A Short Anonymously Revocable Group Signature Scheme from Decision Linear Assumption

Toru Nakanishi
Dept. of Communication Network Engineering
Okayama University
Okayama, 700-8530 Japan
nakanisi@cne.okayama-u.ac.jp

Nobuo Funabiki
Dept. of Communication Network Engineering
Okayama University
Okayama, 700-8530 Japan
funabiki@cne.okayama-u.ac.jp

ABSTRACT

In group signature schemes, a signature is anonymous for a verifier, while only a designated Privacy Manager (PM) can identify the signer. This identification is used for tracing a dishonest anonymous signer in case of an illegal act using the signature. However, PM can violate signers' anonymity. Recently, Brickell and Li propose a novel countermeasure for the anonymous dishonest signer without PM in the setting of the direct anonymous attestation. Here, we call the generalized group signature version *anonymously revocable group signature scheme*. In this scheme, after an illegal act using a group signature was found, the membership of the dishonest signer can be anonymously revoked for excluding the signer without the help of any PM. However, since the Brickell-Li scheme is based on the RSA assumption and the DDH assumption, the signature is long. In this paper, we propose a short anonymously revocable group signature scheme from supersingular curves, where we adopt the decision linear (DLIN) assumption. Compared to the simple adoption of the Brickell-Li DDH-based revoking approach to supersingular curves, the length of our signature is reduced to about from 30% to 60%.

Categories and Subject Descriptors

D.4.6 [**Software**]: Security and Protection—*Authentication*

General Terms

Security, Algorithms

Keywords

Group signature, Anonymity, Revocation

1. INTRODUCTION

Group signature scheme [5] allows a group member to anonymously sign a message on behalf of a group, where the membership of the group is controlled by a group manager (GM). The simple but important application is an anonymous authentication between anonymous users (group members) and the servers (GM or verifiers). Consider a network service available for only valid users. In advance, a user registers with GM to join the group. In the authentication for the use of the service, the user sends his group signature to a server in order to convince the server that the user is valid for the service as a group member. The anonymity of the group signature can protect users' privacy from servers. However, in case of complete anonymity, dishonest users may make abuse of the services, since the users are untraceable. For example, in an anonymous BBS (Bulletin Board System), Weblog services, or SNS (Social Network Services), an anonymous user may submit libelous articles, while it is difficult to trace the user. For solving this problem, the group signature schemes have introduced a designated party who can identify the signer from the group signature. We call this party a privacy manager (PM) here. Then, after a user made abuse in an anonymous service, the user can be traced by PM via the group signature.

However, PM can violate signers' anonymity, whereas the signers are unaware of the violation. Thus, PM can collect users' privacy secretly, and PM may be a *big brother*.

We can find a countermeasure against the anonymous abuse without introducing PM, in a direct anonymous attestation (DAA) scheme [4]. The DAA scheme is a variant of group signature scheme without PM, which is designed for the remote authentication of a Trusted Platform Module (TPM) while keeping user's privacy. The TPM can anonymously prove to a remote server that it is a valid module. This scheme has a novel anonymously revoking method; The membership of a dishonest user can be anonymously revoked and the user is excluded without the help of any PM. Namely, the dishonest user remains anonymous after the illegal acts, but the signatures that the dishonest user issues after the revocation, can be detected. In this method, when GM and/or verifiers want to exclude a dishonest user who issued a signature $\hat{\sigma}$, they add a tag included in $\hat{\sigma}$ into $\boldsymbol{RL}$. Given $\boldsymbol{RL}$, another honest signer computes his signature σ ensuring that the signer of σ is different from the signer of $\hat{\sigma}$ in $\boldsymbol{RL}$. Thus, the verifiers can check whether a signer is the dishonest signer or not, and can revoke the anonymous dishonest signer. Except for this check, the signature reveals no information about the signer to all verifiers and even GM, and thus there is no big brother. In addition, even if a user is illegally revoked via $\boldsymbol{RL}$ generated by dishonest verifiers, the user can be aware of the revocation by checking the tags in $\boldsymbol{RL}$. To emphasize the anonymous revocation in the setting of general group signatures instead of DAA, we call such

ASIACCS '08, March 18-20, Tokyo, Japan

a scheme *anonymously revocable group signature scheme*.

