A Group Signature Scheme with Unbounded Message-Dependent Opening

Kazuma Ohara
UEC[*] and AIST[†]
Tokyo and Ibaraki, Japan
k-ohara@uec.ac.jp

Yusuke Sakai[‡]
UEC and AIST
Tokyo and Ibaraki, Japan
yusuke.sakai@uec.ac.jp

Keita Emura
NICT[§]
Tokyo, Japan
k-emura@nict.go.jp

Goichiro Hanaoka
AIST
Ibaraki, Japan
hanaoka-goichiro@aist.go.jp

ABSTRACT

Group signature with message-dependent opening (GS-MDO) is a kind of group signature in which only the signers who have created group signatures on problematic messages will be identified. In the previous GS-MDO scheme, however, the number of problematic messages is bounded owing to a limitation of the Groth-Sahai proofs. In this paper, we propose the first GS-MDO scheme with the unbounded-MDO functionality in the random oracle model. Our unbounded GS-MDO scheme is based on the short group signature scheme proposed by Boneh, Boyen, and Shacham and the Boneh-Franklin identity-based encryption scheme. To combine these building blocks and to achieve CCA-anonymity, we also construct a special type of multiple encryption. This technique yields an efficient construction compared with the previous bounded GS-MDO scheme: the signature of our scheme contains about 16 group elements (3630 bits), whereas that of the previous scheme has about 450 group elements (75820 bits).

Categories and Subject Descriptors

D.4.6 [**Management of Computing and Information Systems**]: Security and Protection—*authentication*; E.3 [**Data**]: Data Encryption—*public key cryptosystems*

General Terms

Theory, Security

Keywords

Group Signature; Unbounded Message-Dependent Opening; Random Oracle Model

1. INTRODUCTION

Group signature is a kind of digital signature, proposed by Chaum and van Heyst [9]. Each signer belongs to a group and can create a group signature, which can be verified whether it was created by a group member, without identifying the actual signer. If it is necessary to identify the signer of a group signature (e.g., a problem that may be caused by the group signature), only the authority called the "opener" can identify the corresponding signer of the group signature. However, since the opener can identify the signers without any restriction, it seems that the opener's power is unfairly strong. For example, there is a possibility that a non-problematic user will be identified.

To decentralize the power of the opener, Sakai et al. proposed a model for group signature with a new capability, which is called group signature with message-dependent opening (GS-MDO) [15], where a new authority called the "admitter" is introduced. If a group signature is found on a problematic message, the admitter issues a token corresponding to this message, and the opener can identify the signer of this group signature only when using both the given token and the opener's secret key. One of the significant functionalities of GS-MDO is that no interaction between the opener and the admitter is required. In other words, tokens can merely be published by the admitter, and once the opener receives the token, he is able to open the signatures without any further interaction with any other entity. Furthermore, once the admitter releases a token for a problematic message, the opener can open all signatures on that message.

An application of GS-MDO is an anonymous bulletin board system, which allows users to post their comments without revealing their own identity. In the case of disputes, which may be caused by posting inappropriate comments (e.g., leaking some personal information of others, a crime

[*] UEC: University of Electro-Communications
[†] AIST: National Institute of Advanced Industrial Science and Technology
[‡] The second author is supported by a JSPS Fellowship for Young Scientists.
[§] NICT: National Institute of Information and Communications Technology

ASIA CCS'13, May 8–10, 2013, Hangzhou, China.
Copyright 2013 ACM 978-1-4503-1767-2/13/05 ...$15.00.

notice, and so on), GS-MDO comes into effect: the admitter indicates messages that should be prohibited, and the opener can identify only the writers who have posted inappropriate comments on the board. Another application of GS-MDO is an anonymous auction. To bid anonymously, each bidder produces a group signature on his bidding price. After checking the validity of the group signatures, the admitter issues a token only to open the signatures on the highest bid, thereby determining the winner(s). One benefit of this system (compared with applying the conventional group signature) is that no loser(s) of this auction can be identified by the opener.

Sakai et al. also presented a generic construction of GS-MDO from a tag-based key encapsulation mechanism (tag-based KEM), digital signature, identity-based KEM (IB-KEM), and non-interactive zero knowledge (NIZK) proof. Moreover, they gave an instantiation of the generic construction using Shacham's decision-linear (DLIN) Cramer-Shoup encryption scheme (actually a tag-based KEM variant thereof), the Abe-Haralambiev-Ohkubo structure-preserving signature [2, 1], k-resilient a DLIN variant of the Heng-Kurosawa IB-KEM [14]), and the Groth-Sahai proof system [13], which is used as an instantiation of the NIZK proof in the standard model.

