社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DPS－126 (29)
2006－CSEC－ 32 (29)
2006／3／16

効率的な削除機能を持つグループ署名

田中 大嗣† 宮地 充子†

† 北陸先端科学技術大学院大学情報科学研究科 〒923-1292 石川県能美市旭台 1-1
E-mail: †{d-tanaka,miyaji}@jaist.ac.jp

あらまし 双線形写像を用いた署名検証の計算量や署名長が効率のよいグループ署名が提案されている．しかし，これらの方式では削除されたメンバーに署名検証の計算量が依存する問題点がある．そこで本稿では削除メンバーに依存しないような双線形写像を用いたグループ署名を提案する．この方式は，メンバーをサブグループに分けて管理する．サブグループに分けて管理することにより，署名検証の計算量はサブグループに属する削除メンバー数に依存する．
キーワード グループ署名，双線形写像，削除機能

Group Signature Scheme with An Efficient Revocation

Daiji TANAKA† and Atsuko MIYAJI†

† School of Infomation Science, Japan Advanced Institute of Science and Technology(JAIST) 1-1, Asahidai, Nomi-shi, Ishikawa 923-1292 Japan
E-mail: †{d-tanaka,miyaji}@jaist.ac.jp

Abstract The group signature scheme with efficient computational cost of verification and signature length that uses bilinear maps is proposed. But these scheme is problem that computational cost of verification depends on revoked member. So we propose the group signature scheme that doesn't depend on revoked member. This scheme divides a member into a sub-group and controlls it. By using proposed scheme, cost of signature verification depends on revoked member who belongs to sub-group.
Key words Group Signature, Bilinear Maps, Revocation

1. はじめに

グループ署名は，Chaum と van Heyst [1] によって提案された．グループ署名は，グループのメンバーが匿名でグループの代表として署名ができ，誰でもその署名がグループの署名であることを検証できる．しかし，不正や問題が生じた場合など，必要なときにはグループ管理者のみが署名者を特定することができる．

グループ署名の署名方式に RSA 署名をベースにする手法が提案されている [2]．しかし，この手法は署名長が長くなるという問題がある．これに対して，グループ署名の署名方式に双線形写像を用いる手法が提案されている [3] [5] [6]．双線形写像を用いる手法は，署名長が短くなるという利点がある．

グループ署名ではメンバーをあらかじめグループに登録し，グループの権限を失えばグループから削除する．削除されたメンバーの署名を無効化する削除機能の付加を行う．削除機能を持つグループ署名では，検証者が削除されたメンバーのリストを参照し，そこに署名者の情報が公開されているかの検証を行なう方法と署名者自身が削除されたメンバーでないことを示す方法がある．グループ署名はグループ公開鍵及び署名のサイズと署名生成及び署名検証の計算量がメンバー数及び削除されたメンバー数に依存しないことが求められている．

そこで，本稿では署名検証の計算量が削除されたメンバー数に依存しない方式を提案する．

2. 準 備

2.1 双線形写像

提案方式で用いる双線形写像の関係の概念を記す．

定義 2.1. (双線形写像)

1. $\mathbb{G}_1$ と $\mathbb{G}_2$ は素数 p の位数の二つの巡回群で $\mathbb{G}_1 = \langle G_1 \rangle$, $\mathbb{G}_2 = \langle G_2 \rangle$ とする．
2. $\mathbb{G}_T$ は位数 p の巡回群とする．
3. e は以下の性質を持つ計算可能な写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ である．

   双線形性：$U \in \mathbb{G}_1$, $V \in \mathbb{G}_2$, $a, b \in \mathbb{Z}$ に対して，$e(aU, bV) = e(U, V)^{ab}$ の関係がある．

   非退化：$e(G_1, G_2) \neq 1$ である．

2.2 安全性の仮定

提案方式で用いる安全性の仮定について述べる.

定義 2.2. DDH(Decisional Diffie-Hellman) 仮定

有限群 $\mathbb{G}$, 元 $G \in \mathbb{G}$ と 3 つの元 $xG, yG, wG \in \mathbb{G}$ の入力に対し, 無視できない確率で $xyG = wG$ かどうかを判定できる確率的多項式時間アルゴリズムは存在しない.

定義 2.3. q-SDH(q-Strong Diffie-Hellman) 仮定

任意の t 時間アルゴリズム $\mathcal{A}$ の $(\mathbb{G}_1, \mathbb{G}_2)$ の q-SDH 問題を解く確率が ϵ より小さいとき, (q, t, ϵ)-SDH 仮定が $(\mathbb{G}_1, \mathbb{G}_2)$ で成立するという. ここで解く確率は

$$\Pr[\mathcal{A}(G_1, G_2, \gamma G_2, \cdots, (\gamma)^q G_2) = ((\frac{1}{\gamma + x})G_1, x)] < \epsilon$$

で定義される.

