathrm{O}(n^2)$. In addition, in the public parameter the "randomizers" $\mathbf{x}_i$ are just random encodings of zero while the parameter $\mathbf{y}$ is a level-one encoding of 1 (correctly, encoding of $1+I$).

**Sampling level-zero encodings:** samp($params$). It takes as input $params$, the randomized algorithm outputs a level-zero encoding $\mathbf{d}$ of the coset $\mathbf{a}+I$, such as $\mathbf{d} \in S_0^{\mathbf{a}}$. Essentially, according to a discrete Gaussian distribution with an appropriate variance, one can randomly choose a short vector $\mathbf{d} \in R$, which can be viewed as a small representative of the coset $\mathbf{a}+I$ because of its very small coefficients compared to the modulus $q$.

**Encodings at higher levels:** enc($params, i, \mathbf{d}$). Given the input parameters $params$ and a level-zero encoding $\mathbf{d} \in S_0^{\mathbf{a}}$, the level-$i$ encoding $\mathbf{u} \in S_i^{(\mathbf{a})}$ of $\mathbf{d}$ can be obtained by multiplying $\mathbf{d}$ with $\mathbf{y}^i$, where $\mathbf{y}$ included in $params$ is a level-1 encoding of 1.

**Re-randomization:** re-Rand($params$, $i$, $\mathbf{u}$). This algorithm re-randomizes the encoding $\mathbf{u} \in S_i^{(\mathbf{a})}$ to the same level and obtains another encoding $\mathbf{u}^* \in S_i^{(\mathbf{a})}$, which involves adding a random Gaussian linear combination of the level-$i$ encodings of zero in

*params* (e.g.$\mathbf{x}_i$), whose noisiness "drowns out" the initial encoding. Moreover, for any two encodings $\mathbf{u}_1, \mathbf{u}_2 \in S_i^{(\mathbf{a})}$ whose noise bound is at most $\mathbf{b}$, the output distribution of re-Rand$(params, i, \mathbf{u}_1)$ and re-Rand$(params, i, \mathbf{u}_2)$ is statically the same.

**Addition:** add$(params, \mathbf{u}_1, \mathbf{u}_2)$ **and Negation** neg$(params, \mathbf{u}_1)$. Given any two level-i encodings $\mathbf{u}_1 \in S_i^{(\mathbf{a})}$ and $\mathbf{u}_2 \in S_i^{(\mathbf{b})}$, we can obtain an adding encoding $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2 \in S_i^{(\mathbf{a}+\mathbf{b})}$, while the output of algorithm neg$(params, \mathbf{u}_1)$ belongs to $S_i^{(-\mathbf{a})}$.

**Multiplication:** mult$(params, \mathbf{u}_1 \in S_i^{\mathbf{a}}, \mathbf{u}_2 \in S_j^{\mathbf{b}})$. Given any two encodings $\mathbf{u}_1 \in S_i^{\mathbf{a}}$ and $\mathbf{u}_2 \in S_j^{\mathbf{b}}$, we have multiplying encoding $\mathbf{u} = \mathbf{u}_1 \cdot \mathbf{u}_2 \in S_{i+j}^{(\mathbf{a}\cdot\mathbf{b})}$ as long as $i+j<k$.

**Zero-testing:** isZero$(params, \mathbf{p}_{zt}, \mathbf{u})$. Given a level-$k$ encoding $u$, if $\left\| [\mathbf{p}_{zt} \cdot \mathbf{u}]_q \right\| \leq q^{3/4}$ where $\|.\|$ denotes the length of vector, it is denoted that $u$ belongs to the set $S_k^0$, and the algorithm outputs 1 and 0 otherwise. Note that the encoding is additively homomorphic, so we can test quality between encodings by subtracting them and comparing to zero.

**Extraction:** ext$(params, \mathbf{p}_{zt}, \mathbf{u})$. Given a level-$k$ encoding $\mathbf{u}$, the algorithm extracts a "canonical" and "random" representative of coset from the encoding $\mathbf{u}$. Namely, ext$(params, \mathbf{p}_{zt}, \mathbf{u})$ outputs (say) $\mathbf{K} \in \{0,1\}^{\lambda}$, such that:

(a) For any two level-$k$ encodings $\mathbf{u}_1, \mathbf{u}_2 \in S_k^{\mathbf{a}}$, ext$(params, \mathbf{p}_{zt}, \mathbf{u}_1) =$ ext$(params, \mathbf{p}_{zt}, \mathbf{u}_2)$ with overwhelming probability.