One of the weaknesses of the specific construction by Sakai et al. is that it only achieves "k-bounded" security, in the sense that the number of tokens the admitter can issue must be determined when the scheme is set up. This stems from the (in)compatibility of the known identity-based encryption (IBE) schemes and the Groth-Sahai proof system. As the implication result by Sakai et al. suggests, using IBE as a building block to construct a GS-MDO scheme is indispensable. Recall a widely used approach for constructing group signature, in which each group member is assigned a digital signature and generate group signature by encrypting that digital signature and prove the validity of encrypted signature by using an NIZK proof. It is also crucial to use an non-interactive *zero-knowledge* proof system to ensure "well-formedness" of the encrypted certificate, which serves as a group signature. Unfortunately, the Groth-Sahai proof system provides the zero-knowledge property only for a restricted type of theorem. Basically, when a theorem involves equations between elements of the target group $\mathbb{G}_T$, the zero-knowledge property is not guaranteed, which is why the instantiation by Sakai et al. used a k-resilient scheme to instantiate IB-KEM instead of an ordinary IBE scheme.

Such a k-bounded limitation seems to be unavoidable. All known IBE schemes (of the discrete-log type) depend on pairing-type assumptions, and more particularly contain target-group elements in their ciphertexts. Hence the "well-formedness" of an IBE ciphertext is described as equations between target-group elements, for which the Groth-Sahai proof system does not provide the zero-knowledge property. Considering the fact that the Groth-Sahai proof system is currently the only choice for an efficient instantiation of a zero-knowledge proof system, we have no other way of providing a proof of this type.

Of course if we want an unbounded GS-MDO scheme, it is easily possible by applying general NIZK techniques (as in the BMW/BSZ constructions [4, 5]). However, it might be hard to achieve an efficient instantiation of the known NIZK proofs for general NP-languages (The same holds even in the random oracle model).

From the above considerations, it is difficult to construct efficient unbounded GS-MDO schemes in the standard model. Therefore, applying random oracles seems to be a reasonable solution.

Our Contribution.

In this paper, we propose the first unbounded GS-MDO scheme in the random oracle model. The proposed scheme is based on the Boneh-Boyen-Shacham (BBS) group signature [7], which is one of the most efficient group signature schemes in the random oracle model. The opening procedure is implemented by linear encryption, and a user's certificate is implemented by the Boneh-Boyen short signature [6]. The functionality of MDO is realized by adopting the Boneh-Franklin (BF) IBE [8]. In order to combine the short group signature and the BF IBE, we replace the linear encryption with a certain type of 2-out-of-2 multiple encryption.

Note that the BBS scheme satisfies only CPA-anonymity, the security game of which does not allow the adversary to access the opening oracle. We make a further improvement to the above approach to achieve CCA-anonymity. This improvement is carried out by changing the "linear" part of the multiple encryption to a kind of double encryption similar to the Naor-Yung construction and adding a validity check component that ensures "well-formedness" of the ciphertext, which could be reminiscent of the Cramer-Shoup encryption scheme [11, 12].

For efficiency reasons, to realize the proof, we do not follow the construction of the Cramer-Shoup scheme directly, but instead use the Fiat-Shamir heuristics. This strategy yields a more efficient construction compared with that obtained when directly using another DLIN-based CCA-secure public-key encryption (PKE) is directly used, e.g., Shacham's DLIN-variant of the Cramer-Shoup PKE scheme [16].

The proposed scheme simultaneously achieves a higher degree of efficiency and security than the previous scheme by Sakai et al. The signature contains 16 group elements (3630 bits for 80-bit security), whereas that of the previous scheme contains about 450 elements (about 76000 bits for the same security level). Furthermore, the proposed scheme allows the admitter to issue an *unbounded* number of tokens, which is not achieved by the previous efficient construction. See Section 4 for a detailed comparison.

2. PRELIMINARIES

In this section, we present a formal model of the GS-MDO proposed by Sakai et al. in [15], and computational assumptions for our proposed scheme.

2.1 Group Signature with Message-dependent Opening

GS-MDO is an extension of group signature, which allows members of the group to sign a message anonymously. In addition, as described in the introduction, there are two authorities in GS-MDO, the opener and the admitter. The admitter is able to issue a token that is specific to a message. The opener is able to identify the signer of a signature on a message for which a token from the admitter is available.