2.3 署名方式

グループ署名の署名方式は示す. アルゴリズムは, KeyGen, Join, Sign, Verify, Open, Revoke の 6 つから成る.

KeyGen: グループの公開鍵と秘密鍵を生成する.

Join: グループにメンバーを追加する.

Sign: メンバーの秘密鍵とメッセージを用いてグループ署名を生成する.

Verify: 公開鍵とメッセージとグループ署名を用いて, 署名の有効性の検証を行う.

Open: グループ管理者がグループ管理者の秘密鍵とメッセージとグループ署名を用いて署名者を特定する.

Revoke: グループのメンバーをメンバーリストから削除する.

2.4 グループ署名の安全性

グループ署名は以下の安全性を満たす必要がある.

Correctness: 正当なグループのメンバーによって作られたグループ署名は受理される.

Anonymity: 正当な署名が与えられたとき, グループ管理者以外が署名生成者を特定することはできない.

Non-frameability: グループ管理者やグループのメンバーでさえ, 他のメンバーに代わりにグループ署名を作ることはできない.

Traceability: グループ管理者はいつでも正当な署名から署名生成者を特定することができる.

3. 提案方式

提案方式は FI05 [6] をベースに各メンバーをサブグループに振り分けてを削除機能を追加した. また, 署名検証時の計算量を削除メンバー数に依存しない方式を提案する.

図 1 のようにサブグループにメンバーを振り分け, 検証時にどのサブグループに属するメンバーの署名かの検証を行う. その後, どのサブグループに属する署名かが分かれば, そのサブグループの削除情報との検証を行う. この削除情報の検証にはどのサブグループに属するかの検索に最大 k 回, その後にサブグループ内の検索を行う. このサブグループ内の検索は最大 t 回行う必要がある. ここで, k はサブグループ数であり, t はサブグループに属するメンバー数である.

以下に提案方式のアルゴリズムを示す. T-KeyGen, Open のアルゴリズムは FI05 と同様であるので省略する.

M-KeyGen(1^k)

1. 全メンバー数を n とし, n を k 個のサブグループに分け $n = kt$ とする.
2. k-bit の位数 p の群を $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathbb{G}$ とし, $(G_1, G_2, G) \in_R \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}$ と $\gamma \in_R \mathbb{Z}_p$ と $\{H_1, H_2, K_1, K_2, D_1, \cdots, D_k\} \in_R \mathbb{G}_1$ を選択する. また, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ とする.
3. $Y = \gamma G_2$ を計算する.
4. $\{msk, mpk\} = \{\gamma, \{p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \mathbb{G}, G_1, G_2, G, \psi, \mathcal{H}, Y, H_1, H_2, K_1, K_2, D_1, \cdots D_k\}\}$ を出力する.

$\mathrm{Join}_{GM,U}\langle(\mathcal{L}, U, mpk, msk), (mpk)\rangle$

1. GM に $(\mathcal{L}, U, mpk, msk)$ を与え, メンバー U に mpk を与える. メンバーは D_j のサブグループに属するとする.
2. U は以下を実行する.

(a) U は $sk_i := x_i \in_R \mathbb{Z}_p$ と $\{z_i', \hat{z}_i'\} \in_R \mathbb{Z}_p$ を選び, $ider_i := Q_i = x_i G, H_i = x_i H_1 + z_i' K_1$, $R_i = x_i D_j, \hat{H}_i = x_i H_2 + \hat{z}_i' K_2$ を計算する. U は x_i と $z_i', \hat{z}_i'$ の零知識証明とともに $(Q_i, H_i, R_i, \hat{H}_i)$ を GM に送信する.

(b) U は $\{x_i', z', \hat{z}'\} \in_R \mathbb{Z}_p$ を選び, $Q_i' = x_i' G, H_i' = x_i' H_1 + z' K_1, R_i' = x_i' D_j, \hat{H}_i' = x_i' H_2 + \hat{z}_i' K_2$ を計算する.

(c) $(Q_i, H_i, R_i, \hat{H}_i)$ と $(x_i, z_i, \hat{z}_i)$ の知識証明と $(Q_i', H_i', R_i', \hat{H}_i')$ と $(x_i', z', \hat{z}')$ の知識証明を GM に送信する.

3. GM は $c_i \in_R \mathbb{Z}_p$ を選択し, c を U に送信する.
4. U は $r_i = c_i x_i + x_i', s_i = c_i z_i' + z', \hat{s}_i = c_i \hat{z}_i' + \hat{z}'$ を計算し, GM に $\{r_i, s_i, \hat{s}_i\} \in \mathbb{Z}_p$ を送信する.
5. GM は以下を実行する.