(b) For $\alpha \in R$ and any encoding $\mathbf{u} \in S_k^{\mathbf{a}}$, the distribution of ext$(params, \mathbf{p}_{zt}, \mathbf{u})$ is statistically uniform over $\{0,1\}^{\lambda}$.

For ease of description, let re-enc$(params, i, \mathbf{d})$ denotes the function of re-Rand$(params, i, \text{enc}(params, i, \mathbf{d}))$ where $\mathbf{d}$ is a result of a call to samp$(params)$. In addition, we also omit *params* arguments that are provided to every algorithm in GGH framework as above. For instance, we will write samp() to instead of samp$(params)$.

### 2.3 GCDH/GDDH Hard Assumptions

Now, we describe the hard assumptions in GGH framework: Graded Computational Diffie-Hellman problem (GCDH) and Graded Decisional Diffie-Hellman problem (GDDH), which are the basis of the security of our new ring signature in this paper.

**Definition 1 (GCDH/GDDH).** On parameters $\lambda, n, q, k$, a challenger runs InstGen$(1^{\lambda}, 1^{k})$ to get the public parameters $(params, \mathbf{p}_{zt})$ of the GGH graded encoding system, and it calls samp() several times to pick the random $\mathbf{e}_0, \cdots \mathbf{e}_k$. Then,

(1) Given *params*, $\mathbf{p}_{zt}$, re-enc$(1, \mathbf{e}_0), \cdots,$ re-enc$(1, \mathbf{e}_k)$, the goal of the GCDH is to find a level-$k$ encoding of $\prod_{i\in[0,k]} \mathbf{e}_i$.

(2) Given *params*, $\mathbf{p}_{zt}$, re-enc$(1, \mathbf{e}_0), \cdots,$ re-enc$(1, \mathbf{e}_k)$ and a random level-$k$ encoding $\mathbf{u} \leftarrow \text{re} - \text{enc}(k, \text{samp}())$, the goal of the $k$-GDDH is to distinguish between the level-$k$ encoding $\text{re} - \text{enc}(k, \prod_{i\in[0,k]} \mathbf{e}_i)$ and the random encoding $\mathbf{u}$.

In [17], an extensive cryptanalysis has been done to prove the security of GGH graded encoding system, and it shows that the GCDH/GDDH problems are hard for any polynomial-time algorithm to solve. Recently, some effective cryptography primitives based on GCDH/GDDH are proposed, such as multiparty key agreement [17], full domain hash from multilinear maps and identity-based aggregate signatures [19], identity-based key-encapsulation mechanism [20], attribute-based encryption for circuits [21] and so on.

### 2.4 Full Domain Hash from Multilinear Maps

Full domain hash (FDH) is an important cryptographic technique and has been widely used in bilinear map cryptography where typically a hash function is employed to hash a string into a bilinear group. In this section, we briefly describe a method to achieve the full domain hash from multilinear maps, which will be used in our ring signature scheme. The construction in terms of GGH framework and message signature based on it are described as follows, and the details can be referred to [19].

**Hash-and-Sign from GGH Framework.** A trusted algorithm generates a GGH instance by running $(params, \mathbf{p}_{zt}) \leftarrow \text{InstGen}(1^{\lambda}, 1^{k=l+1})$, where $\lambda$ is the security parameter and $l$ is the length of message. Then, it obtains $2l$ elements $\mathbf{A}_{i,j} \leftarrow \text{re} - \text{enc}(1, \text{samp}())$, where $i \in [l]$ and $j \in \{0,1\}$. For a message $m \in \{0,1\}^l$, the full domain hash function (FDH) $H$ mapping the $l$ bits message to a level-$l$ encoding can be computed iteratively. Specifically, let $H_1(m) = \mathbf{A}_{1,m[i]}$ where $m[i]$ denotes the $i$ - th bit of message $m$. For $i \in [2, l]$, $H_i(m) = H_{i-1}(m) \cdot \mathbf{A}_{i,m[i]}$. So, the FDH based on GGH framework can be defined as $H(m) = \text{re} - \text{enc}(l, H_l(m))$.

