A BLS Signature Scheme from Multilinear Maps

Fei Tang[1] and Dong Huang[2,3]
(Corresponding author: Fei Tang)

School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications[1]
Chongqing, China
Chongqing University of Science and Technology [2]
Chongqing Vocational and Technical University of Mechatronics[3]
(Email: tangfei@cqupt.edu.cn)

(Received Mar. 12, 2019; Revised and Accepted Dec. 10, 2019; First Online Apr. 6, 2020)

Abstract

The security of the BLS signature scheme is based on the random oracle model. Hence, there is a question that how to instantiate BLS scheme without random oracles. In this work, by using a powerful tool multilinear map, we answer this question. The main contributions of this work are as follows. First of all, we describe the BLS scheme in the setting of multilinear group and prove its security in the standard model. Then, we design a ring signature scheme based on the multilinear BLS scheme. In the proposed scheme, ring signatures consist of a single multilinear group element.

Keywords: BLS Signatures; Multilinear Map; Ring Signatures; Standard Model

1 Introduction

Digital signatures are one of the most fundamental and well studied cryptographic primitives. The research of digital signatures has two aspects: practicability and security. As for the aspect of practicability, we mainly consider the efficiencies of the signing and verification algorithms, the storage space of the state information, and the properties that the scheme can provide, such as aggregate signatures [17], ring signatures [23], blind signatures [16,19,20] and so on. As for the aspect of the security, we mainly focus on the assumptions that the scheme based on, such as one-way function, and whether in the random oracle model or standard model.

At ASIACRYPT 2001, Boneh, Lynn, and Shacham [6] designed a short signature scheme based on bilinear group, the so called BLS scheme. The BLS scheme has shown to be very useful to construct other cryptographic primitives, such as threshold signature scheme [7], blind signature scheme [7], signcryption scheme [10], key-generation algorithm of identity-based encryption (IBE) scheme [4]. The main reason of the BLS scheme is so useful is that it has a relatively simple structure. The security of the BLS scheme is rely on the random oracle model. However, it is well known that random oracle is an ideal model. After BLS scheme, there has several works that presented some signature schemes which secure in the standard model, such as [3]. However, all of these schemes do not preserve the BLS scheme's simple structure. This leads us to a question: *Can we instantiate the BLS signature scheme without random oracles?* In this work, by using a powerful tool multilinear map, we answer this question.

The notion of multilinear maps was introduced (but without concrete instantiation) by Boneh and Silverberg [8]. Until 2013, Garg, Gentry, and Helevi [12] gave the first approximate candidate. Then there has many multilinear map schemes been proposed or analyzed, *e.g.*, [9,15,21] *et al.*

There are several relevant works answered the above question. Hohenberger *et al.* [18] instantiated the random oracle with an actual family of hash functions for the BLS scheme by using a more powerful tool indistinguishability obfuscation [13]. Freire *et al.* [11] took advantage of multilinear maps to realize programmable hash functions and construct IBE, BLS signature, and SOK non-interactive key exchange schemes. In addition, Hohenberger *et al.* [17] made use of the multilinear BLS scheme to construct an (identity-based) aggregate signature scheme which admits unrestricted aggregation. In [17], Hohenberger *et al.* followed in the Waters [25] framework and proved the adaptive security of the multilinear BLS signature scheme.[1] However, their proof is based on a *strong* new assumption, (n,k)-modified multilinear computational Diffie-Hellman exponent where n is a polynomial of the number of queries made by the adversary.

In this work, we also give an adaptive proof for the multilinear BLS scheme. However, our proof which takes advantage of the technique of admissible hash function [2] is based on a *weaker* assumption, multilinear computa-

[1] Their adaptive proof of the aggregate signature scheme implies this result. (Please refer to Appendix D.2 of [17] for details.)

tional Diffie-Hellman assumption [12]. In addition, we consider the applications of the multilinear BLS signature scheme. It can be served as the key-generation algorithm of the multilinear IBE scheme [11]. It also can be used to construct aggregate signature [17], threshold signature scheme [7] and so on. In this work, we take advantage of the structure of the multilinear BLS scheme to construct a ring signature scheme in the standard model. In a ring signature scheme [23], a signer can generate signatures on behalf of a group of users (*i.e.*, ring) if and only if he is a member of the ring. Then, any verifier can confirm that the message has been signed by one of the members in the ring, but he cannot know who is the real signer. Our ring signature scheme has an attractive feature that for n members of a ring the signatures consist of just a single group element.

2 Preliminaries

2.1 Notations

The following notations will be used in this paper. Let $\mathbb{Z}$ be the set of integers and $\mathbb{Z}_p$ be the ring modulo p. 1^λ denotes the string of λ ones for $\lambda \in \mathbb{N}$. $|x|$ denotes the length of the bit string x. $[k]$ is a shorthand for the set $\{1, 2, \ldots, k\}$. Finally, we write PPT for the probabilistic polynomial time.

2.2 Multilinear Maps

Let $(\mathbb{G}_1, \ldots, \mathbb{G}_k)$ be a sequence of groups each of large prime order p, and g_i be a generator of group $\mathbb{G}_i$, where we let $g = g_1$. There exists a set of bilinear maps $\{\mathbf{e}_{i,j} : \mathbb{G}_i \times \mathbb{G}_j \to \mathbb{G}_{i+j} | i, j \geq 1 \land i + j \leq k\}$, which satisfy:

$$\mathbf{e}_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab} : \forall a, b \in \mathbb{Z}_p.$$

When the context is obvious, we omit the indexes i and j, *i.e.*, $\mathbf{e}(g_i^a, g_j^b) = g_{i+j}^{ab}$. It also will be convenient to abbreviate $\mathbf{e}(h_1, h_2, \ldots, h_j) = \mathbf{e}(h_1, \mathbf{e}(h_2, \ldots, \mathbf{e}(h_{j-1}, h_j) \ldots)) \in \mathbb{G}_i$ for $h_j \in \mathbb{G}_{i_j}$ and $i_1 + i_2 + \ldots + i_j \leq k$.