(a) GM は $r_i G = c_i Q_i + Q_i', r_i H_1 + s_i K_1 = c_i H_i + H_i'$, $r_i D_j = c_i R_i + R_i', r_i H_2 + \hat{s}_i K_2 = c_i \hat{H}_i + \hat{H}_i'$ の式が成り立つかを検証する. 成立しないなら棄却する.

(b) GM は $\{y_i, z_i'', \hat{y}_i', \hat{z}_i''\} \in_R \mathbb{Z}_p$ を選び, $A_i = 1/(\gamma + y_i)(G_1 - H_i - z_i'' K_1)$ と $\hat{A}_i = 1/(\gamma + \hat{y}_i)(D_j - \hat{H}_i - \hat{z}_i'' K_2)$ を計算し, U に $(A_i, y_i, z_i'', \hat{A}_i, \hat{y}_i, \hat{z}_i'')$ を送信する.

(c) GM はグループのメンバーリスト $\mathcal{L}$ に $(U, ider_i, R_i) = (U, Q_i, R_i)$ を加える.

6. U は

$e(A_i, Y + y_i G_2) \cdot e(x_i H_1, G_2) \cdot e(z_i K_1, G_2) = e(G_1, G_2)$, $e(\hat{A}_i, Y + \hat{y}_i G_2) \cdot e(x_i H_2, G_2) \cdot e(\hat{z}_i K_2, G_2) = e(D_j, G_2)$

の式が成り立つか検証し, 成り立つなら以下をグループメンバーの証明書とする.

$cert_i := (A_i, y_i, z_i = z_i' + z_i'', \hat{A}_i, \hat{y}_i, \hat{z}_i = \hat{z}_i' + \hat{z}_i'')$

成立しないなら棄却する.

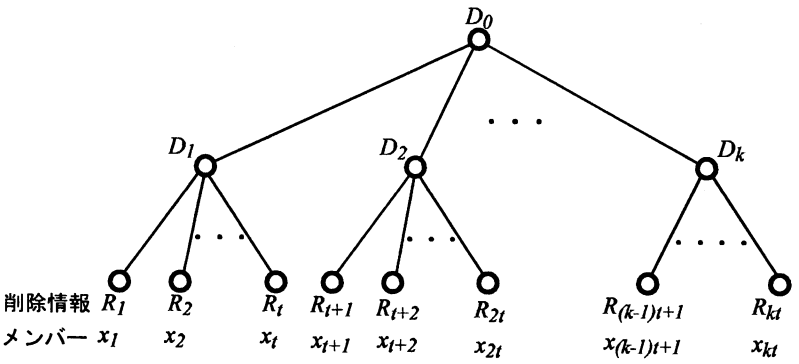

図 1 メンバーの振り分け

7. GM はメンバー U を追加した $\mathcal{L}$ を出力する．U は $(cert_i, sk_i, ider_i, R_i)$ として $((A_i, y_i, z_i, \hat{A}_i, \hat{y}_i, \hat{z}_i), x_i, Q_i, R_i)$ を出力する．

Revoke(i)

1. GM は $\tau \in_R \mathbb{Z}_p$ を選択し，削除リスト RL の全ての R_i に対して $R_i' = \tau R_i$ を計算し，$G_2' = \tau G_2$ を計算する．

2. GM は削除リスト RL に R_i' を公開し，G_2' を公開する．

Sign($mpk, tpk, cert_i, sk_i, M$)

1. $\{r, q, \hat{q}\} \in_R \mathbb{Z}_p$ を選び，$\eta = qx_i$ を計算し，

$$B_1 = A_i + qK_1, B_2 = \hat{A}_i + \hat{q}K_2, U = Q_i + rG, V = rS,$$
$$W = rT, d = e(D_j, x_i G_2')^q, E = qG_2 \quad (1)$$

を計算する．また，以下の関係が成り立つ．

$$e(G_1, G_2) = e(B_1, Y) \cdot e(H_1, G_2)^{x_i} \cdot e(B_1, G_2)^{y_i} \cdot e(K_1.G_2)^{z_i - qy_i} \cdot e(K_1, Y)^{-q} \quad (2)$$
$$e(D_j, G_2) = e(B_2, Y) \cdot e(H_2, G_2)^{x_i} \cdot e(B_2, G_2)^{\hat{y}_i} \cdot e(K_2.G_2)^{\hat{z}_i - \hat{q}\hat{y}_i} \cdot e(K_2, Y)^{-\hat{q}} \quad (3)$$