The disadvantage of the anonymously revocable group signature scheme is that the identity of the dishonest signer is untraceable. Thus, it is not suitable for applications where illegal acts cause very serious problems. On the other hand, it can be suitable for the situation where illegal acts make other users unpleasant, or the problems caused by dishonest users can be compensated by insurance. An example of the applications is the anonymous authentication in an anonymous BBS, Weblog, or SNS. By the scheme, the dishonest user who sent a libelous article is anonymously excluded and the following articles can be stopped by the server (i.e, verifier), while the anonymity of other users remains.

The previous scheme [4] is based on the strong RSA assumption and the DDH assumption. However, since we need the RSA modulus with the long key size (1024 bits or more), signatures becomes long.

In this paper, we explore an anonymously revocable group signature scheme from bilinear maps, since pairing-friendly elliptic curves make signatures short. Let $e : \mathcal{G} \times \mathcal{H} \to \mathcal{T}$ be a bilinear map (i.e., pairing) on groups $\mathcal{G}, \mathcal{H}, \mathcal{T}$ with the same prime order. Then, since we can have the DDH assumption on $\mathcal{T}$, we can simply adapt the DDH-based anonymously revoking method of [4] to $\mathcal{T}$. However, elements of $\mathcal{T}$ must be as long as the RSA modulus, and thus we cannot expect short signatures. On the other hand, we can find the XDH (eXternal DH) assumption [3], where the DDH assumption holds on $\mathcal{G}$ with short elements. It can be expected that this assumption is true in a subset of non-supersingular curves, but this does not hold for supersingular curves (i.e., $\mathcal{G} = \mathcal{H}$). In [6], we can find an alternative method for short signatures, where, in addition to bilinear groups $\mathcal{G}, \mathcal{H}, \mathcal{T}$, another DDH group with the same order is utilized. Using these groups, we achieve the DDH-based anonymously revoking method with short signatures (Very recently, the solution is proposed in [8]). However, in this case, implementations of two elliptic curves are required, which is an overhead.

In this paper, we propose a short anonymously revocable scheme that can be efficiently implemented by supersingular curves with the embedding degree 6, in the random oracle model. To achieve the anonymity, instead of using the DDH assumption, we adopt the decision linear (DLIN) assumption often used in pairing-based group signature schemes [2, 3]. The length of our signature is about from 30% to 60% of the signature that is simply adapted the DDH-based method of [4] on $\mathcal{T}$, where the ratio varies according to the number of revoked members. In almost all cases (more than 2 revoked members), the ratio is from 30% to 40%.

2. MODEL AND SECURITY DEFINITIONS

The previous work [4] proves the security in a universally composable framework. On the other hand, it is popular that literatures on recent group signatures (e.g, [2, 3, 6]) prove the security in the model formalizing attacking games [1]. Thus, we adopt the latter model.

The participants in the model are group members (users), verifiers, and GM.

A *anonymously revocable group signature scheme* consists of the following algorithms and protocols. Non-negative integer ℓ is a security parameter.

Setup: This probabilistic initial setup algorithm, on input 1^ℓ, outputs public parameters $param$.

KeyGen: This probabilistic key generation algorithm for GM, on input $param$, outputs the group public key gpk and GM's secret key msk. Assume that gpk includes $param$.

Join: This is an interactive protocol between a probabilistic algorithm **Join-U** for the i-th user and a probabilistic algorithm **Join-GM** for GM, where the user joins the group managed by GM w.r.t. gpk. **Join-U**, on input gpk, outputs $\boldsymbol{usk}[i]$ that is the user's secret key. On the other hand, **Join-GM**, on inputs gpk, msk, outputs nothing.

Sign: This probabilistic algorithm, on inputs gpk, $\boldsymbol{usk}[i]$, a revocation list $\boldsymbol{RL}$ of tags of revoked signatures, and a message M to be signed, outputs the signature σ including a tag part tag.