Let $\mathsf{MulGen}(1^\lambda, k)$ be a PPT multilinear group generator algorithm which takes as input a security parameter λ and an integer k, where k is the number of allowed pairing operations, then it outputs the multilinear parameters $\mathbb{MP} = (\mathbb{G}_1, \ldots, \mathbb{G}_k, p, g = g_1, g_2, \ldots, g_k, \mathbf{e}_{i,j})$ to satisfy the above properties.

In recent years, there has many multilinear maps been proposed, *e.g.*, [9,12,14,22]. However, some of them have been shown to be insecure, *e.g.*, [15, 21]. Fortunately, there still has several multilinear maps are beyond the existing cryptanalysis, *e.g.*, [1,14]. Therefore, we also can use this tool to design cryptographic schemes. For example, [26,28,29] take advantage of the multilinear maps to design different cryptographic schemes.

2.3 Complexity Assumption

We assume that the following assumption holds in the setting described above: Multilinear Computational Diffie-Hellman (MCDH) assumption.

Definition 1. For any PPT algorithm $\mathcal{B}$, any polynomial $p(\cdot)$, any integer k, and all sufficiently large $\lambda \in \mathbb{N}$,

$$\Pr\left[\begin{array}{ll} \mathbb{MP} \leftarrow \mathsf{MulGen}(1^\lambda, k); & \\ c_1, \ldots, c_k \xleftarrow{R} \mathbb{Z}_p; & : v = g_{k-1}^{\prod_{i\in[k]} c_i} \\ v \leftarrow \mathcal{B}(\mathbb{MP}, g^{c_1}, \ldots, g^{c_k}) & \end{array}\right] < \frac{1}{p(\lambda)}.$$

This assumption can be viewed as an adaptation of the Bilinear Computational Diffie-Hellman (BCDH) assumption [4] in the setting of multilinear groups.

3 Digital Signatures

3.1 Definitions

For ease of description, we define digital signature schemes with four algorithms: Setup, KeyGen, Sign, and Vrfy. Formally, given a security parameter λ, the PPT algorithm Setup, run by a trusted authority, generates public parameters $\mathbb{PP}$. The public parameters will be used in all of the following three algorithms, for simplicity, we omit this fact. The PPT algorithm KeyGen outputs a signing/verification key pair (SK, VK) for the signer. The PPT algorithm Sign takes as input a signing key SK and a message M, then outputs a signature σ. Finally, the deterministic algorithm Vrfy processes a purported signature σ with respect to a message M and verification key VK, accordingly, it outputs 1 to indicate a successful verification and 0 otherwise.

3.2 Existential Unforgeability

The security model for signature schemes is Existential Unforgeability against adaptive Chosen-Message Attacks (EU-CMA) which is defined by the following game.

1) **Setup:** Challenger runs Setup and KeyGen algorithms to generate the public parameters and challenge keys (SK^*, VK^*). Adversary $\mathcal{A}$ is given the public parameters and VK^*.

2) **Signing queries:** Adversary $\mathcal{A}$ is allowed to adaptively queries the signing oracle at most q times on messages $M_1, \ldots, M_q$. In its i-th query, it receives back a signature $\sigma_i \leftarrow \mathsf{Sign}(SK^*, M_i)$.

3) **Output:** Finally, adversary $\mathcal{A}$ outputs a tuple of (M^*, σ^*), where $M^* \neq M_i$ for all $i \in [q]$. $\mathcal{A}$ wins the game if $\mathsf{Vrfy}(VK^*, M^*, \sigma^*) = 1$.

We denote the success probability of a PPT adversary $\mathcal{A}$ (taken over the random choices of the challenger and adversary) to win the game as $\mathbf{Adv}_{\mathcal{A}}^{eu-cma}$.

Definition 2. We say that a signature scheme is EU-CMA secure, if for any PPT adversary $\mathcal{A}$, it cannot win the above game with non-negligible advantage.

Selective security. The model of selective security is a weaker notion of the model of EU-CMA. In such model, we require that the adversary gives its challenge message M^* before the setup phase, then it cannot make signing query for M^*.

Definition 3. We say that a signature scheme is selectively secure, if for any PPT adversary, it cannot win the selective game with non-negligible advantage.

4 Multilinear BLS Scheme

In this section, we describe the multilinear BLS signature scheme and its security.

4.1 Construction

We specify the message space $\mathcal{M} := \{0,1\}^\ell$, more generally, a collision resistant hash function can be used to hash messages to this size. The construction of the multilinear BLS signature scheme is as follows:

- $\mathsf{Setup}(1^\lambda, \ell)$: Trusted authority takes as input a security parameter λ and the length ℓ of messages to runs this algorithm to generate the public parameters. It first runs $\mathbb{MP} = (\mathbb{G}_1, \ldots, \mathbb{G}_k, p, g, \ldots, g_k, \mathbf{e}) \leftarrow \mathsf{MulGen}(1^\lambda, k = \ell+1)$. Next, it chooses 2ℓ random integers $(a_{1,0}, a_{1,1}), \ldots, (a_{\ell,0}, a_{\ell,1}) \in \mathbb{Z}_p^2$ and computes $A_{i,\beta} = g^{a_{i,\beta}} \in \mathbb{G}_1$, for $i \in [\ell]$ and $\beta \in \{0,1\}$. The public parameters $\mathbb{PP}$ contain the group descriptions $\mathbb{MP}$ and $(A_{1,0}, A_{1,1}), \ldots, (A_{\ell,0}, A_{\ell,1})$.

- $\mathsf{KeyGen}(\mathbb{PP})$: Each user chooses a random element $x \in \mathbb{Z}_p$ as his signing key SK. The corresponding verification key is $VK = g^x \in \mathbb{G}_1$.