2. $\{r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_\eta\} \in_R \mathbb{Z}_p$ を選び，
$o_1' = e(H_1, G_2)^{r_1} \cdot e(B_1, G_2)^{r_2} \cdot e(K_1, G_2)^{r_3} \cdot e(K_1, Y)^{r_4}$,
$o_2' = e(H_2, G_2)^{r_1} \cdot e(B_2, G_2)^{r_6} \cdot e(K_2, G_2)^{r_7} \cdot e(K_2, Y)^{r_8}$,
$U' = (r_1 + r_5)G, V' = r_5 S, W' = r_5 T, d' = e(D_j, G_2)^{r_\eta}$,
$E' = r_4 G_2, F' = r_1 E - r_\eta G_2$ を計算する．

3. $c = \mathcal{H}(p, G_1, G_2, G_T, G, \psi, Y, S, T, H_1, H_2, K_1, K_2, B_1, B_2, U, V, W, d, E, o_1', o_2', U', V', W', d', E', F', M)$ を計算する．

4. $r_1' = cx_i + r_1, r_2' = cy_i + r_2, r_3' = c(z_i - qy_i) + r_3$,
$r_4' = -cq + r_4, r_5' = cr + r_5, r_6' = c\hat{y}_i + r_6$,
$r_7' = c(\hat{z}_i - \hat{q}\hat{y}_i) + r_7, r_8' = -c\hat{q} + r_8, r_\eta' = c\eta + r_\eta$ を計算する．

5. メッセージ M の署名 σ として $(B_1, B_2, U, V, W, d, E, c, r_1', r_2', r_3', r_4', r_5', r_6', r_7', r_8', r_\eta')$ を出力する．

Verify(mpk, tpk, M, σ)

1. $\tilde{o}_1 = e(H_1, G_2)^{r_1'} \cdot e(B_1, G_2)^{r_2'} \cdot e(K_1, G_2)^{r_3'} \cdot e(K_1, Y)^{r_4'} (\frac{e(G_1, G_2)}{e(B_1, Y)})^{-c}, \tilde{U} = (r_1' + r_5')G - cU$,
$\tilde{V} = r_5' S - cV, \tilde{W} = r_5' T - cW, \tilde{E} = r_5' G_2 - cE, \tilde{F} = r_1' E - r_\eta' G_2$ を計算する．

2. 各 $j \in [1, k]$ に対し，$\tilde{o}_2 = e(H_2, G_2)^{r_1'} \cdot e(B_2, G_2)^{r_6'} \cdot e(K_2, G_2)^{r_7'} \cdot e(K_2, Y)^{r_8'} (\frac{e(D_j, G_2)}{e(B_2, Y)})^{-c}$,
$\tilde{d} = e(D_j, G_2)^{r_\eta'} \cdot (1/d)^c$ を求める．

3. $c = \mathcal{H}(p, G_1, G_2, G_T, G, \psi, Y, S, T, H_1, H_2, K_1, K_2, B_1, B_2, U, V, W, d, E, \tilde{o}_1, \tilde{o}_2, \tilde{U}, \tilde{V}, \tilde{W}, \tilde{d}, \tilde{E}, \tilde{F}, M)$ が成り立つなら受理する．成立しないなら D_j を変えて c を再度計算して検証を行う．全ての D_j に対して c が成立しないなら棄却する．

4. 3 で成立した D_j の削除リスト RL_j に対し，$d \neq e(R_i, E)$ を検証する．$d = e(R_i, E)$ となるような署名であれば棄却する．

3.1 安 全 性

定理 3.1. 提案方式は，SDH 仮定のもとで Traceability の性質を持つ

補題 3.2. メッセージ m の署名とランダムオラクルの二つの集合を与える．

$\{(B_1, B_2, U, V, W, E, o_1', o_2', U', V', W', E', F', c_1', r_1', r_2', r_3', r_4', r_5', r_6', r_7', r_8', r_\eta'), \mathcal{H}_1\}$
$\{(B_1, B_2, U, V, W, E, o_1', o_2', U', V', W', E', F', c_2, r_1'', r_2'', r_3'', r_4'', r_5'', r_6'', r_7'', r_8'', r_\eta''), \mathcal{H}_2\}$

上記の関係は以下の通りである．

$(r_1', r_2', r_3', r_4', r_5', r_6', r_7', r_8', r_\eta') \neq (r_1'', r_2'', r_3'', r_4'', r_5'', r_6'', r_7'', r_8'', r_\eta'')$
$c_1 = \mathcal{H}_1(p, G_1, G_2, G_T, G, \psi, Y, S, T, H_1, H_2, K_1, K_2, B_1, B_2, U, V, W, E, o_1', o_2', U', V', W', E', F', M)$
$\neq c_2 = \mathcal{H}_2(p, G_1, G_2, G_T, G, \psi, Y, S, T, H_1, H_2, K_1, K_2, B_1, B_2, U, V, W, E, o_1', o_2', U', V', W', E', F', M)$
$\tilde{o}_1 = e(H_1, G_2)^{r_1'} \cdot e(B_1, G_2)^{r_2'} \cdot e(K_1, G_2)^{r_3'} \cdot e(K_1, Y)^{r_4'} (\frac{e(G_1, G_2)}{e(B_1, Y)})^{-c_1}$