Therefore, given a private key $\mathbf{a} \leftarrow \text{samp}()$ and the corresponding verification key $VK = \text{re} - \text{enc}(1, \mathbf{a})$, a signature on message $m$ is $\sigma = \text{re} - \text{enc}(k-1, H(M) \cdot \mathbf{a})$ and verified by testing $\text{isZero}(\mathbf{p}_{zt}, \sigma \cdot \mathbf{y} - H(M) \cdot VK)$ where $\mathbf{y}$ is a level-1 encoding of 1 that is included in *params* of the GGH instance. In [19], Hohenberger et al. showed that this signature was secure against adaptively chosen message attack in standard model conditioned on the k-GCDH assumption holding against subexponential advantage.

### 2.5 Secure Model

For a secure ring signature scheme $\Phi$ with $N$ members, it must satisfy some anonymity and unforgeability. In [2], according to various security strength, Bender et al. defined various levels of anonymity and unforgeability, respectively. In this paper, the anonymity uses the strongest definition, which is against full key exposure, while the existential unforgeability is defined under the fixed-ring attack.

**Anonymity.** The anonymity $Anon(\Phi, \mathcal{A}, \lambda, N)$ under full key exposure is defined using the following experiment between a challenger and an adversary $\mathcal{A}$.

(1) Given the security parameter $\lambda$, the challenger runs the Setup algorithm to generate the common public parameters $PP$ and the keypairs $\{pk_i, sk_i\}_{i \in [N]}$ for the signature scheme. Then, the challenger sends pp and $\bar{R} = \{pk_i\}_{i \in [N]}$ to the adversary.

(2) The adversary can make polynomially many ring signing queries, the form of which is $(i, m, \bar{R})$ for varying index $i \in [N]$ and message $m \in \mathcal{M}$. After receiving them, the challenger replies $\sigma \leftarrow \text{Sign}(PP, m, sk_i, \bar{R})$.
(3) The adversary can adaptively query the signing secret key of the $i$ - th user, where $i \in [N]$. The challenger replies $sk_i$.
(4) The adversary chooses a message $m \in \mathcal{M}$ as well as two indexes $i_0, i_1 \in [\max]$ where $pk_{i0}, pk_{i1} \in \bar{R}$, and makes ring signing query. The challenger chooses a random bit $b \in \{0, 1\}$ and replies a ring signature $\sigma^* \leftarrow \text{Sign}(PP, m, sk_{ib}, \bar{R})$ where $sk_{ib}$ is the corresponding signing secret key of the public key $pk_{ib}$.
(5) The adversary $\mathcal{A}$ outputs a guess $b^* \in \{0, 1\}$ for $b$.

We say the adversary wins if $b^*=b$. Define $Anon_{\mathcal{A}}^{\Phi-\text{FKE}}$ as the probability that $b^*=b$, where the probability is over the coin tosses of the Setup, sign algorithm and of $\mathcal{A}$.

**Definition 2.** A ring signature $\Phi$ is unconditional anonymity against full key exposure if for all probabilistic polynomial-time adversaries, the function $Anon_{\mathcal{A}}^{\Phi-\text{FKE}}$ is negligible in $\lambda$.

**Existential Unforgeability.** For the ring signature scheme $\Phi$, the existential unforgeability $Unforg(\Phi, \mathcal{F}, \lambda, N)$ with respect to adaptive chosen-message attack and fixed-ring attack can be defined using the following experiment between a challenger and a forger $\mathcal{F}$.

**Setup.** The challenger firstly chooses security parameter $\lambda$ and runs the Setup algorithm to generate the common public parameters $PP$ and the keypairs $\{pk_i, sk_i\}_{i\in[N]}$ for the signature scheme. Then, it sends $PP$ and $\bar{R} = \{pk_i\}_{i\in[N]}$ to the adversary.

**Query.** The adversary $\mathcal{F}$ can make polynomially many ring signing queries. The form of query is $(i, m, \bar{R})$ where messages $m \in \mathcal{M}$ which are chosen adpatively, and the index $i \in [N]$. After receiving them, the challenger replies $\sigma \leftarrow \text{Sign}(PP, m, sk_i, \bar{R})$.