- $\mathsf{Sign}(SK, M)$: Given a message, M, of length ℓ, let $m_1, \ldots, m_\ell$ be the bits of this message, the signer computes the signature as:

$$\sigma = \mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell})^x = (g_{k-1}^{\prod_{i=1}^{\ell} a_{i,m_i}})^x \in \mathbb{G}_{k-1}.^2$$

- $\mathsf{Vrfy}(VK, M, \sigma)$: Given a verification key VK and a purported signature σ on message M, verify the following equation:

$$\mathbf{e}(\sigma, g) \stackrel{?}{=} \mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell}, VK).$$

Correctness. To see the correctness, a signature σ on message M is $(g_{k-1}^{\prod_{i=1}^{\ell} a_{i,m_i}})^x$, and thus we have $\mathbf{e}(\sigma, g) = \mathbf{e}((g_{k-1}^{\prod_{i=1}^{\ell} a_{i,m_i}})^x, g) = \mathbf{e}((g_{k-1}^{\prod_{i=1}^{\ell} a_{i,m_i}}), g^x) = \mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell}, VK)$.

4.2 Security of Multilinear BLS Scheme in the Standard Model

We now prove the security of the multilinear BLS scheme in the standard model based on the MCDH assumption. Our proof needs an admissible hash function h which can be used to partition the message space to two subsets with probability $1/\theta(q)$ (where q is the upper bound of the adversary's queries) so that: the adversary's query messages M_i fall in one subset where we know a trapdoor that allows us to answer its queries, and the adversary's challenge message M^* falls in the other set where we do not know any trapdoor but hope to embed a challenge element. We show that we can leverage the structure of the multilinear BLS signature scheme to prove adaptive security. For simplicity of exposition, we assume that there is a polynomial $s(\lambda)$ which denotes the length of messages space to be signed. We use a function $h : \{0,1\}^{s(\lambda)} \to \{0,1\}^{\ell(\lambda)}$ maps the messages to ℓ bits, and an efficient randomized algorithm Sample that is θ-admissible. The following definition of admissible hash functions is from [17] which is a slight variant of the simplified definition in [11].

Definition 4. Let s, ℓ and θ be efficiently computable univariate polynomials. We say that a function $h : \{0,1\}^{s(\lambda)} \to \{0,1\}^{\ell(\lambda)}$, and an efficient randomized algorithm Sample, are *θ-admissible* if the following properties hold:

- For any $u \in \{0,1,\perp\}^\ell$, define $P_u : \{0,1\}^s \to \{0,1\}$ as follows: $P_u(X) = 0$ iff $\forall i : h(X)_i \neq u_i$, and otherwise (if $\exists i : h(X)_i = u_i$) we have $P_u(X) = 1$.

- We require that for any efficiently computable polynomial $q(\lambda)$, for all $X_1, \ldots, X_q, Z \in \{0,1\}^s$, where $Z \notin \{X_i\}$, we have $\Pr[P_u(X_1) = \ldots = P_u(X_q) = 1 \wedge P_u(Z) = 0] \geq 1/\theta(q)$, where the probability is taken only over $u \leftarrow \mathsf{Sample}(1^\lambda, q)$.

Theorem 1. For any efficiently computable polynomials s, ℓ, there exists an efficiently computable polynomial θ such that there exists θ-admissible function families mapping s bits to ℓ bits.

The construction is identical to the multilinear BLS scheme with the exception of the Setup algorithm creates the admissible hash functions. Then the signing and verification algorithms take as input $h(M)$ instead of M.

Theorem 2. If h is a θ-admissible function and the k-MCDH problem is hard in the multilinear groups, then the multilinear BLS signature scheme with an admissible hash is adaptively secure.

[2] In the bilinear BLS signature scheme [6], signer computes a signature as $\sigma = H(M)^x$, where $H(\cdot)$ is a collision-resistant hash function that will be treated as a random oracle in the proof. In the multilinear BLS signature scheme, $H(M)$ is defined as $\mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell})$ which can be computed from the public parameters of the (leveled) multilinear maps.

Proof. If there exists a PPT adversary $\mathcal{A}$ who can break the security of the multilinear BLS signature scheme with an admissible hash in the EU-CMA game with advantage ϵ for message length s, level k of the multilinear maps, and security parameter λ, then we can construct a PPT challenger $\mathcal{B}$ to break the k-MCDH assumption with probability $\epsilon' \geq \epsilon/\theta(q)$. The challenger $\mathcal{B}$ takes as input a k-MCDH instance $(g^{c_1}, \ldots, g^{c_k})$ together with the group descriptions $\mathbb{MP}$ to interactive with the adversary. The challenger's goal is to compute $g_{k-1}^{\prod_{i\in[k]} c_i}$.

We describe the proof as a sequence of hybrid games where the first hybrid corresponds to the original EU-CMA game. Then in the first hybrid step we do a "partitioning" of the space of the messages. After the first proof step, we prove that any PPT adversary's advantage must be close with negligible gap at most between each successive hybrid games. We finally show that any PPT adversary in the final game that succeeds with non-negligible advantage can be used to break the k-MCDH assumption.