Verify: This is a deterministic algorithm for verification. The input is gpk, a signature σ, a revocation list $\boldsymbol{RL}$, and the message M. Then the output is 'valid' or 'invalid'. The validity means that the signature is issued by a group member, and that the signer is different from the signers computing tags in $\boldsymbol{RL}$.

The security requirements, *t-revocability, anonymity, non-frameability* are informally defined as follows. The formal definitions will be shown in the full paper.

t-Revocability: This property captures the unforgeability of the signature in the environment that signatures can be anonymously revoked, which is derived from the traceability in the conventional group signatures [1]. Consider the revocability game between an adversary $\mathcal{A}$ and the challenger, where $\mathcal{A}$ corrupting t members tries to forge $t+1$ valid signatures $\sigma_0, \ldots, \sigma_t$ including $tag_0, \ldots, tag_t$ respectively. The revocation list $\boldsymbol{RL}_0$ given to σ_0 is empty, and $\boldsymbol{RL}_i$ given to σ_i is $(tag_0, \ldots, tag_{i-1})$ for $1 \le i \le t$. Namely, $\mathcal{A}$ tries to forge a valid signature after t signatures are revoked. $\mathcal{A}$ can request joining for honest users and corrupted users, honest user's signing, and corrupting honest users. The t-revocability requires that for all PPT $\mathcal{A}$, the probability that $\mathcal{A}$ wins the revocability game is negligible.

Anonymity: This is defined as well as traceable signature scheme [7]. Consider the anonymity game between an adversary $\mathcal{A}$ and a challenger, where $\mathcal{A}$ tries to guess the identity of the signer among two non-corrupted candidates given a signature in the situation that even GM is corrupted. The permitted queries are joining for honest users, honest user's signing, and corrupting honest users. The anonymity requires that for all PPT $\mathcal{A}$, the advantage of $\mathcal{A}$ on the anonymity game is negligible.

Non-Frameability: This requires that a signature of an honest member cannot be computed by other members and even GM. In the conventional group signature scheme, this property is required to protect the honest member against being illegally traced from a signature that was not issued by the member. In the anonymously revocable setting, the honest member cannot be traced, but may be illegally revoked using the tag. This is why this non-frameability is also required in the anonymous revocation setting.

Consider the non-frameability game between an adversary $\mathcal{A}$ and a challenger, where $\mathcal{A}$ tries to forge a signature of a honest member. In this game, $\mathcal{A}$ also corrupts GM. Thus, the permitted queries are the same as the anonymity game. The non-frameability requires that for all PPT $\mathcal{A}$, the probability that $\mathcal{A}$ wins the non-frameability game is negligible.

3. PRELIMINARIES

3.1 Bilinear Groups

Our scheme utilizes bilinear groups as follows:

1. $\mathcal{G}$ and $\mathcal{T}$ are cyclic groups of prime order p,
2. e is an efficiently computable bilinear map: $\mathcal{G} \times \mathcal{G} \to \mathcal{T}$, i.e., (1) for all $u, v \in \mathcal{G}$ and $a, b \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$, and (2) $e(g, g) \neq 1$.

This bilinear map can be efficiently implemented with the Tate pairing on supersingular curves. To reduce the length of $\mathcal{G}$ elements, we can adopt supersingular curves with the embedding degree 6.

3.2 Assumptions

Our scheme is based on the q-SDH assumption [2, 3] and decision linear (DLIN) assumption [2, 3].

DEFINITION 1 (q-SDH ASSUMPTION). *For all PPT algorithm $\mathcal{A}$, the probability*

$$\Pr[\mathcal{A}(u, u^a, \ldots, u^{(a^q)}) = (b, u^{(1/a+b)}) \wedge b \in Z_p]$$

is negligible, where $u \in_R \mathcal{G}$ and $a \in_R Z_p$.

DEFINITION 2 (DLIN ASSUMPTION). *For all PPT algorithm $\mathcal{A}$, the probability*

$$|\Pr[\mathcal{A}(u, v, w, u^a, v^b, w^{a+b}) = 1] - \Pr[\mathcal{A}(u, v, h, u^a, v^b, w^c) = 1]|$$

is negligible, where $u, v, w \in_R \mathcal{G}$ and $a, b, c \in_R Z_p$.