A GS-MDO scheme consists of five probabilistic polynomial-time algorithms $(\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Td}, \mathsf{Open})$. GKg takes as inputs $(1^\lambda, 1^n)$ where λ is a security parameter and n is the number of group members, and outputs $(gpk, ok, ak,$

$(gsk_i)_{1 \le i \le n})$ where gpk is a group public key, ok is an opening key for the opener, ak is the message specification key for the admitter, and gsk_i is a group signing key for each group member i. GSig takes as inputs (gpk, i, gsk_i, M) where M is a message, and outputs a group signature σ. GVf takes as inputs (gpk, M, σ) and outputs $\top$ or $\bot$. Td takes as inputs (gpk, ak, M) and outputs the token t_M for M. Open takes as inputs $(gpk, ok, M, \sigma, t_M)$ and outputs $i \in \{1, 2, \ldots, n\}$ or $\bot$.

Note that in the case where the number of tokens issued by the admitter is bounded by k (like the Sakai et al.'s scheme [15]), the group key generation algorithm GKg takes as input $(1^\lambda, 1^n, 1^k)$.

2.2 The Security Requirements of GS-MDO

Sakai et al. defined the following three requirements for a GS-MDO (the definition of these properties is based on Bellare, Micciancio, and Warinschi's security model [4]).

Opener Anonymity.

The opener should be unable to identify the signer of any group signature without cooperation with the admitter, even if some group members are corrupted. This requirement is formalized by the following game. Note that, in order to model anonymity against the opener, we give the opening key to the adversary in this game.

Definition 1. *We say that a GS-MDO scheme* $\Pi = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Td}, \mathsf{Open})$ *has opener anonymity if for all probabilistic polynomial-time adversaries* $\mathcal{A}$*, the success probability of* $\mathcal{A}$ *in the following game between a challenger is negligible in the security parameter* λ*.*

Setup. *The challenger runs* $\mathsf{GKg}(1^\lambda, 1^n)$ *and obtain* $(gpk, ok, ak, (gsk_i)_{1 \le i \le n})$*. Then the challenger sends* $(gpk, ok, (gsk_i)_{1 \le i \le n})$ *to* $\mathcal{A}$*.*

Token Query I. $\mathcal{A}$ *is allowed to interact with a token oracle. For a token query for* M*, the challenger runs* $\mathsf{Td}(gpk, ak, M)$ *to obtain* t_M *and return* t_M *to* $\mathcal{A}$*.*

Challenge. *At some point* $\mathcal{A}$ *requests a challenge for* $i_0, i_1 \in \{1, \ldots, n\}$ *and a message* M^**. The challenger chooses a random bit* b*, and return* $\mathsf{GSig}(gpk, gsk_{i_b}, M^*)$*. In this phase* $\mathcal{A}$ *is forbidden to submit* M^* *which is already queried in Token Query I.*

Token Query II. $\mathcal{A}$ *continues to query tokens. In this phase* $\mathcal{A}$ *is forbidden to query* M^* *which is submitted in challenge phase.*

Guess. $\mathcal{A}$ *outputs a bit* b'*. The advantage of* $\mathcal{A}$ *is defined by the absolute difference between the probability that* b' *is equal to* b *and* $1/2$*.*

Admitter Anonymity.

The admitter should be unable to identify the signer of any group signature without cooperation with the opener, even if some group members are corrupted. This requirement is formalized by the following game. Note that, in order to model anonymity against the admitter, we give the message specification key to the adversary in this game.

Definition 2. *We say that a GS-MDO scheme* $\Pi = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Td}, \mathsf{Open})$ *has admitter anonymity if for all probabilistic polynomial-time adversaries* $\mathcal{A}$*, the success probability of* $\mathcal{A}$ *in the following game between a challenger is negligible in the security parameter* λ*.*

Setup. *The challenger runs* $\mathsf{GKg}(1^\lambda, 1^n)$ *and obtain* $(gpk, ok, ak, (gsk_i)_{1 \le i \le n})$*. Then the challenger sends* $(gpk, ak, (gsk_i)_{1 \le i \le n})$ *to* $\mathcal{A}$*.*

Open Query I. $\mathcal{A}$ *is allowed to interact with an open oracle. For an open query for* (M, σ)*, the challenger runs* $\mathsf{Td}(gpk, ak, M)$ *to obtain* t_M *and return* $\mathsf{Open}(gpk, ok, M, \sigma, t_M)$ *to* $\mathcal{A}$*.*

Challenge. *At some point* $\mathcal{A}$ *requests a challenge for* $i_0, i_1 \in \{1, \ldots, n\}$ *and a message* M^**. The challenger chooses a random bit* b*, and return* $\mathsf{GSig}(gpk, gsk_{i_b}, M^*)$*.*

Open Query II. $\mathcal{A}$ *continues to query tokens. In this phase* $\mathcal{A}$ *is forbidden to query* σ^* *which is submitted in challenge phase.*

Guess. $\mathcal{A}$ *outputs a bit* b'*. The advantage of* $\mathcal{A}$ *is defined by the absolute difference between the probability that* b' *is equal to* b *and* $1/2$*.*

Traceability.