- Game_0 is the original EU-CMA game.
  1) **Setup:** Challenger $\mathcal{B}$ runs $\mathsf{MulGen}(1^\lambda, k)$ to produce group parameter $\mathbb{MP}$. It then chooses a random exponent $x \in \mathbb{Z}_p$ for the secret key and sets the challenge verification key as $VK^* = g^x$. It also randomly chooses $(a_{1,0}, a_{1,1}), \ldots, (a_{\ell,0}, a_{\ell,1})$ from $\mathbb{Z}_p$ and computes $A_{i,\beta} = g^{a_{i,\beta}}$ for $i \in [\ell], \beta \in \{0,1\}$. Finally, it sets $\mathbb{PP} = (\mathbb{MP}, \{A_{i,\beta} | i \in [\ell], \beta \in \{0,1\}\})$ and gives $\mathbb{PP}$ and VK^* to the adversary $\mathcal{A}$.
  2) **Signing queries:** Adversary $\mathcal{A}$ adaptively queries the signing oracle at most q times on messages $M_1, \ldots, M_q$. In its i-th query, it receives back $\mathbf{e}(A_{1,m_{i_1}}, \ldots, A_{\ell,m_{i_\ell}})^x$ from challenger $\mathcal{B}$.
  3) **Output:** At some point $\mathcal{A}$ outputs a forgery σ^* with respect to the challenge key VK^* and message M^*, it wins the game if $\mathsf{Vrfy}(VK^*, M^*, \sigma^*) = 1$ and $M^* \neq M_i$ for $i \in [q]$.
- Game_1 is the same as Game_0 except that the challenger begins by sampling a string $u \in \{0, 1, \perp\}^\ell$ by revoking $u \leftarrow \mathsf{Sample}(1^\lambda, q)$. At the end of the game, the adversary is only considered to be successful if both its output satisfies the winning conditions and for the challenge message M^* we have $P_u(M^*) = 0$ and for all messages M_i queried $P_u(M_i) = 1$.
- Game_2 is the same as Game_1 except that the following modification. The challenger sets the parameters $(A_{1,0}, A_{1,1}), \ldots, (A_{\ell,0}, A_{\ell,1})$ in the following way: for $i \in [\ell]$ and $\beta \in \{0,1\}$ it chooses random $b_{i,\beta} \in \mathbb{Z}_p$ and sets

$$A_{i,\beta} = \begin{cases} g^{b_{i,\beta}}, & \text{if } \beta = u_i \\ (g^{c_i})^{b_{i,\beta}}, & \text{if } \beta \neq u_i. \end{cases}$$

Lemma 1. Assume an adversary that makes at most a polynomial of signing queries $q = q(\lambda)$ in Game_0. If the advantage of an adversary in Game_0 is ϵ, then the advantage of the adversary in Game_1 will be at least $\epsilon/\theta(q)$. In particular, any PPT adversary with non-negligible advantage in Game_0 will also have non-negligible advantage in Game_1.

Proof. The lemma follows immediately from the property of function h satisfies the definition of a θ-admissibility, since the only independent choice of $u \leftarrow \mathsf{Sample}(1^\lambda, q)$ determines whether or not the game aborts. □

Lemma 2. The advantage of any PPT adversary in Game_2 is the same as its advantage in Game_1.

Proof. The two games are equivalent as all $A_{i,\beta} \in \mathbb{G}_1$ are still set to uniformly at random in both games. □

Lemma 3. If the k-MCDH assumption holds, then the advantage of any PPT adversary in Game_2 is negligible.

Proof. We prove this lemma by giving a reduction to the k-MCDH assumption. To do so, we construct an algorithm $\mathcal{B}$.

$\mathcal{B}$ takes as input a k-MCDH problem instance $(\mathbb{MP}, g^{c_1}, \ldots, g^{c_k})$. Next, $\mathcal{B}$ runs $u \leftarrow \mathsf{Sample}(1^\lambda, q)$. It sets the challenge key as $VK^* = g^{c_k}$. All these steps together simulate the Setup phase of the Game_2. Now, it plays the game with the adversary $\mathcal{A}$ by using public parameters $\mathbb{PP} = (\mathbb{MP}, \{A_{i,\beta} | i \in [\ell], \beta \in \{0,1\}\})$ and challenge key VK^*.

The adversary $\mathcal{A}$ will then adaptively make at most q signing queries each for message M_i. If $P_u(M_i) = 0$, $\mathcal{B}$ aborts and quits. Otherwise, $P_u(M_i) = 1$ and there exists an γ we have $h(M_i)_\gamma = u_\gamma$. Thus, $\mathcal{B}$ can compute the signature as $\sigma = \mathbf{e}(A_{1,h(M_i)_1}, \ldots, A_{\gamma-1,h(M_i)_{\gamma-1}}, A_{\gamma+1,h(M_i)_{\gamma+1}}, \ldots, A_{\ell,h(M_i)_\ell}, VK^*)^{b_{\gamma,h(M_i)_\gamma}}$ by knowing the exponent $b_{\gamma,h(M_i)_\gamma}$ of the parameter $A_{\gamma,h(M_i)_\gamma}$.

Finally, the adversary $\mathcal{A}$ outputs an attempted forgery σ^* with respect to the challenge verification VK^* on some message M^*. $\mathcal{B}$ first checks the signature verification $\mathsf{Vrfy}(VK^*, M^*, \sigma^*)$ and aborts if it returns 0. Next, it checks if $P_u(M^*) = 1$ and aborts if that is the case. Otherwise, $P_u(M^*) = 0$ and for all i we have $h(M^*)_i \neq u_i$. This means that the hash of M^* will be $g_{k-1}^{\prod_{i\in[k-1]} c_i}$ raised to some known product of $b_{i,\beta}$ values. The signature therefore contains $g_{k-1}^{\prod_{i\in[k]} c_i}$ raised to some known product of $b_{i,\beta}$ values. This value can be recovered by taking the proper root of the signature, *i.e.*, $(\sigma^*)^{1/\prod_{i\in[\ell]} b_{i,h(M^*)_i}} = g_{k-1}^{\prod_{i\in[k]} c_i}$, and thus if σ^* is a successful forgery, then this root of the signature is a solution to the challenge instance of the k-MCDH problem.

By construction of the algorithm $\mathcal{B}$, the probability of $\mathcal{B}$ succeeds is exactly the advantage that the adversary $\mathcal{A}$ succeeds in Game_2. Whenever $\mathcal{B}$ aborted, the adversary by the rules of Game_2 was not considered to be successful since its queries or forgery violated the partition. The lemma follows. □

These three lemmas together yield the main theorem that the multilinear BLS signature scheme with an admissible hash is adaptively secure. □

5 Ring Signatures from Multilinear BLS Scheme

In this section, we show the applications of the multilinear BLS signatures. It can be served as the key-generation algorithm of the multilinear IBE scheme [11], it also can be used to construct aggregate signature [17]. In addition, based on Boldyreva's [7] work, we can easily obtain a threshold signature, a multi-signature, and a blind signature scheme, respectively, based on the multilinear BLS scheme in the standard model. Here, we take advantage of the multilinear BLS scheme to construct a ring signature scheme in the standard model. The resultant scheme has an attractive feature that for n members of a ring our signatures consist of just a single group element.