$$\tilde{o}_1' = e(H_1,G_2)^{r_1''}\cdot e(B_1,G_2)^{r_2''}\cdot e(K_1,G_2)^{r_3''}\cdot e(K_1,Y)^{r_4''}\left(\frac{e(G_1,G_2)}{e(B_1,Y)}\right)^{-c_2}$$

$$\tilde{o}_2 = e(H_2,G_2)^{r_1'}\cdot e(B_2,G_2)^{r_6'}\cdot e(K_2,G_2)^{r_7'}\cdot e(K_2,Y)^{r_8'}\left(\frac{e(D_j,G_2)}{e(B_2,Y)}\right)^{-c_1}$$

$$\tilde{o}_2' = e(H_2,G_2)^{r_1''}\cdot e(B_2,G_2)^{r_6''}\cdot e(K_2,G_2)^{r_7''}\cdot e(K_2,Y)^{r_8''}\left(\frac{e(D_j,G_2)}{e(B_2,Y)}\right)^{-c_2}$$

$$\tilde{U} = (r_1'+r_5')G - c_1U$$

$$\tilde{U}' = (r_1''+r_5'')G - c_2U$$

$$\tilde{V} = r_5'S - c_1V$$

$$\tilde{V}' = r_5''S - c_2V$$

$$\tilde{W} = r_5'S - c_1W$$

$$\tilde{W}' = r_5''S - c_2W$$

$$\tilde{E} = r_\eta' D_j - c_1E$$

$$\tilde{E}' = r_\eta'' D_j - c_2E$$

そのとき，(1) と (2) を満たすような $(A_i,x_i,y_i,z_i,q,r)\in\mathbb{G}_1\times(\mathbb{Z}_p)^5$ を計算できる．また，同様に (1) と (3) を満たすような $(\hat{A}_i,x_i,\hat{y}_i,\hat{z}_i,\hat{q},v)\in\mathbb{G}_1\times(\mathbb{Z}_p)^5$ を計算できる．

証明

以下の (A_i,x_i,y_i,z_i,q,r) は補題を証明する．

$$A_i = B_1 - \left(\frac{r_4'-r_4''}{c_1-c_2}\right)K_1$$

$$x_i = \frac{r_1'-r_1''}{c_1-c_2}$$

$$y_i = \frac{r_2'-r_2''}{c_1-c_2}$$

$$z_i = \frac{(r_3'-r_3'')(c_1-c_2)-(r_2'-r_2'')(c_1-c_2)}{(c_1-c_2)^2}$$

$$q = \frac{r_4'+r_4''}{c_1-c_2}$$

$$r = \frac{r_5'-r_5''}{c_1-c_2}$$

補題 3.3. q-1 回よりも少ない Join プロトコルに従い，Traceability を破るような攻撃者 $\mathcal{A}$ が存在するなら，ブラックボックスとして $\mathcal{A}$ を使い q-SDH を破るか離散対数問題を解く攻撃者 $\mathcal{A}'$ が存在する．

証明 $\mathcal{A}'$ に q+2 個の入力 $(Q_1,Q,\gamma Q,\gamma^2Q,\cdots,\gamma^qQ)$ を与える．ここで，$Q\in\mathbb{G}_2$ であり，$Q_1=\psi(Q)$ とする．

1. $\mathcal{A}'$ はランダムに $\alpha\in_R\mathbb{Z}_p,\{\{a_i,b_i\}\in_R\mathbb{Z}_p\}_{i\in[q-1]}$，$m\in_R[q-1]$ を選択する．
2. $\gamma=w-a_m$ と仮定する．$\mathcal{A}'$ はランダムに $\theta\in_R\mathbb{Z}_p$ を選択し，以下を計算する．

$$G_2 = \Big(b_m\prod_{i=1,i\neq m}^{q-1}(w+a_i-a_m)\Big)Q + \Big(\alpha\prod_{i=1}^{q-1}(w+a_i-a_m)\Big)Q$$

$$G_1 = \psi(G_2)$$

$$H_1 = \prod_{i=1,i\neq m}^{q-1}\Big(w+a_i-a_m\Big)\psi(Q)$$

$$K_1 = \theta H_1$$

$$Y = \gamma G_2 = \Big((w-a_m)b_m\prod_{i=1,i\neq m}^{q-1}(w+a_i-a_m)\Big)Q + \Big((w-a_m)\alpha\prod_{i=1}^{q-1}(w+a_i-a_m)\Big)Q$$