3.3 Proving Relations on Representations

As well as [2, 3, 6], we adopt signatures converted by Fiat-Shamir heuristic from zero-knowledge proofs of knowledge (PK). We call the signatures SPKs. The SPKs we adopt are the generalization of the Schnorr signature. We introduce the following notation.

$$SPK\{(x_1, \ldots, x_t) : R(x_1, \ldots, x_t)\}(M),$$

which means a signature of message M by a signer who knows secret values $x_1, \ldots, x_t$ satisfying a relation $R(x_1, \ldots, x_t)$. This paper utilizes an SPK proving the knowledge of a representation of $C \in \mathcal{G}$ to the bases $g_1, g_2, \ldots, g_t \in \mathcal{G}$ on message M, which is denoted as

$$SPK\{(x_1, \ldots, x_t) : C = g_1^{x_1} \cdots g_t^{x_t}\}(M).$$

This can be also constructed on group $\mathcal{T}$. The SPK can be extended to proving multiple representations with equal parts.

4. PROPOSED SCHEME

4.1 Construction Idea

The recent conventional group signature schemes (e.g., [2, 6]) with PM basically consist of a component for a membership authentication and a component for PM's tracing the signer. Thus, we can easily extract an untraceable group signature scheme without PM. We borrow this basic component from Furukawa-Imai group signature scheme [6], which is the one improved on the efficiency from [2] and is the most efficient pairing-based scheme. To this component, we add an anonymously revoking method using the pairing.

For the comparison, we first show the DDH-based method of [4]. In the method, a tag appended to every signature is computed as a pair of a random base S and $T = S^{x_{i^*}}$ for signer's secret x_{i^*}. When a signature with tag $(\hat{S}, \hat{T})$ is revoked, any signer with secret x_i shows that he did not produce tag $(\hat{S}, \hat{T})$ by the denying proof ($D = \hat{S}^\gamma$, $E = \hat{T}^\gamma$, $F = D^{x_i}$) for $\gamma \in_R Z_p$. The verifier checks it by $E \neq F$. Since the DDH assumption holds on $\mathcal{T}$, we can simply adapt this method to the pairing-based scheme. However, due to long $\mathcal{T}$ elements, the signature becomes long.

In our method, the tag is computed as $f \in_R \mathcal{G}$ (via a hash function), $S = g^{x_{i^*}+\beta}$ and $T = f^\beta$ for a public common base $g \in \mathcal{G}$ and $\beta \in_R Z_p$. Given tag $(\hat{f}, \hat{S}, \hat{T})$, the denying proof is computed as $D = g^{\gamma(x_i+\epsilon)}$, $E = \hat{f}^\epsilon$, $F = g^\gamma$ and $G = \hat{f}^\gamma$ for $\epsilon, \gamma \in_R Z_p$. Then, if and only if $i = i^*$, the relation $e(\hat{f}, D)/e(E, F) = e(G, \hat{S})/e(\hat{T}, F)$ holds. Thus, the verifier can check the denying proof. On the other hand, (f, S, T) and (E, D, F, G) reveal no information on i or i^* except for the check, under the DLIN assumption. Note that all elements in the tag and the denying proof are from $\mathcal{G}$, and thus it is expected that the signature is shorter.

4.2 Proposed Algorithms and Protocols

Setup: The input of this algorithm is security parameter 1^ℓ, and the output is $param$.

1. Select bilinear groups $\mathcal{G}, \mathcal{T}$ with the same prime order p of length ℓ, and the bilinear map e. Select hash functions $H_\mathcal{G} : \{0,1\}^* \to \mathcal{G}$, and $H : \{0,1\}^* \to Z_p$.
2. Select $g, g_1, g_2 \in_R \mathcal{G}$.
3. Output $param = (p, \mathcal{G}, \mathcal{T}, e, H_\mathcal{G}, H, g, g_1, g_2)$.