5.1 Definition of Ring Signatures

For convenience, we define an algorithm Setup, run by trusted authority, to generate public parameters and build the system of the ring signature scheme. The public parameters will be used in all of the following three algorithms. In addition, we refer to an ordered set $R = \{VK_1, \ldots, VK_n\}$ of verification keys as a ring, and let $R[i] = VK_i$. We will also freely use set notation, *e.g.*, $VK \in R$ if there exists an index i such that $R[i] = VK$.

Definition 5. A ring signature scheme contains the following four algorithms:

- $\mathsf{Setup}(1^\lambda) \rightarrow \mathbb{PP}$: The system setup algorithm takes as input a security parameter λ to produce the system public parameters $\mathbb{PP}$.
- $\mathsf{KeyGen}() \rightarrow (SK, VK)$: The key generation algorithm generates users' signing and verification keys (SK, VK).
- $\mathsf{Sign}(SK_s, R, M) \rightarrow \sigma$: The signing algorithm takes as input a message M to be signed, a set of verification keys R (*i.e.*, the ring), and an user's signing key SK_s. It is required that $VK_s \in R$ meanings that the signer is a member of the signing ring. The algorithm outputs a signature σ.
- $\mathsf{Vrfy}(R, M, \sigma) \rightarrow 0/1$: The verification algorithm takes as input a purported signature σ on a ring R and a message M. It outputs 1 if σ is valid. Otherwise, it outputs 0.

5.2 Security Models of Ring Signatures

Security models of the ring signature scheme contains two parts: unforgeability and anonymity.

5.2.1 Ring Unforgeability

This security guarantees that an adversary can compute a valid signature on behalf of a ring only if he knows a secret key corresponding to one of them. In this work, we use Bender *et al.*'s [5] model: unforgeability with respect to insider corruption[3] which is defined by the following game:

1) **Setup:** The challenger runs Setup and KeyGen algorithms to generate public parameters and users' keys $\{(SK_i, VK_i)\}_{i=1}^{n(\lambda)}$. Then it gives the adversary $\mathcal{A}$ the system parameters and verification keys $S = \{VK_i\}_{i=1}^{n(\lambda)}$. In addition, the challenger maintains a set C to record the corrupted users, initially, $C \leftarrow \emptyset$.

2) **Signing queries:** The adversary $\mathcal{A}$ can adaptively make singing queries on inputs (M, R, s), where M is the message to be signed, $R \subseteq S$ is a ring of verification keys and s is an index such that $VK_s \in R$. The challenger returns back a ring signature $\sigma \leftarrow \mathsf{Sign}(SK_s, R, M)$ to $\mathcal{A}$.

3) **Corruption queries:** The adversary $\mathcal{A}$ also can adaptively make some corruption queries on input $s \in [n(\lambda)]$. The challenger returns back SK_s to $\mathcal{A}$ and adds VK_s into the set C.

4) **Output:** Finally, the adversary $\mathcal{A}$ outputs a tuple of (M^*, σ^*, R^*). We say that $\mathcal{A}$ wins the game if the following conditions hold: (1) $\mathsf{Vrfy}(R^*, M^*, \sigma^*) = 1$; (2) $R^* \subseteq S \backslash C$; (3) it never made a singing query (M^*, R^*, s) for any s.

We denote the success probability of a PPT adversary $\mathcal{A}$ (taken over the random choices of the challenger and adversary) to win the above game as $\mathbf{Adv}_{\mathcal{A}}^{Unf}$.

Definition 6. We say that a ring signature scheme has the property of unforgeability with respect to insider corruption, if for any PPT adversary $\mathcal{A}$, it cannot win the above game with non-negligible advantage.

Selective security. We define a weaker notion, selective security, to the above model. In the game of selective security, the adversary $\mathcal{A}$ is required that to give a forgery ring/message pair (R^*, M^*)[4] to the challenger before the setup phase, then it cannot make

[3] We make use of a weaker notion of this security model in which corruptions of honest users are allowed but adversary-chosen public keys are not allowed. This weaker notion has been used in [24, 27].

[4] In the beginning, $\mathcal{A}$ does not given the keys $S = \{VK_i\}_{i=1}^{n(\lambda)}$. In order to obtain the forgery ring R^*, we require that $\mathcal{A}$ outputs a set of index $I_{R^*} = \{i_1, \ldots, i_{|R^*|}\} \subseteq [n(\lambda)]$. Then, after the keys $S = \{VK_i\}_{i=1}^{n(\lambda)}$ be generated, the forgery ring $R^* = \{VK_{i_1}, \ldots, VK_{i_{|R^*|}}\} \subseteq S$ also be defined.

signing query on inputs (M^*, R^*, s) for any s, it also cannot make corruption query on input s for which $VK_s \in R^*$.

Definition 7. We say that a ring signature scheme is selectively unforgeable with respect to insider corruption, if for any PPT adversary $\mathcal{A}$, it cannot win the selective game with non-negligible advantage.

5.2.2 Ring Anonymity

This security guarantees that any verifier can be convinced that someone in the ring has generated a valid ring signature, but the real signer remains unknown. In this paper, we make use of the notion of perfect anonymity. We say that a ring signature scheme is perfectly anonymous, if a signature on a message M^* under a ring R^* and key VK_{i_0} looks exactly the same as a signature on the same message M^* under the same ring R^* and a different key VK_{i_1}. This means that the signer's key is hidden among all the honestly generated keys in the ring. Formally, it is defined by the following game:

1) **Setup:** The challenger runs Setup and KeyGen algorithms to generate public parameters and users' keys $\{(SK_i, VK_i)\}_{i=1}^{n(\lambda)}$. Then it returns back the public parameters and all keys $\{(SK_i, VK_i)\}_{i=1}^{n(\lambda)}$ to the adversary $\mathcal{A}$.