**Forgery.** The forger $\mathcal{F}$ outputs a ring signature $(\sigma^*, m^*, \bar{R})$.

We say the forger $\mathcal{F}$ wins if and only if the algorithm $\text{Verf}(PP, \sigma^*, m^*, \bar{R})$ outputs 1 and $m^*$ is not one of the messages for which a signature was queried during the query phase. Define $Unforg_{\mathcal{F}}^{\Phi-\text{adp}-uf}$ as the probabilistic that $\text{Verf}(PP, \sigma^*, m^*, \bar{R}) = 1$, where the probability is over the coin tosses of the Setup, Sign algorithms and of $\mathcal{F}$.

**Definition 3 (Adaptive Unforgeability).** A ring signature scheme $\Phi$ is existentially unforgeable with respect to adaptive chosen-message attack and fixed-ring attack if for all probabilistic polynomial-time adversaries, the function $Unforg_{\mathcal{F}}^{\Phi-\text{adp}-uf}$ is negligible in $\lambda$.

We will also use the selective variant to $Unforg(\Phi, F, \lambda, \max)$ where there is an Init phase before the setup phase, wherein the forger $\mathcal{F}$ gives to the challenger the forgery message $m^* \in \mathcal{M}$. This message $m^*$ cannot be queried for a signature during the Query phase. Finally, $\mathcal{F}$ outputs a ring signature $(\sigma^*, m^*, \bar{R})$. If the algorithm $\text{Verf}(PP, \sigma^*, m^*, \bar{R})$ outputs 1, the forger $\mathcal{F}$ wins. In this case, we define $Unforg_{\mathcal{F}}^{\Phi-\text{Sel}-\text{uf}}$ as the probabilistic that the forger $\mathcal{F}$ wins the game, taken over the random bits of the challenger and the forger.

**Definition 4 (Selective Unforgeability).** A ring signature scheme $\Phi$ is existentially unforgeable with respect to selective chosen-message attack and fixed-ring attack if for all probabilistic polynomial-time adversaries, the function $Unforg_{\mathcal{F}}^{\Phi-\mathrm{sel}-uf}$ is negligible in $\lambda$.

## 3 Ring Signature Scheme in GGH Framework

According to the definition of ring signature, our new ring signature scheme in GGH framework is as follows.

Setup($1^{\lambda}$). The algorithm includes two parts: Setup - params and Setup - Keys.

(1) Setup-params($1^{\lambda}$). It is a sub-algorithm in setup phase, which takes as input $\lambda$ and runs $(params, \mathbf{p}_{zt}) \leftarrow \mathrm{InstGen}(1^{\lambda}, 1^{k=N+l})$ to generate a GGH instance where $N$ is the maximum number of ring supported by the scheme and $l$ is the bit-length of messages. (It is noted that $N$ and $l$ are all bounded by a polynomial in $\lambda$). Recall that we omit *params* arguments that are provided to every algorithm in GGH framework.

Next, the sub-algorithm chooses random encodings $\mathbf{a}_{i,v} \leftarrow \mathrm{samp}()$ where $i \in [l]$ and $v \in \{0,1\}$. Then it generates the corresponding level-1 encodings $\mathbf{A}_{i,v} = \text{re-enc}\ (1, \mathbf{a}_i)$ for $i \in [l]$ and $v \in \{0,1\}$. Let $A = \{(\mathbf{A}_{1,0}, \mathbf{A}_{1,1}), \cdots, (\mathbf{A}_{i,0}, \mathbf{A}_{i,1})\}, i \in [l]$ and the common public parameters $PP = \{params, A\}$.

(2) Setup - Keys($PP$). Each user can use the sub-algorithm to generate the public key and secret key. Let $U_1, \cdots U_N$ denote the users in the ring signature scheme. The user $U_{j\in[N]}$ chooses random encoding $\mathbf{b}_j \leftarrow \mathrm{samp}()$ and takes it as the secret key, while the public key is $\mathbf{B}_j \leftarrow \mathrm{re} - \mathrm{enc}(1, \beta_j)$. Therefore, the ring can be denoted by a set of public keys, such as $\bar{R} = \{\mathbf{B}_1, \cdots, \mathbf{B}_N\}$.

Sign($PP, m, \mathbf{b}_j, \bar{R}$). The member $U_{j\in[N]}$ use the secret key $\mathbf{b}_j$ to generate a ring signature of a message $m \in \{0,1\}^l$ about ring $\bar{R}$. The steps are as follows.