Even the opener and the admitter collude, they should not be able to produce any forged signature or untraceable signature. This requirement is formalized by the following definition.

Definition 3. *We say that a GS-MDO scheme* $\Pi = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf}, \mathsf{Td}, \mathsf{Open})$ *has traceability if for all probabilistic polynomial-time adversaries* $\mathcal{A}$*, the success probability of* $\mathcal{A}$ *in the following game between a challenger is negligible in the security parameter* λ*.*

Setup. *The challenger runs* $\mathsf{GKg}(1^\lambda, 1^n)$ *and obtain* $(gpk, ok, ak, (gsk_i)_{1 \le i \le n})$*. Then the challenger sends* $(gpk, ok, ak, (gsk_i)_{1 \le i \le n})$ *to* $\mathcal{A}$*.*

Private Key Query. $\mathcal{A}$ *is allowed to interact with a private key oracle. For a private key query for* i*, the challenger returns* gsk_i *to* $\mathcal{A}$*.*

Signing Query. $\mathcal{A}$ *is allowed to interact with signing oracle. For a signing query for* (i, M)*, the challenger returns* $\mathsf{GSig}(gpk, i, gsk_i, M)$ *to* $\mathcal{A}$*.*

Forge. $\mathcal{A}$ *outputs a message-signature pair* (M^*, σ^*)*. The adversary wins the game if* $\mathsf{GVf}(gpk, M^*, \sigma^*) = \top$ *and one of the following conditions (a) and (b) holds: (a)* $\mathsf{Open}(gpk, ok, M^*, \sigma^*, \mathsf{Td}(gpk, ak, M^*)) = \bot$*, or (b)* $\mathsf{Open}(gpk, ok, M^*, \sigma^*, \mathsf{Td}(gpk, ak, M^*)) = i^* \neq \bot$ *and both the signing key of the user* i^* *and a signature on* (i^*, M^*) *are never queried to the above oracles. The advantage of* $\mathcal{A}$ *is defined by the probability that* $\mathcal{A}$ *wins the game.*

2.3 The Computational Assumptions

Let $\mathcal{G}$ be a probabilistic polynomial-time algorithm that takes a security parameter 1^λ as input and generates a parameter $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ of *bilinear groups*, where p is a λ-bit prime, $\mathbb{G}$ and $\mathbb{G}_T$ are groups of order p, e is a bilinear map from $\mathbb{G} \times \mathbb{G}$ to $\mathbb{G}_T$, and g is a generator of $\mathbb{G}$. We then describe several computational assumptions on which the proposed scheme is based.

The q-strong Diffie-Hellman Assumption.

Let $(p, \mathbb{G}, \mathbb{G}_T, e, g) \xleftarrow{\$} \mathcal{G}(1^\lambda)$, $\gamma \xleftarrow{\$} \mathbb{Z}$ and $A_i \leftarrow g^{\gamma^i}$ for $i = 0, \ldots, q$. The q-strong Diffie-Hellman problem in $\mathbb{G}$ is stated as follows: given $(g, (A_i)_{0 \le i \le q})$, output $(c, g^{1/(\gamma+c)})$ where $c \in \mathbb{Z}_p^*$. The advantage of an algorithm $\mathcal{A}$ against the q-strong Diffie-Hellman problem is defined as

$$\mathrm{Adv}_{\mathcal{A}}^{q\text{-SDH}}(\lambda) = \Pr[\mathcal{A}(g, (A_i)_{0 \le i \le q}) = (c, g^{1/(\gamma+c)}) \wedge c \in \mathbb{Z}_p].$$

We say that the q-strong Diffie-Hellman assumption holds if $\mathrm{Adv}_{\mathcal{A}}^{q\text{-SDH}}(\lambda)$ is negligible in λ for any probabilistic polynomial-time algorithm $\mathcal{A}$.

The Decision Linear Assumption.