2) **Challenge:** The adversary $\mathcal{A}$ gives a tuple of (M^*, R^*, i_0, i_1), where M^* is the challenge message, R^* is the challenge ring, i_0 and i_1 are two indices such that $\{VK_{i_0}, VK_{i_1}\} \subseteq R^*$, to the challenger. The challenger chooses random $b \in \{0,1\}$, computes $\sigma^* \leftarrow \mathsf{Sign}(M^*, SK_{i_b}, R^*)$, and sends σ^* to the adversary.

3) **Guess:** Finally, the adversary outputs b', indicating his guess for b.

We denote the advantage of an unbounded adversary $\mathcal{A}$ (taken over the random choices of the challenger and the adversary) to win the above game as $\mathbf{Adv}_{\mathcal{A}}^{Ano} = |\Pr[b' = b] - \Pr[b' \neq b]|$.

Definition 8. A ring signature scheme has the property of perfect anonymity, if even an unbounded adversary cannot win the above game with non-negligible advantage.

5.3 Construction

We now construct a ring signature scheme based on the multilinear BLS scheme. We specify the message space $\mathcal{M} := \{0,1\}^\ell$, more generally, a collision resistant hash function can be used to hash messages to this size. Let $m_1, \ldots, m_\ell$ be the bits of the message $M \in \mathcal{M}$. The following construction is an n-user ring signature scheme, means that $|R| = n$.

- $\mathsf{Setup}(1^\lambda, n, \ell)$: Trusted authority takes as input a security parameter λ, the length ℓ of messages and ring size n to runs this algorithm to generate public parameters. It first runs $\mathbb{MP} = (\mathbb{G}_1, \ldots, \mathbb{G}_k, p, g, \ldots, g_k, \mathbf{e}_{i,j}) \leftarrow \mathsf{MulGen}(1^\lambda, k = n + \ell)$. Next, it chooses 2ℓ random values $(a_{1,0}, a_{1,1}), \ldots, (a_{\ell,0}, a_{\ell,1}) \in \mathbb{Z}_p^2$ and computes $A_{i,\beta} = g^{a_{i,\beta}} \in \mathbb{G}_1$, for $i \in [\ell]$ and $\beta \in \{0,1\}$. The public parameters $\mathbb{PP}$ contain the group descriptions $\mathbb{MP}$ and group elements $(A_{1,0}, A_{1,1}), \ldots, (A_{\ell,0}, A_{\ell,1})$.

- $\mathsf{KeyGen}(\mathbb{PP})$: Each user i chooses a random value $x_i \in \mathbb{Z}_p$ as his signing key SK_i. The corresponding verification key is $VK_i = g^{x_i} \in \mathbb{G}_1$.

- $\mathsf{Sign}(M, SK_s, R = \{VK_1, \ldots, VK_n\})$: Given a ring of n verification keys, the holder of signing key SK_s with $s \in [n]$ can sign some message $M \in \mathcal{M}$ as $\sigma = \mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell}, VK_1, \ldots, VK_{s-1}, VK_{s+1}, \ldots, VK_n)^{x_s}$. The signature consists of just a single group element. In fact, $\sigma = g_{k-1}^{(\prod_{i=1}^{\ell} a_{i,m_i})\cdot(\prod_{j=1}^{n} x_j)} \in \mathbb{G}_{k-1}$.

- $\mathsf{Vrfy}(M, \sigma, R = \{VK_1, \ldots, VK_n\})$: Given a ring of n verification keys and a purported signature σ on a message M, check the following equation: $\mathbf{e}(\sigma, g) \overset{?}{=} \mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell}, VK_1, \ldots, VK_n)$.

Correctness. To see the correctness, a signature σ on message M and ring R is $g_{k-1}^{(\prod_{i=1}^{\ell} a_{i,m_i})\cdot(\prod_{j=1}^{n} x_j)}$, and thus we have $\mathbf{e}(\sigma, g) = \mathbf{e}(g_{k-1}^{(\prod_{i=1}^{\ell} a_{i,m_i})\cdot(\prod_{j=1}^{n} x_j)}, g) = \mathbf{e}(g_{k-1}^{\prod_{i=1}^{\ell} a_{i,m_i}}, g^{\prod_{j=1}^{n} x_j}) = \mathbf{e}(A_{1,m_1}, \ldots, A_{\ell,m_\ell}, VK_1, \ldots, VK_n)$.

In the setting of the multilinear maps, the space to represent a group element might grow with k (which is $n + \ell$), because this happens in the GGH [12] framework. To mitigate this problem, we can use the method in [17], which differs the message alphabet size in a tradeoff between computation and storage. The above construction uses a binary message alphabet. If it uses an alphabet of 2^d symbols, then the ring signature could resident in the group $\mathbb{G}_{\ell/d+n}$ with $\ell/d + n - 1$ pairings required to compute it, at the cost of the public parameters requiring $2^d \cdot \ell$ group elements in $\mathbb{G}_1$.

5.4 Security

Theorem 3. The ring signature scheme with message length ℓ and ring size n in the above is selectively unforgeable with respect to insider corruption under the $(n+\ell)$-MCDH assumption.

Proof. If there exists a PPT adversary $\mathcal{A}$ who can break the selective security of the ring signature scheme with advantage ϵ for message length ℓ, ring size n, level $k = n + \ell$ of multilinear maps, and security parameter λ, then we show that we can construct a PPT challenger $\mathcal{B}$ to break the k-MCDH assumption for security parameter λ with probability ϵ. Initially, $\mathcal{A}$ gives $(M^* \in \{0,1\}^\ell, I_{R^*} = \{i_1, \ldots, i_n\} \subseteq [n(\lambda)])$ to $\mathcal{B}$ who is given an instance, $(\mathbb{MP}, g^{c_1}, \ldots, g^{c_k})$, of the k-MCDH assumption.