(1) Let $m[1], \cdots, m[l]$ be the bits of message $m$. A level-$l$ encoding $H(m) = \text{re-enc}(l, H_l(m))$ of the $l$ bits message can be computed by using the full domain hash function $H$ described in Sect. 2.
(2) Compute $\mathbf{s}_1 = \mathbf{b}_j \cdot H(m) \cdot \prod_{i\in[N]\cap i\neq j} \mathbf{B}_i$
(3) Output the ring signature $\mathbf{s} = \mathrm{re} - \mathrm{enc}(k-1, \mathbf{s}_1)$

Verf($PP, \mathbf{s}, m, \bar{R}$). The algorithm takes as input the common public parameters $PP$, a signature $\mathbf{s}$, a message $m$ and the ring $\bar{R} = \{\mathbf{B}_1, \cdots, \mathbf{B}_N\}$. The authentication process is as follows.

(1) Compute the level-$l$ encoding $H(m) = \mathrm{re} - \mathrm{enc}(l, H_l(m))$ about message $m$ by using the full domain hash function $H$.
(2) Check the signature by calling $\mathrm{isZero}(\mathbf{p}_{zt}, \mathbf{s} \cdot \mathbf{y} - H(m) \cdot \prod_{i\in[n]} \mathbf{B}_i)$, where $\mathbf{y}$ is a canonical level-1 encoding of 1 that is included in *params*, part of the public parameter $PP$. The signature is accepted if and only if the zero testing algorithm outputs 1.

Correctness. The correctness property requires that each valid ring signature can pass the verification algorithm. In the above ring signature scheme, the signature $\mathbf{s}$ is a level-$k-1$ encoding of $\prod_{i\in[l]} \mathbf{a}_{i,m[i]} \cdot \prod_{j\in[N]} \mathbf{b}_j$. Since $\mathbf{y}$ is a canonical level-1 encoding of 1, $\mathbf{s}\cdot\mathbf{y}$ is a level-$k$ encoding of $\prod_{i\in[l]} \mathbf{a}_{i,m[i]} \cdot \prod_{j\in[N]} \mathbf{b}_j$. On the other hand, $H(m)\cdot\prod_{i\in[N]} \mathbf{B}_i$ is also level-$k$ encoding of $\prod_{i\in[l]} \mathbf{a}_{i,m[i]} \cdot \prod_{j\in[n]} \mathbf{b}_j$. Therefore, it can be concluded that all valid ring signatures will be pass the testing algorithm, as long as the underlying algorithms run correctly in GGH graded encoding system, e.g. samp( ),enc( ), re-Rand( ).

## 4 Security Analysis

In this section, according to the security model that is defined in Sect. 3, we analyze the anonymity and unforgeability of the proposed ring signature scheme in the standard model.

### 4.1 Anonymity

**Theorem 1.** If the GDDH assumption holds, then the proposed ring signature scheme based on GGH graded encoding system satisfies the unconditional anonymity.

Proof. According to the anonymity game in Sect. 3, the proof of Theorem 1 is as follows.

(a) According to the corresponding parameters in the proposed signature scheme, the challenger runs $(params, \mathbf{p}_{zt}) \leftarrow \text{InstGen}(1^{\lambda}, 1^{k=N+l})$ to generate a GGH instance, and chooses random encodings $\mathrm{a}_{i,v} \leftarrow \text{samp}(), i \in [l], v \in \{0,1\}$. At the same time, for the users $U_1, \cdots U_N$, the challenger picks out random encodings $\mathbf{b}_j \leftarrow \text{samp}(), j \in [N]$. The private key of user $U_{j\in[N]}$ is $\mathrm{b}_j$ while the public key is $\mathbf{B}_j = \text{re-enc}(1, \mathbf{b}_j)$. Let $\mathbf{A}_{i,v} = \text{re}-\text{enc}(1, \mathbf{a}_i)$ for $i \in [l]$ and $v \in \{0,1\}$, and a set of public keys $\bar{R} = \{\mathbf{B}_1, \cdots, \mathbf{B}_n\}$ denotes the ring. Finally, the challenger sends $PP = \{params, (\mathbf{A}_{1,0}, \mathbf{A}_{1,1}), \ldots, (\mathbf{A}_{l,0}, \mathbf{A}_{l,1})\}$ and $\bar{R}$ to the adversary $\mathcal{A}$.