Let u, v, $h \xleftarrow{\$} \mathbb{G}$, α, β, $r \xleftarrow{\$} \mathbb{Z}_p$ and $g_1 \leftarrow u^\alpha, g_2 \leftarrow v^\beta$. The decision linear problem in $\mathbb{G}$ is stated as follows: given $(u, v, h, u^\alpha, v^\beta, z)$, output 1 if $z = h^{\alpha+\beta}$, otherwise 0 if $z = h^r$. The advantage of an algorithm $\mathcal{A}$ against the decision linear problem is defined as

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DLIN}}(\lambda) = |&\Pr[\mathcal{A}(u, v, h, u^\alpha, v^\beta, z) = 1 \mid z = h^{\alpha+\beta}] \\ &- \Pr[\mathcal{A}(u, v, h, u^\alpha, v^\beta, z) = 1 \mid z = h^r]|.\end{aligned}$$

We say that the decision linear assumption holds if $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DLIN}}(\lambda)$ is negligible in λ for any probabilistic polynomial-time algorithm $\mathcal{A}$.

The Decision Bilinear Diffie-Hellman Assumption.

Let $(p, \mathbb{G}, \mathbb{G}_T, e, g) \xleftarrow{\$} \mathcal{G}(1^\lambda)$ and a, b, c, $r \xleftarrow{\$} \mathbb{Z}_p$. The decision linear problem in $(\mathbb{G}, \mathbb{G}_T)$ is stated as follows: given (g, g^a, g^b, g^c, z), output 1 if $z = e(g, g)^{abc}$, otherwise 0 if $z = e(g, g)^r$. The Advantage of an algorithm $\mathcal{A}$ against the decision bilinear Diffie-Hellman problem is defined as

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DBDH}}(\lambda) = |&\Pr[\mathcal{A}(g, g^a, g^b, g^c, z) = 1 \mid z = e(g, g)^{abc}] \\ &- \Pr[\mathcal{A}(g, g^a, g^b, g^c, z) = 1 \mid z = e(g, g)^r]|.\end{aligned}$$

We say that the decision bilinear Diffie-Hellman assumption holds if $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DBDH}}(\lambda)$ is negligible in λ for any probabilistic polynomial-time algorithm $\mathcal{A}$.

3. THE PROPOSED SCHEME

In this section we describe the proposed scheme and its security.

Underlying Idea.

Our proposed scheme is based on the BBS group signature, in which each group member is provided with a (Boneh-Boyen) signature [6], to certify the membership of the owner. The group signature consists of two parts: the first part is the linear encryption of the certificate, while the second part is the "signature of knowledge" of the encrypted certificate. The decryption key for the linear encryption, which is held by the opener, is used to revoke the anonymity of any group signature.

We extend the BBS group signature scheme by replacing the linear encryption with a certain type of 2-out-of-2 multiple encryption of ordinary PKE and IBE. The multiple encryption is designed to ensure that only when *both* the PKE and the IBE are decrypted, can the entire ciphertext be decrypted. Such multiple-encryption can be accomplished using a simple 2-out-of-2 secret sharing.

This feature enables us to realize the MDO functionality. If the opener only possesses the decryption key of the PKE and the admitter holds the master secret of the IBE, the decryption key of the IBE (under a certain ID) can serve as the message-dependent token. The multiple encryption ensures that the opener cannot identify the originator of a signature even if the opener has the decryption key of the PKE scheme. Furthermore, if the opener receives the token, which is merely a derived decryption key of the IBE, the opener, using both his own decryption key and the message-specific decryption key received from the admitter, is able to decrypt the ciphertext included in the group signature, thereby identifying the originator of the signature.

Our Construction.

$\mathsf{GKg}(1^\lambda, 1^n)$**.** The proposed scheme uses two hash functions $H_1\colon \{0,1\}^* \to \mathbb{G}$ and $H_2\colon \{0,1\}^* \to \mathbb{Z}_p$. They are modeled as random oracles in the security analysis. Given a security parameter 1^λ, the algorithm runs $\mathcal{G}(1^\lambda)$ to generate a parameter of bilinear group (p, $\mathbb{G}, \mathbb{G}_T, e, g$). Then the algorithm selects a random element u, v, $h \xleftarrow{\$} \mathbb{G} \setminus \{1\}$ and random integers ξ_1, ξ_2, ξ_3, ζ, $\gamma \xleftarrow{\$} \mathbb{Z}_p$, sets $g_1 \leftarrow u^{\xi_1} h^{\xi_3}$, $g_2 \leftarrow v^{\xi_2} h^{\xi_3}$, $y \leftarrow g^\zeta$, and $w \leftarrow g^\gamma$. The algorithm then select $x_i \xleftarrow{\$} \mathbb{Z}_p$ and sets $A_i \leftarrow g^{1/(\gamma+x_i)}$ for each user i $(1 \le i \le n)$. Finally the algorithm outputs the group public key $gpk \leftarrow (p, \mathbb{G}, \mathbb{G}_T, e, g, u, v, h, g_1, g_2, y, w, H_1, H_2)$, the message-specification key $ak \leftarrow \zeta$, the opening key $ok \leftarrow (\xi_1, \xi_2, \xi_3, (e(A_i, g))_{1 \le i \le n})$, and the users' signing keys $(gsk_i)_{1 \le i \le n} \leftarrow (A_i, x_i)_{1 \le i \le n}$.