1) **Setup:** The challenger $\mathcal{B}$ first sets signing and verification keys for the challenge ring $(SK_{i_1} = c_{\ell+1}, VK_{i_1} = g^{c_{\ell+1}}), \ldots, (SK_{i_n} = c_k, VK_{i_n} = g^{c_k})$ (it does not know these c_i). For indices $i \notin I_{R^*}$, it chooses random $x_i \in \mathbb{Z}_p$ and sets $SK_i = x_i, VK_i = g^{x_i}$. It then generates parameters as follows:

   - Choose random integers $a_1, \ldots, a_\ell \in \mathbb{Z}_p$.
   - For $i \in [\ell]$, set $A_{i,m_i^*} = g^{c_i}$ and compute $A_{i,\bar{m}_i^*} = g^{a_i}$.

   Note that these parameters are distributed uniformly at random as in the real ring signature scheme. Then $\mathcal{B}$ sets the public parameters $\mathbb{PP} = (\mathbb{MP}, \{A_{i,\beta} | i \in [\ell], \beta \in \{0,1\}\})$. Finally, it gives $\mathbb{PP}$ and $\{VK_i\}_{i=1}^{n(\lambda)}$ to $\mathcal{A}$.

2) **Signing queries:** Conceptually, the challenger $\mathcal{B}$ can generate signatures for the adversary, because the adversary's requests and the challenge ring or message will be different in at least one bit. Specifically, when $\mathcal{A}$ makes a query to the signing oracle on input $(M, R = \{VK_1, \ldots, VK_n\}, s)$. If $R \neq R^*$, we assume that $VK_j \in R$ but $\notin R^*$, then $\mathcal{B}$ ignores the index s and signs M with SK_j in the usual way since $\mathcal{B}$ knows VK_j's singing key x_j. If $R = R^*$, then we know $M \neq M^*$ and assume that $m_\gamma \neq m_\gamma^*$, where m_γ and m_γ^* are the γ-th bit of the message M and M^*, respectively. Hence $\mathcal{B}$ can compute $\sigma = \mathbf{e}(A_{1,m_1}, \ldots, A_{\gamma-1,m_{\gamma-1}}, A_{\gamma+1,m_{\gamma+1}}, \ldots, A_{\ell,m_\ell}, VK_1, \ldots, VK_n)^{a_\gamma}$ by knowing the exponent a_γ of the parameter $A_{\gamma,\bar{m}_\gamma^*}$. Finally, it returns σ to the adversary $\mathcal{A}$.

3) **Corruption queries:** When $\mathcal{A}$ makes a query to the corruption oracle with input an index i for $i \notin I_{R^*}$, $\mathcal{B}$ gives SK_i to $\mathcal{A}$ and adds VK_i to the set C of the corrupted users.

4) **Output:** Finally, $\mathcal{A}$ outputs a forgery σ^* with respect to the challenge ring $R^* = \{VK_{i_1}, \ldots, VK_{i_n}\}$ and message M^*. Then $\mathcal{B}$ outputs σ^* as the solution to the given instance of the k-MCDH assumption. According to the setting of the public parameters and the verification keys of the challenge ring in the setup phase, and the assumption that σ^* is valid, we know that σ^* should be equal to $\mathbf{e}(A_{1,m_1^*}, \ldots, A_{\ell,m_\ell^*}, VK_1, \ldots, VK_{j-1}, VK_{j+1}, \ldots, VK_n)^{c_{\ell+j}} = g_{k-1}^{\prod_{i\in[1,k]} c_i}$, where $c_{\ell+j}$ is a certain signing key $\mathcal{A}$ uses. It implies that σ^* is a solution for the given instance to the k-MCDH problem, and thus $\mathcal{B}$ breaks the k-MCDH assumption.

It is clear that $\mathcal{B}$ succeeds whenever $\mathcal{A}$ does. □

Theorem 4. The ring signature scheme with message length ℓ and ring size n in the above is anonymous against any unbounded adversary.

Given a ring signature, we show that any ring member could possibly have created it. Consider a signature σ^* on ring $R^* = \{VK_1, \ldots, VK_n\}$ and message M^*, that has been created using key SK_{i_0}. We will show that with the same probability it could have been created using SK_{i_1} with $i_1 \neq i_0$. The proof is straight-forward.

Proof. For any tuple (M^*, R^*, i_0, i_1) which are chosen by an unbounded adversary $\mathcal{A}$, the signatures created by the member i_0 and i_1 are $\sigma_{i_0}^* = \mathbf{e}(A_{1,m_1^*}, \ldots, A_{\ell,m_\ell^*}, VK_1, \ldots, VK_{i_0-1}, VK_{i_0+1}, \ldots, VK_n)^{x_{i_0}}$ and $\sigma_{i_1}^* = \mathbf{e}(A_{1,m_1^*}, \ldots, A_{\ell,m_\ell^*}, VK_1, \ldots, VK_{i_1-1}, VK_{i_1+1}, \ldots, VK_n)^{x_{i_1}}$, respectively. However, $\sigma_{i_0}^* = \sigma_{i_1}^* = g_{k-1}^{(\prod_{i=1}^{\ell} a_{i,m_i^*})\cdot(\prod_{i=1}^{n} x_i)}$ since the signing algorithm is deterministic. Therefore, any member of a ring can compute a same signature on a given message and ring. The perfect anonymity follows easily from this observation. □

6 Conclusion

In this work, we consider the BLS signature scheme in the setting of multilinear groups. First of all, we present a proof of adaptive security for the multilinear BLS scheme based on MCDH assumption. Then, we construct a ring signature scheme that, based on the multilinear BLS scheme, has an attractive feature that for n members of a ring the signatures consist of just a single group element.

Acknowledgments

This study was supported by the National Natural Science Foundation of China under Grant 61702067, the Natural Science Foundation of Chongqing under Grants cstc2017jcyjAX0201 and cstc2019jcyj-msxmX0551, and the key project of science and technology research program of Chongqing Education Commission of China under Grants KJZD-K201803701 and KJQN201903701. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. R. Albrecht, P. Farshim, D. Hofheinz, E. Larraia, K. G. Paterson, "Multilinear maps from obfuscation," in *Proceedings of Part I of the 13th International Conference on Theory of Cryptography (TCC'16)*, vol. 9562, pp. 446-473, 2016.