(b) The adversary makes polynomially many ring signing queries for messages $m \in \{0,1\}^l$ with respect to the ring $\bar{R}$. After receiving them, the challenger calls the algorithm Sign in Sect. 3 and returns the results to $\mathcal{A}$.

(c) The adversary continues to adaptively query the signing secret key of the $j$ - th user, where $j \in [N]$. The challenger replies the corresponding secret key $\mathrm{b}_j$.

(d) The adversary chooses a message $m \in \{0,1\}^l$ and two members $w_0, w_1 \in U_{i\in[N]}$ in the ring, and sends them to the challenger. After receiving them, the challenger chooses a random bit $b \in \{0,1\}$ and replies a ring signature $\mathbf{s}^* \leftarrow \text{Sign}(PP, m, \mathrm{b}_{w[b]}, \bar{R})$ where $\mathrm{b}_{w[b]}$ is the corresponding signing secret key of the user $w_b$.

(e) Finally, $\mathcal{A}$ wants to determine the identity of signer and outputs a guess $b^* \in \{0,1\}$ for $b$.

Now, let us analyze the advantage of $\mathcal{A}$. On the one hand, According to the algorithm Sign in the proposed signature scheme, each valid ring signature in the above

game is a random encoding on the level-$k-1$. Therefore, we only need to analyze the distribution of the ring signature. Firstly, regardless of the ring signature $\mathbf{s}^*$ from the user $w_0$ or the user $w_1$, the valid signature $\mathbf{s}^*$ on message $m \in \{0,1\}^l$ about $\bar{R}$ is a random level-$k-1$ encoding of $\prod_{i\in[l]} \mathbf{a}_{i,m[i]} \cdot \prod_{j\in[N]} \mathbf{b}_j$(Accurately, which is a level-$k-1$ encoding of the coset $\prod_{i\in[l]} \mathbf{a}_{i,m[i]} \cdot \prod_{j\in[N]} \mathbf{b}_j + I$). That is, for the same message, the distribution of the ring signature from the different members in the ring is indistinguishable. On the other hand, without loss of generality, we can assume that the private key of the user $w_b$ is $\mathrm{b}_1$. According to the definition of GDDH assumption, the adversary cannot distinguish between the level-$(k-1)$ encoding $\mathbf{s}_1 \leftarrow \mathbf{b}_1 \cdot H(m^*) \cdot \prod_{i\in[N]\cap i\neq 1} \mathbf{B}_i$ that is the ring signature computed by challenger and an element $\bar{\mathbf{s}}_1 \leftarrow \mathbf{d}^* \cdot H(m^*) \cdot \prod_{i\in[N]\cap i\neq 1} \mathbf{B}_i$ that is obtained for a random and independent $\mathbf{d}^* \leftarrow \mathrm{samp}()$. Because of the randomness property of the sampling procedure, $\bar{\mathbf{s}}_1$ is nearly uniformly distributed among the cosets of $I$. Therefore, we can conclude that the advantage $Anon_{\mathcal{A}}^{\Phi-\mathrm{fke}}$ can be ignored, and the proposed ring signature scheme is unconditional anonymity.

### 4.2 Unforgeability

In this section, according to the unforgeable security model described in Sect. 2, we will prove the existential unforgeability of the proposed ring signature in the standard model, which could be reduced to the GDDH problem that holds for the underlying encoding scheme. To prove the existential unforgeability in the fixed-ring setting, we employ the Hohenberger's approach used in [19]. Specifically, we firstly consider the selective variant to the proposed scheme,then from which the adaptive security can be derived.

**Theorem 2.** The proposed ring signature scheme for message length l and the number of members N is selectively secure in the unforgeability game under $k$-GCDH assumption where $k = l + N$.

Proof. With the usual method of reduction, assume there is a polynomial-time algorithm (the forger) $\mathcal{F}$ that can break the selective security of the proposed ring signature scheme with probability $\varepsilon$ for message length $l$ and the number of members $N$, then we can construct an efficient algorithm (the challenger) that can break the $k$-GCDH assumption with probability $\varepsilon$.

Now, given a GGH's GCDH instance $E = \{params, \mathbf{p}_{zt}, \mathbf{C}_1 \leftarrow \mathrm{re}-\mathrm{enc}(1, \mathbf{a}_1), \cdots \mathbf{C}_k \leftarrow \mathrm{re}-\mathrm{enc}(1, \mathbf{a}_k)\}$ where $\mathbf{a}_i \leftarrow \mathrm{samp}()$, $k = l + N$ and $i \in [k]$. The challenger employs $\mathcal{F}$ to solve GCDH problem as follows.