同様に H_2,K_2 を計算する．

3. $\mathcal{A}'$ は $mpk=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,\mathbb{G},G_1,G_2,G,\psi,\mathcal{H},Y,H_1,H_2,K_1,K_2,D_j)$ を出力し，$\mathcal{A}$ に提供する．
4. $\mathcal{A}'$ は $\mathcal{A}$ から $tpk=(S,T)$ を受信する．
5. $\mathcal{A}$ が実行されるとき，$\mathcal{A}'$ のメンバー U として i 番目の Join プロトコルのはじめの 2 ステップを終え，以下のように行う．

(a) $\mathcal{A}'$ は $\mathcal{A}$ を巻き戻し，他のランダムオラクルを選択することによって x_i と z_i' を得る．

(b) $\mathcal{A}'$ は以下のように A_i,y_i,z_i'' を計算する．

$$z_i'' = \frac{b_i-x_i}{\theta} - z_i'$$

$$y_i = a_i$$

$$A_i = \frac{1}{y_i+\gamma}(G_1 - x_iH_1 - (z_i'+z_i'')K_1) = \frac{1}{a_i+\gamma}(G_1 - b_iH_1) = \alpha\prod_{j=1,j\neq i}^{q-1}\Big(w+a_j-a_m\Big)\psi(Q) + (b_m-b_i)\prod_{j=1,j\neq m,i}^{q-1}\Big(w+a_i-a_m\Big)\psi(Q)$$

ここで，$i=m$ のとき $b_i-b_m=0$ である．そのとき，$\mathcal{A}'$ は $\mathcal{A}$ に (A_i,y_i,z_i'') を送る．

(c) $\mathcal{A}$ は $\mathcal{L}$ に $(U,Q_i=x_iG,R_i=x_iD_j)$ を追加する．

6. $\mathcal{A}$ は (m,σ) を出力し，無視できない確率 ϵ_1 で成功する．それは $acc\leftarrow\texttt{Verify}(mpk,tpk,m,\sigma)$ と $(\perp',proof)\leftarrow\texttt{Open}(mpk,tpk,tsk,m,\sigma,\mathcal{L})$ である．そのとき，Forking Lemma と補題 3.2 から，$\mathcal{A}'$ は (1) と (2)，$x_iG\notin\mathcal{L}$ を満たすような $(A_i,x_i,y_i,z_i,q,r)\in\mathbb{G}_1\times(\mathbb{Z}_p)^5$ を得ることができる．ここで，

$$A_i = \frac{1}{y_i+\gamma}(G_1 - x_iH_1 - (z_i'+z_i'')K_1) = \frac{1}{y_i+\gamma}(G_1 - (x_i+\theta z_i)H_1) = \frac{\alpha w-(x_i+\theta z_i+b_m)}{w+y_i-a_m}\prod_{j=1,j\neq m}^{q-1}\Big(w+a_j-a_m\Big)\psi(Q)$$

である．

7. (4) は離散対数問題を解くことが困難である限り，無視できる確率でしか起こらない．

$$(w+y_i-a_m)\,|\,(\alpha w-(x_i+\theta z_i)+b_m) \qquad (4)$$

$y_i\notin\{a_i\}_{i=1,\cdots,q-1}$ が成り立つような確率は ϵ_1 より小さいので，$y_i\notin\{a_i\}_{i=1,\cdots,q-1}\backslash a_m$ である確率は無視できない確率 $\frac{\epsilon_1}{(q-1)}$ より大きくなる．それゆえ，少なくとも無視できない確率を持つ A_i の分母として $w+y_i-a_m$ が存在する．

$$\frac{\alpha w-(x_i+\theta z_i+b_m)}{w+y_i-a_m}\prod_{j=1,j\neq m}^{q-1}\Big(w+a_j-a_m\Big)$$

が割り切れる場合，以下のような $\{c_i\in Z_p\}$ を計算できる．

$$A_i = \sum_{i=0}^{q-1}(c_iw^i)\psi(Q) + \frac{c_q}{w+y_i-a_m}\psi(Q)$$

$A_i,\{c_i\in\mathbb{Z}_p\}_{i=0,\cdots,q},\theta,x_i,y_i,z_i,\{a_i\}_{i=1,\cdots,q-1},b_m$ から与えられた q-SDH の解を以下に示す．

$$\Big(\frac{1}{c_q}(A_i-\sum_{i=0}^{q-1}(c_iw^i)\psi(Q)),y_i-a_m\Big)$$

ここで，(4) と $a_m\neq y_i$ が無視できない確率で成り立つ場合を考える．(4) から

$$\alpha(y_i-a_m)+x_i+\theta z_i-b_m=0$$

が成り立つ．

$\{L, N\} \in \mathbb{G}_2$ を与えられた別の攻撃者 $\mathcal{A}''$ を考える．$\mathcal{A}''$ はランダムに $\{b_m, w, a_m, \theta\} \in \mathbb{Z}_p$ を選択し，以下を計算する．