[2] D. Boneh, X. Boyen, "Secure identity based encryption without random oracles," in *Annual International Cryptology Conference*, pp. 443-459, 2004.

[3] D. Boneh, X. Boyen, "Short signatures without random oracles," in *International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 3027, pp. 56-73, 2004.

[4] D. Boneh, M. Franklin, ”Identity-based encryption from the Weil pairing,” in *Annual International Cryptology Conference*, vol. 2139, pp. 213-229, 2001.

[5] A. Bender, J. Katz, R. Morselli, ”Ring signatures: Stronger definitions, and constructions without random oracles,” *Journal of Cryptolog*, vol. 22, no. 1, pp. 114-138, 2009.

[6] D. Boneh, B. Lynn, H. Shacham, ”Short signatures from the Weil pairing,” *Journal of Cryptology*, vol. 17, no. 4, pp. 297-319, 2004.

[7] A. Boldyreva, ”Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme,” in *International Workshop on Public Key Cryptography*, pp. 31-46, 2002.

[8] D. Boneh, A. Silverberg, ”Applications of multilinear forms to cryptography,” *Contemporary Mathematics*, vol. 324, pp. 71-90, 2002.

[9] J. S. Coron, T. Lepoint, M. Tibouchi, ”New multilinear maps over the integers,” in *Annual Cryptology Conference*, vol. 9215, pp. 267-286, 2015.

[10] L. Chen, J. Malone-Lee, ”Improved identity-based signcryption,” *International Workshop on Public Key Cryptography*, vol. 3386, pp. 362-379, 2005.

[11] E. S. V. Freire, D. Hofheinz, K. G. Paterson, C. Striecks, ”Programmable hash functions in the multilinear setting,” in *Annual Cryptology Conference*, vol. 8042, pp. 513-530, 2013.

[12] S. Garg, C. Gentry, S. Halevi, ”Candidate multilinear maps from ideal lattices,” *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 7881, pp. 1-17, 2013.

[13] S. Garg, C. Gentry, S. Helevi, M. Raykova, A. Sahai, B. Waters, ”Canditate indistinguishability obfuscation and functional encryption for all circuits,” *IEEE 54th Annual Symposium on Foundations of Computer Science*, pp. 40-49, 2013. ISBN: 978-0-7695-5135-7.

[14] C. Gentry, S. Gorbunov, S. Halevi, ”Graph-induced multilinear maps from lattices,” in *Theory of Cryptography Conference*, vol. 9015, pp. 498-527, 2015.

[15] Y. Hu, H. Jia, ”Cryptanalysis of GGH map,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 9665, pp. 537-565, 2016.

[16] M. S. Hwang, C. C. Lee, Y. C. Lai, ”An untraceable blind signature scheme,” *IEICE Transactions on Foundations*, vol. E86-A, no. 7, pp. 1902-1906, 2003.

[17] S. Hohenberger, A. Sahai, B. Waters, ”Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures,” in *Annual Cryptology Conference*, vol. 8024, pp. 494-512, 2013.

[18] S. Hohenberger, A. Sahai, B. Waters, ”Replacing a random oracle: full domain hash from indistinguishability obfuscation,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 8441, pp. 201-220, 2004.

[19] M. S. Hwang, C. C. Lee, Y. C. Lai, “An untraceable blind signature scheme”, *IEICE Transactions on Foundations*, vol. E86-A, no. 7, pp. 1902–1906, July 2003.

[20] C. C. Lee, M. S. Hwang, and W. P. Yang, “A new blind signature based on the discrete logarithm problem for untraceability”, *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837–841, May 2005.

[21] H. T. Lee, H. J. Seo, ”Security analysis of multilinear maps over the integers,” in *Annual Cryptology Conference*, vol. 8616, pp. 224-240, 2014.

[22] A. Langlois, D. Stehlé, R. Steinfeld, ”GGHLite: More efficient multilinear maps from ideal lattices,” *Advances in Cryptology*, vol. 8441, pp. 239-256, 2014.

[23] R. Rivest, A. Shamir, Y. Tauman, ”How to leak a secret,” in *International Conference on the Theory and Application of Cryptology and Information Security*, vol. 2248, pp. 552-565, 2001.

[24] S. SchageS, J. Schwenk, ”A CDH-based ring signature scheme with short signatures and public keys,” in *International Conference on Financial Cryptography and Data Security*, vol. 6052, pp. 129-142, 2010.

[25] B. Waters, ”Efficient identity-based encryption without random oracles,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 3494, pp. 114-127, 2005.

[26] H. Wang, D. He, J. Shen, Z. Zheng, X. Yang, M. H. Au, ”Fuzzy matching and direct revocation: A new CP-ABE scheme from multilinear maps,” *Soft Computing*, vol. 22, no. 7, pp. 2267-2274, 2017.

[27] F. Tang, H. Li, ”Ring signatures of constant size without random oracles,” in *International Conference on Information Security and Cryptology*, vol. 8957, pp. 93-108, 2015.

[28] F. Tang, H. Li, B. Liang, ”Attribute-based signatures for circuits from multilinear maps,” in *International Conference on Information Security*, vol. 8783, pp. 54-71, 2014.

[29] F. Tang, Y. Zhou, ”Policy-based signatures for predicates,” *International Journal of Network Security*, vol. 19, no. 5, pp. 811-822, 2017.

Biography

Fei Tang received his Ph.D from the Institute of Information Engineering of Chinese Academy of Sciences in 2015. He is currently an associate professor of the College of Cyberspace Security and Law, Chongqing University of Posts and Telecommunications. His research interests are public key cryptography and blockchain.

Dong Huang received his Ph.D from the Chongqing University in 2012. He is currently a professor of the Chongqing University of Science and Technology and Chongqing Vocational and Technical University of Mechatronics. His research interest is public key cryptography.