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

**Setup.** The challenger chooses random $\mathbf{z}_1, \cdots \mathbf{z}_l$ by calling to the algorithm samp() and generates the corresponding level-1 encodings $\mathbf{Z}_i \leftarrow \mathrm{re}-\mathrm{enc}(1, \mathbf{z}_i)$ where $i \in [l]$. Let $m^*[i]$ be the bits of message $m^* \in \{0,1\}^l$ and $\bar{m}^*[i]$ denote $(1 - m^*[i])$. For $i = 1$ to $l$, let $\mathbf{A}_{i,m*[i]} = \mathbf{C}_i$ and $\mathbf{A}_{i,\bar{m}*[i]} = \mathbf{Z}_i$. In addition, let $\bar{R} = \{\mathbf{C}_{l+1}, \cdots \mathbf{C}_{l+N}\}$ denote the set of public keys of $N$ users in the ring. Finally, the challenger sends the common public

parameter $PP = \{params, (\mathbf{A}_{1,m^*[1]}, \mathbf{A}_{1,\bar{m}^*[1]}), \cdots (\mathbf{A}_{l,m^*[l]}, \mathbf{A}_{l,\bar{m}^*[l]})\}$ as well as the set $\bar{R} = \{\mathbf{C}_{l+1}, \cdots \mathbf{C}_{l+N}\}$ to the forger $F$. It is noted that the parameters are distributed independently and uniformly at random as in the real scheme.

**Query.** The forger $\mathcal{F}$ chooses messages $m \in \{0,1\}^l$ and $m \neq m^*$. Then it requests ring signature under $\bar{R}$ on these $l-$ bit messages. Let $j$ be the first index such that $m[j] \neq m^*[j]$. The challenger computes $\mathbf{s}_1 = \mathbf{z}_j \cdot \prod_{i \in l \cap i \neq j} \mathbf{A}_{m[i]} \cdot \prod_{l+1 \leq v \leq l+N} \mathbf{C}_v$ and $\mathbf{s} = \text{re-enc}(k-1, \mathbf{s}_1)$. Next, the challenger takes $\mathbf{s}$ as the ring signature on $m$ and returns it to $\mathcal{F}$.

Since the result of $\text{IsZero}(\mathbf{s} \cdot \mathbf{y} - H(m) \cdot \prod_{l+1 \leq v \leq l+N} \mathbf{C}_v)$ is 1, where $H(m)$ is a level-$l$ encoding of $\prod_{i \in [l]} \mathbf{A}_{m[i]}$ and $H$ is the full domain hash function based on GGH, the signature can pass the verification of $\text{Verf}(PP, \mathbf{s}, m, \bar{R})$. Namely, the responses of the challenger are valid ring signatures, which are distributed statistically exponentially closely to the real unforgeability game because of the rerandomization in the re-enc algorithm.

**Response.** The forger $\mathcal{F}$ outputs a ring signature $\mathbf{s}^*$ on the forgery message $m^*$.

Now, we analyze the reduction and show that the ring signature $\mathbf{s}^*$ is a solution of the GCDH instance $E = \{params, \mathbf{p}_{zt}, \mathbf{C}_1 \leftarrow \text{re} - \text{enc}(1, \mathbf{c}_1), \cdots \mathbf{C}_k \leftarrow \text{re} - \text{enc}(1, \mathbf{c}_k)\}$. If $\mathbf{s}^*$ is a valid ring signature on message $m^*$, it should pass the verification such as $1 \leftarrow \text{IsZero}(\mathbf{s}^* \cdot \mathbf{y} - H(m^*) \cdot \prod_{l+1 \leq v \leq l+N} \mathbf{C}_v)$. However we know that $H(m^*) \cdot \prod_{l+1 \leq v \leq l+N} \mathbf{C}_v = \prod_{i \in [l]} A_{m^*[i]} \cdot \prod_{l+1 \leq v \leq l+N} \mathbf{C}_v$ is a level-$k$ encoding of $(\prod_{i \in [k]} \mathbf{c}_i)$. Therefore, the verification of the ring signature $\mathbf{s}^*$ implies a solution to $E$. Consequently, the challenger succeeds whenever the forger does, and the Theorem 2 is proved.