$G_2 = b_m L + wN$

$G_1 = \psi(G_2)$

$H_1 = \psi(N)$

$K_1 = \theta H_1$

$Y = \gamma G_2 = (w - a_m)G_2$

$\mathcal{A}''$ は $\gamma = w - a_m$ を知っているので，グループ管理者の代わりを完全に務める．以下の関係を考える．

$$L \Leftrightarrow \prod_{i=1, i\neq m}^{q-1} \Big(w + a_i - a_m\Big)Q$$

$$N \Leftrightarrow \alpha \prod_{i=1, i\neq m}^{q-1} \Big(w + a_i - a_m\Big)Q$$

$\mathcal{A}''$ は (4) から $\alpha = \log_D N$ を計算できることが分かる．ここで，(4) と $a_m = y_i$ が無視できない確率で成り立つ場合を考える．(4) から

$\theta z_i - b_m = 0$

が成り立つ．

$\{L, K\} \in \mathbb{G}_2$ を与えられた別の攻撃者 $\mathcal{A}'''$ を考える．$\mathcal{A}''$ は以下で示していること以外 $\mathcal{A}''$ と同じである．

(a) $\mathcal{A}'''$ は $\alpha \in \mathbb{Z}_p$ を生成するが，$\theta \in \mathbb{Z}_p$ は生成できない．

(b) $\mathcal{A}'''$ は $N = \alpha L$ を計算し，公開鍵の与えられた K_1 を使用する．

$\mathcal{A}''$ は $\theta = \log_L K_1 = \frac{b_m}{z_i}$ を計算できることが分かる．

定理 3.1 は補題 3.3 から得られる．

定理 3.4. 提案方式は，DDH 仮定のもとで Anonymity の性質を持つ

補題 3.5. Sign プロトコルの x_i, y_i, z_i, q, r の知識証明の構成は零知識である．

証明 以下のシミュレータ $\mathcal{S}$ が補題 3.5 を証明する．

1. $\mathcal{S}$ はランダムに $\{r'_1, r'_2, r'_3, r'_4, r'_5, r'_6, r'_7, r'_8, r'_\eta, c\} \in \mathbb{Z}_p$ を選択する．

2. $\mathcal{S}$ は以下を生成する．

$\tilde{o}_1 = e(H_1, G_2)^{r'_1} \cdot e(B_1, r'_2 G_2 + cY) \cdot e(K_1, G_2)^{r'_3} \cdot e(K_1, Y)^{r'_4} \cdot e(G_1, G_2)^{-c}$

$\tilde{o}_2 = e(H_2, G_2)^{r'_1} \cdot e(B_2, r'_2 G_2 + cY) \cdot e(K_2, G_2)^{r'_7} \cdot e(K_2, Y)^{r'_8} \cdot e(D_j, G_2)^{-c}$

$\tilde{U} = (r'_1 + r'_5)G - cU$

$\tilde{V} = r'_5 S - cV$

$\tilde{W} = r'_5 T - cW$

$\tilde{E} = r'_\eta D_j - cE$

$\tilde{F} = r'_1 E - r'_\eta G_2$

$\mathcal{S}$ は $\tilde{o}_1, \tilde{o}_2, \tilde{U}, \tilde{V}, \tilde{W}, \tilde{d}, \tilde{E}, \tilde{F}, c, r'_1, r'_2, r'_3, r'_4, r'_5, r'_6, r'_7, r'_8, r'_\eta$ を出力する．

補題 3.6. Anonymity を破るような攻撃者 $\mathcal{A}$ が存在するなら，ブラックボックスとして $\mathcal{A}$ を使い DDH を破るような攻撃者 $\mathcal{A}'$ が存在する．

証明 グループ署名の (U, V, W) は $Q_i = x_i G$ の二重暗号である．そして，DDH 仮定を仮定するなら強秘匿である．残りのグループ署名は，ランダムオラクルモデルで $r = \log_S V = \log_T W$ の非対話零知識証明である．従って，グループ署名は Q_i の IND-CCA2 の暗号化としてみなすことができる．

グループ署名の Anonymity を破るような攻撃者 $\mathcal{A}$ を使って上記の IND-CCA2 安全な暗号法を破ることを示す．以下の通信を考える．