$\mathsf{GSig}(gpk, i, gsk_i, M)$**.** Given an input (gpk, i, gsk_i, M), the algorithm generates a group signature as follows: choose random α, β, ρ, $\eta \xleftarrow{\$} \mathbb{Z}_p$, computes

$$(T_1, T_2, T_3, T_4) \leftarrow (u^\alpha, v^\beta, h^{\alpha+\beta}, g_1^\alpha g_2^\beta A_i g^\eta)$$

and

$$(T_5, T_6) \leftarrow (g^\rho, e(y, H_1(M))^\rho e(g, g)^{-\eta}).$$

Then choose random r_α, r_β, r_ρ, r_η, r_x, $r_{\alpha x}$, $r_{\beta x}$, $r_{\rho x}$, $r_{\eta x} \xleftarrow{\$} \mathbb{Z}_p$, compute

$$\begin{aligned}
R_1 &\leftarrow u^{r_\alpha}, \\
R_2 &\leftarrow v^{r_\beta}, \\
R_3 &\leftarrow h^{r_\alpha + r_\beta}, \\
R_4 &\leftarrow e(T_4, g)^{r_x} e(g_1, w)^{-r_\alpha} e(g_1, g)^{-r_{\alpha x}} \\
&\qquad \cdot e(g_2, w)^{-r_\beta} e(g_2, g)^{-r_{\beta x}} e(g, w)^{-r_\eta} e(g, g)^{-r_{\eta x}}, \\
R_5 &\leftarrow g^{r_\rho}, \\
R_6 &\leftarrow e(y, H_1(M))^{r_\rho} e(g, g)^{-r_\eta}, \\
R_7 &\leftarrow T_1^{r_x} u^{-r_{\alpha x}}, \\
R_8 &\leftarrow T_2^{r_x} v^{-r_{\beta x}}, \\
R_9 &\leftarrow T_5^{r_x} g^{-r_{\rho x}}, \\
R_{10} &\leftarrow T_6^{r_x} e(y, H_1(M))^{-r_{\rho x}} e(g, g)^{r_{\eta x}},
\end{aligned}$$

compute $c \leftarrow H_2(M, T_1, \ldots, T_6, R_1, \ldots, R_{10})$, and further computes

$$\begin{aligned}
s_\alpha &\leftarrow r_\alpha + c\alpha,\\
s_\beta &\leftarrow r_\beta + c\beta,\\
s_\rho &\leftarrow r_\rho + c\rho,\\
s_\eta &\leftarrow r_\eta + c\eta,\\
s_x &\leftarrow r_x + cx_i,\\
s_{\alpha x} &\leftarrow r_{\alpha x} + c\alpha x_i,\\
s_{\beta x} &\leftarrow r_{\beta x} + c\beta x_i,\\
s_{\rho x} &\leftarrow r_{\rho x} + c\rho x_i,\\
s_{\eta x} &\leftarrow r_{\eta x} + c\eta x_i.
\end{aligned}$$

Finally let σ be

$$(T_1, \ldots, T_6, c, s_\alpha, s_\beta, s_\rho, s_\eta, s_x, s_{\alpha x}, s_{\beta x}, s_{\rho x}, s_{\eta x})$$

and output σ as the group signature.