KeyGen: The input of this algorithm is $param$, and the output consists of gpk and msk.

1. Select $X \in_R Z_p$ and compute $Y = g^X$.
2. Output $gpk = (p, \mathcal{G}, \mathcal{T}, e, H_\mathcal{G}, H, g, g_1, g_2, Y)$, $msk = X$.

Join: This is an interactive protocol between the i-th joining user U_i and GM. The common input is $gpk = (p, \mathcal{G}, \mathcal{T}, e, H_\mathcal{G}, H, g, g_1, g_2, Y)$, and the input of GM is $msk = X$. The output of U_i is $\boldsymbol{usk}[i]$.

1. U_i selects $x_i, y_i' \in Z_p$, computes
$$A_i' = g_1^{x_i} g_2^{y_i'},$$
and sends A_i' to GM.
2. In addition, U_i proves the validity of A_i' using an SPK for representations.

3. GM computes $A_i = (A_i' g_2^{y_i''} g)^{1/(X+z_i)}$ for $y_i'', z_i \in_R Z_p$, and return (A_i, y_i'', z_i) to U_i.

4. U_i computes $y_i = y_i' + y_i''$ mod p, verifies $e(A_i, Y g^{z_i}) = e(g_1^{x_i} g_2^{y_i} g, g)$, and obtains $\boldsymbol{usk}[i] = (A_i, x_i, y_i, z_i)$ s.t. $A_i^{X+z_i} = g_1^{x_i} g_2^{y_i} g$.

Sign: The input of this algorithm consists of $gpk = (p, \mathcal{G}, \mathcal{T}, e, H_{\mathcal{G}}, H, g, g_1, g_2, Y)$, $\boldsymbol{usk}[i] = (A_i, x_i, y_i, z_i)$, $\boldsymbol{RL} = (tag_1, \ldots, tag_k)$, and $M \in \{0,1\}^*$, where $tag_j = (\hat{f}_j, \hat{S}_j, \hat{T}_j) \in \mathcal{G}^3$ for all $1 \le j \le k$. The output is σ.

1. Select a random nonce $r \in_R Z_p$, and compute $f = H_{\mathcal{G}}(gpk \| M \| r)$.

2. Select a random $\alpha \in_R Z_p$, and compute a commitment $C = A_i g_2^{\alpha}$.

3. Select a random $\beta \in_R Z_p$, and compute $S = g^{x_i+\beta}$ and $T = f^{\beta}$.

   Define $tag = (f, S, T)$, which means the tag part of this signature.

4. For all $1 \le j \le k$, select a random $\epsilon_j, \gamma_j \in_R Z_p$, and compute $D_j = g^{\gamma_j(x_i+\epsilon_j)}$, $E_j = \hat{f}_j^{\epsilon_j}$, $F_j = g^{\gamma_j}$ and $G_j = \hat{f}_j^{\gamma_j}$.

   Define $DP_j = (D_j, E_j, F_j, G_j)$, which means the denying proof for tag_j.

5. Compute an SPK V on message M proving knowledge of $x_i, \delta, \alpha, z_i, \beta, \gamma_1, \ldots, \gamma_k, \epsilon_1, \ldots, \epsilon_k$ s.t.

$$e(C,Y)/e(g,g) = e(g_1,g)^{x_i} e(g_2,g)^{\delta} e(g_2,Y)^{\alpha} / e(C,g)^{z_i},$$

$$S = g^{x_i+\beta},\ T = f^{\beta},$$

$$D_j = F_j^{x_i+\epsilon_j},\ E_j = \hat{f}_j^{\epsilon_j},\ F_j = g^{\gamma_j},\ G_j = \hat{f}_j^{\gamma_j},$$

   for all $1 \le j \le k$. The firstly proved equation ensures the membership, which is derived from the underlying group signature [6]. The other equations ensure the validity of tag, and $DP_1, \ldots, DP_k$.