With the invention of GGH graded coding system as a multilinear maps candidate, to design more common cryptographic primitives based on multi-linear maps becomes a hot research topic. In this paper, we construct a novel ring signature scheme and prove its security in standard model. Under the graded decisional Diffie-Hellman (GDDH) assumption and grade computational Diffie-Hellman (GCDH) assumption, the new ring signature scheme guarantees the anonymity of signer even if the secret key of the signer is exposed and holds the existential unforgeability against adaptive chosen message attack, respectively. However, the main disadvantage of the proposed scheme is that the size of public key is more than that of the schemes based on bilinear-pairing. Recently, Coron et al. proposed a practical grading encoding system in integer ring [22]. We will attempt to use the integer ring instead of ideal lattice to reduce the size of public key.

**Acknowledgements.** This work is supported by the Research Fund for the Graduate Innovation Program of Jiangsu Province (CXZZ13_0493), and the Natural Science Foundation of Universities of Jiangsu Province (13KJB520005).

## References

1. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_32

2. Bender, A., Katz, J., Morselli, R.: Ring signatures: stronger definitions, and constructions without random Oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 60–79. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_4
3. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret: theory and applications of ring signatures. In: Goldreich, O., Rosenberg, A.L., Selman, A.L. (eds.) Theoretical Computer Science. LNCS, vol. 3895, pp. 164–186. Springer, Heidelberg (2006). https://doi.org/10.1007/11685654_7
4. Bresson, E., Stern, J., Szydlo, M.: Threshold ring signatures and applications to Ad-hoc groups. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 465–480. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45708-9_30
5. Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous identification in *Ad Hoc* groups. In: Cachin, C., Camenisch, Jan L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 609–626. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_36
6. Xiao, F.J., Liao, J., Zeng, G.H.: Threshold ring signature for wireless sensor networks. J. Commun. **32**(3), 75–81 (2012)
7. Chow, S.S.M., Yiu, S.-M., Hui, L.C.K.: Efficient identity based ring signature. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 499–512. Springer, Heidelberg (2005). https://doi.org/10.1007/11496137_34
8. Yuen, T.H., Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Efficient linkable and/or threshold ring signature without random oracles. Comput. J. **56**(4), 407–421 (2013)
9. Wang, F.H., Hu, Y.P., Wang, C.X.: A lattice-based ring signature scheme from bonsai trees. J. Electron. Inf. Technol. **32**(10), 2410–2413 (2010)
10. Wang, J., Sun, B.: Ring signature schemes from lattice basis delegation. In: Qing, S., Susilo, W., Wang, G., Liu, D. (eds.) ICICS 2011. LNCS, vol. 7043, pp. 15–28. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25243-3_2
11. Brakerski, Z., Kalai, Y.T.: A framework for efficient signatures, ring signatures and identity based encryption in the standard model. Cryptology ePrint Archive: Report 2010/86 (2010)
12. Tian, M.M., Liu, L.S., Yang, W.: Efficient lattice-based ring signature scheme. Chin. J. Comput. **35**(4), 712–716 (2012)
13. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Presented at the Proceedings of the 40th Annual ACM Symposium on Theory of Computing. Victoria, British Columbia, Canada, pp. 120–131 (2008)
14. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
15. Aguilar Melchor, C., Bettaieb, S., Boyen, X., Fousse, L., Gaborit, P.: Adapting lyubashevsky's signature schemes to the ring signature setting. In: Youssef, A., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 1–25. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38553-7_1
16. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_43
17. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_1
18. Boneh, D., Silverberg, A.: Applications of multilinear forms to cryptography. Contemp. Math. **324**(1), 71–90 (2003)

19. Hohenberger, S., Sahai, A., Waters, B.: Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 494–512. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_27
20. Wang, H., Wu, L., Zheng, Z., Wang, Y.: Identity-based key-encapsulation mechanism from multilinear maps. Cryptology ePrint: Archive: Report 2013/836 (2013)
21. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: Proceedings of the 45th Annual ACM Symposium on Symposium on Theory of Computing, pp. 545–554 (2013)
22. Coron, J.-S., Lepoint, T., Tibouchi, M.: Practical multilinear maps over the integers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 476–493. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_26