Remark 1. The above R_1, ... ,R_{10}, c, s_α, s_β, s_ρ, s_η, s_x, $s_{\alpha x}$, $s_{\beta x}$, $s_{\rho x}$, and $s_{\eta x}$ come from a Schnorr-type protocol that proves knowledge α, β, ρ, η, and x satisfying the equations

$$\begin{aligned}
T_1 &= u^\alpha,\\
T_2 &= v^\beta,\\
T_3 &= h^{\alpha+\beta},\\
e(g, g) &= e(T_4 {g_1}^{-\alpha} {g_2}^{-\beta} g^{-\eta}, w g^x),\\
T_5 &= g^\rho,\\
T_6 &= e(y, H_1(M))^\rho e(g, g)^{-\eta}.
\end{aligned}$$

More concretely, introducing four intermediate variables δ_1, δ_2, δ_3, and δ_4 (which are intended to be $\delta_1 = \alpha x$, $\delta_2 = \beta x$, $\delta_3 = \rho x$, and $\delta_4 = \eta x$), the underlying protocol proves knowledge α, β, ρ, η, x, δ_1, δ_2, δ_3, and δ_4 satisfying the equations

$$\begin{aligned}
T_1 &= u^\alpha,\\
T_2 &= v^\beta,\\
T_3 &= h^{\alpha+\beta},\\
e(g, g)/e(T_4, w) &= e(T_4, g)^x e(g_1, w)^{-\alpha} e(g_1, g)^{-\delta_1}\\
&\quad \cdot e(g_2, w)^{-\beta} e(g_2, g)^{-\delta_2}\\
&\quad \cdot e(g, w)^{-\eta} e(g, g)^{-\delta_4},\\
T_5 &= g^\rho,\\
T_6 &= e(y, H_1(M))^\rho e(g, g)^{-\eta},\\
1 &= T_1^x u^{-\delta_1},\\
1 &= T_2^x v^{-\delta_2},\\
1 &= T_5^x g^{-\delta_3},\\
1 &= T_6^x e(y, H_1(M))^{-\delta_3} e(g, g)^{\delta_4}.
\end{aligned}$$

$\mathsf{GVf}(gpk, M, \sigma)$**.** Given gpk, M and σ, the algorithm verifies the signature as follows. The algorithm computes R'_1, R'_2, R'_3, R'_4, R'_5, R'_6, R'_7, R'_8, R'_9, and R'_{10} by letting

$$\begin{aligned}
R'_1 &\leftarrow u^{s_\alpha} T_1^{-c},\\
R'_2 &\leftarrow v^{s_\beta} T_2^{-c},\\
R'_3 &\leftarrow h^{s_\alpha + s_\beta} T_3^{-c},\\
R'_4 &\leftarrow e(T_4, g)^{s_x} e(g_1, w)^{-s_\alpha} e(g_1, g)^{-s_{\alpha x}}\\
&\quad \cdot e(g_2, w)^{-s_\beta} e(g_2, g)^{-s_{\beta x}}\\
&\quad \cdot e(g, w)^{-s_\eta} e(g, g)^{-s_{\eta x}}\\
&\quad \cdot (e(g, g)/e(T_4, w))^{-c},\\
R'_5 &\leftarrow g^{s_\rho} T_5^{-c},\\
R'_6 &\leftarrow e(y, H_1(M))^{s_\rho} e(g, g)^{-s_\eta} T_6^{-c},\\
R'_7 &\leftarrow T_1^{s_x} u^{-s_{\alpha x}},\\
R'_8 &\leftarrow T_2^{s_x} v^{-s_{\beta x}},\\
R'_9 &\leftarrow T_5^{s_x} g^{-s_{\rho x}},\\
R'_{10} &\leftarrow T_6^{s_x} e(y, H_1(M))^{-s_{\rho x}} e(g, g)^{s_{\eta x}}.
\end{aligned}$$

Then the algorithm verifies whether the equation

$$c = H_2(M, T_1, \ldots, T_6, R'_1, \ldots, R'_{10})$$

holds. If the equation holds, the algorithm outputs $\top$, otherwise outputs $\bot$.

$\mathsf{Td}(gpk, ak, M)$**.** Given gpk, $ak = \zeta$, and M, the algorithm generates a token t_M as $t_M \leftarrow H_1(M)^\zeta$ and outputs t_M.

$\mathsf{Open}(gpk, ok, M, \sigma, t_M)$**.** Given gpk, ok, M, σ, and t_m, the algorithm first verifies the signature using the algorithm GVf. If the signature is invalid, the algorithm outputs $\bot$. If the signature is valid, the algorithm then find i which satisfies the equation

$$e\left(\frac{T_4}{T_1^{\xi_1} T_2^{\xi_2} T_3^{\xi_3}}, g\right) \cdot \frac{T_6}{e(T_5, t_M)} = e(A_i, g).$$

When such i exists, the algorithm outputs i, otherwise outputs $\bot$.

The security of our proposed scheme is proved as follows.