6. Output $\sigma = (r, C, tag, DP_1, \ldots, DP_k, V)$.

Verify: The inputs are $gpk = (p, \mathcal{G}, \mathcal{T}, e, H_{\mathcal{G}}, H, g, g_1, g_2, Y)$, $\boldsymbol{RL} = (tag_1, \ldots, tag_k)$, $\sigma = (r, C, tag, DP_1, \ldots, DP_k, V)$, and $M \in \{0,1\}^*$, where $tag_j = (\hat{f}_j, \hat{S}_j, \hat{T}_j)$ and $DP_j = (D_j, E_j, F_j, G_j)$ for all $1 \le j \le k$. The output is 'valid' or 'invalid'.

1. Check V.

2. Check $e(\hat{f}_j, D_j)/e(E_j, F_j) \neq e(G_j, \hat{S}_j)/e(\hat{T}_j, F_j)$ for all $1 \le j \le k$. This inequation can be efficiently computed by $e(\hat{f}_j, D_j) \neq e(G_j, \hat{S}_j) e(E_j/\hat{T}_j, F_j)$.

3. If all checks are successful, output 'valid'. Otherwise, output 'invalid'.

5. EFFICIENCY

To reduce the signature length on supersingular curves, we can adopt the embedding degree 6. Then, to achieve 1024bit DL difficulty, the sizes of $\mathcal{G}$ (also p) and $\mathcal{T}$ elements need 171 and 1026 bits, respectively. Let R be the number of revoked members. In this case, our signature needs $171(11 + 6R)$ bits. On the other hand, in the DDH-based scheme, the length is $171(7 + R) + 1026(2 + 3R) = 171(18 + 19R)$ bits. As R varies from 0, the ratio of the length of our signature to that of the DDH-based signature varies from about 60% to about 30%, and the ratio is less than 40% in almost all cases ($R > 2$). For example, if $R = 10$, our signature needs 12,141 bits and the DDH-based signature needs 35,568 bits, and the ratio is about 34%.

In the same setting, the lengths of $\boldsymbol{RL}$ are $171 \cdot 3R$ bits and $1024 \cdot 2R$ bits in our scheme and the DDH-based scheme, respectively. Thus, the length of $\boldsymbol{RL}$ is 25%.

As for the performance, we first evaluate the number of pairings depending R in the verification, which are dominant costs. Our verifying algorithm needs $3R$ pairings, although the DDH-based algorithm needs no pairing. This is a disadvantage. However, since the verification is executed by authentication servers in the anonymous authentication, the pairings can be treated by powerful servers.

Finally we compare the performance on signing. Our signing needs 1 multi-exponentiation on $\mathcal{T}$ and $5 + 8R$ exponentiations on $\mathcal{G}$ (Pairings can be pre-computed). The DDH-based one needs $3 + 6R$ (multi-)exponentiations on $\mathcal{T}$ and 1 exponentiation on $\mathcal{G}$. Since the exponentiation on $\mathcal{T}$ is much heavier than that on $\mathcal{G}$, our scheme is more efficient.

6. CONCLUSION

We have proposed a shorter anonymously revocable group signature scheme. A future work is to implement the scheme and to apply to the authentication in WEB servers.

7. REFERENCES

[1] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," Proc. EUROCRYPT 2003, LNCS 2656, pp.614–629, 2003.

[2] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," Proc. CRYPTO 2004, LNCS 3152, pp.41–55, 2004.

[3] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," Proc. ACM-CCS '04, pp.168–177, 2004.

[4] E. Brickell and J. Li, "Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities." Proc. ACM-WPES '07, also in Cryptology ePrint Archive, Report 2007/194, 2007.

[5] D. Chaum and E. van Heijst, "Group signatures," Proc. EUROCRYPT '91, LNCS 547, pp.241–246, 1991.

[6] J. Furukawa and H. Imai, "An efficient group signature scheme from bilinear maps," Proc. ACISP 2005, LNCS 3574, pp.455–467, 2005.

[7] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable signatures," Proc. EUROCRYPT 2004, LNCS 3027, pp.571–589, 2004.

[8] P.P. Tsang, M.H. Au, A. Kapadia, S.W. Smith, "Blacklistable anonymous credentials: blocking misbehaving users without TTPs," Proc. ACM-CCS '07, pp.72–81, 2007