THEOREM 1. *If the decision bilinear Diffie-Hellman assumption holds, the proposed construction has opener anonymity in the random oracle model.*

THEOREM 2. *If the decision linear assumption holds, the proposed construction has admitter anonymity in the random oracle model.*

THEOREM 3. *If the q-strong Diffie-Hellman assumption holds, the proposed construction has traceability in the random oracle model.*

For the details of the proof of these theorems, see the full version of this paper.

4. COMPARISON

Finally, we present a brief comparison of the proposed construction and some related constructions in Table 1. Concretely we compare the proposed scheme with the instantiation presented by Sakai et al. [15] and the BBS group signature scheme, on which the proposed construction is based.

As shown in Table 1, compared with the scheme by Sakai et al., the proposed scheme realizes improvements in two aspects: the first is removing the a priori upper bound on the number of tokens the admitter can issue, while the second is substantially reducing the signature size. For 80-bit security,

Table 1: Performance comparison, where DLIN, DBDH, q-SDH, and SFP respectively stand for the decision linear assumption, the decision bilinear Diffie-Hellman assumption, the q-strong Diffie-Hellman assumption, and the simultaneous flexible pairing assumption [3]. The bit size for the estimation is given in [10].

	Signature length	Message-dependent	Assumption	w/o RO	Anonymity
	# of [$\mathbb{G}$,$\mathbb{Z}_p$,$\mathbb{G}_T$]-elements	Opening			
Proposed	[5,10,1] (3630 bits)	unbounded	DLIN, DBDH, q-SDH	-	CCA
Sakai et al. [15]	[446,0,0] (75820 bits)[1]	k-bounded	DLIN, SFP	✓	CCA
BBS [7]	[3,6,0] (1530 bits)	-	DLIN, q-SDH	-	CPA

[1] This scheme needs an additional (strongly unforgeable) one-time signature scheme, and therefore the total number of group elements becomes slightly larger, and additional complexity assumptions may be required.

the signature length of our scheme is 3630 bits, while those of the schemes by Sakai et al. [15] and Boneh et al. [7] are 75820 bits and 1530 bits (the bit size for the estimation is given in [10]), respectively. These two improvements are achieved at the cost of using random oracles, as indicated in the "w/o RO" column in the table.

Compared with the BBS scheme, we believe that the proposed scheme achieves MDO at a relatively reasonable cost given the increase in signature size. As shown in the table, the signature size of the proposed scheme is almost twice as long as that of the BBS scheme, which we believe to be reasonable. We also note that the proposed scheme achieves CCA-anonymity, which guarantees a remarkably higher level of security than the CPA-anonymity achieved by the BBS scheme.

5. ACKNOWLEDGMENTS

The authors are grateful to Hovav Shacham for pointing out the possibility of using random oracles to achieve unbounded security. The authors would like to thank Shin-Akarui-Angou-Benkyou-Kai for the valuable discussions and comments.

6. REFERENCES

[1] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, Heidelberg, 2010.

[2] M. Abe, K. Haralambiev, and M. Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. `http://eprint.iacr.org/`.

[3] M. Abe, K. Haralambiev, and M. Ohkubo. Group to group commitments do not shrink. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 301–317. Springer, Heidelberg, 2012.

[4] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In E. Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 644–644. Springer, Heidelberg, 2003.

[5] M. Bellare, H. Shi, and C. Zhang. Foundations of group signatures: The case of dynamic groups. In A. Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 136–153. Springer, Heidelberg, 2005.

[6] D. Boneh and X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *J. Cryptol.*, 21:149–177, 2008.

[7] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 227–242. Springer, Heidelberg, 2004.

[8] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[9] D. Chaum and E. van Heyst. Group signatures. In D. W. Davies, editor, *EUROCRYPT '91*, volume 547 of *LNCS*, pages 257–265. Springer, Heidelberg, 1991.

[10] J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee. Shorter IBE and signatures via asymmetric pairings. Cryptology ePrint Archive, Report 2012/224, 2012. `http://eprint.iacr.org/`.

[11] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *CRYPTO 1998*, volume 1462 of *LNCS*, pages 13–25. Springer, Heidelberg, 1998.

[12] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003.

[13] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, 2008.

[14] S.-H. Heng and K. Kurosawa. k-resilient identity-based encryption in the standard model. In T. Okamoto, editor, *CT-RSA 2004*, volume 2964 of *LNCS*, pages 67–80. Springer, Heidelberg, 2004.

[15] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, T. Matsuda, and K. Omote. Group signatures with message-dependent opening. In *Pairing 2012*, pages 270–294, 2012.

[16] H. Shacham. A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. `http://eprint.iacr.org/`.