1. ターゲットの鍵生成は Keygen に対応する．
2. ターゲットの復号オラクルは Open に対応する．
3. ターゲットの IND-CCA2 ゲームの $\mathcal{A}'$ によるチャレンジ平文の選択は $\mathcal{A}$ によるメンバーの証明書と署名鍵を構成するペアに対応する．
4. ターゲットの IND-CCA2 ゲームの終わりの返答は $Exp^{An}_{GS,\mathcal{A}}$ の終わりの $\mathcal{A}$ の返答に対応する．

定理 3.4 は補題 3.6 から得られる．

定理 3.7. 提案方式は，離散対数問題を解くことが困難であるなら Non-Frameability の性質を持つ

証明 グループ署名の Non-Frameability を破るような攻撃者 $\mathcal{A}$ が存在するなら，ブラックボックスとして $\mathcal{A}$ を使い離散対数問題を解く攻撃者 $\mathcal{A}'$ が存在する．

以下は $\mathcal{A}$ の記述である．

1. $\mathcal{A}'$ はインスタンス (Q, G) を与えられ，$\log_G Q$ の計算を尋ねられると仮定する．そのとき，$\mathcal{A}'$ は $\mathcal{A}$ のメンバー U として Join プロトコルで保証する．このプロトコルは $\mathcal{A}'$ がランダムに $z'_i \in_R \mathbb{Z}_p$ 選択し，$Q_i = Q$ と $H_i = Q + z'_i K_1$ を生成する．そして，$\mathcal{A}$ に Q_i と H_i を送信する．$\mathcal{A}'$ は $\log_G Q_i$ を知らないけれども，$\mathcal{A}$ を巻き戻すことによって残りのプロトコルを完了することができる．これは残りのプロトコルが零知識証明であるので可能である．

2. (m, σ) が与えられるなら，$\mathcal{A}$ は Open が Q を出力するようなメッセージ m のグループ署名 σ を生成することを質問する．そのとき，$\mathcal{A}'$ はランダムに $r \in_R \mathbb{Z}_p$ を選択し，$(U, V, W) = (Q + rG, rS, rT)$ を生成する．$\mathcal{A}'$ は $\log_G Q_i$ を知らないけれども，$\mathcal{A}'$ は選ぶランダムオラクルによって残りの署名を生成する．残りのプロトコルは零知識証明 (補題 3.5) であるので可能である．

3. $\mathcal{A}$ は提案されたグループ署名の Non-Frameability を破るので，$\mathcal{A}$ は (σ', m') が無視できない確率で与えられるなら，Open が Q を出力するようなメッセージ m' のグループ署名 σ' を出力する．Forking Lemma と補題 3.2 から $\mathcal{A}'$ は $\mathcal{A}$ を巻き戻しランダムオラクルを選択することで，$Q_i = x_i G$ のような x_i を抽出する．

これは離散対数問題を解いている．

4. 性能評価

計算コストと署名長について [7] の方式との比較を行う．提案方式は [7] の階層 2 のときと等しいのでそのときの計算コストと署名長との比較を行う．表 1 は署名と検証における $\mathbb{G}, \mathbb{G}_1, \mathbb{G}_2$

表 1 演算の種類ごとの計算回数

	NF05 [5]		MNF06 [7](l=2)		提案方式	
	署名	検証	署名	検証	署名	検証
$\mathbb{G}, \mathbb{G}_1, \mathbb{G}_2$ での スカラー倍算	$13S_{\mathbb{G}_1}$	$10S_{\mathbb{G}_1}$	$2S_{\mathbb{G}_1} + 6S_{\mathbb{G}}$	$6S_{\mathbb{G}}$	$2S_{\mathbb{G}_1} + 5S_{\mathbb{G}_2} + 6S_{\mathbb{G}}$	$4S_{\mathbb{G}_2} + 6S_{\mathbb{G}}$
$\mathbb{G}_T$ でのべき乗演算	$5S_{\mathbb{G}_T}$	$6S_{\mathbb{G}_T}$	$9S_{\mathbb{G}_T}$	$11S_{\mathbb{G}_T}$	$10S_{\mathbb{G}_T}$	$(10 + 2k)S_{\mathbb{G}_T}$
ペアリング	2	$3 + r$	2	4	3	$4 + t$
署名長 (bits)	2904		2567		3759	

$S_{\mathbb{G}_1}, S_{\mathbb{G}_2}, S_{\mathbb{G}}$: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}$ 各々のスカラー倍算, $S_{\mathbb{G}_T}$: $\mathbb{G}_T$のべき乗演算, r : 削除メンバー数

のスカラー倍算と $\mathbb{G}_T$ のべき乗演算，ペアリングの計算回数を比較している．提案方式は検証時に削除情報との比較を行う必要があるので，$\mathbb{G}_T$ のべき乗演算にグループ数の k とペアリングの回数にグループの分割サイズ t に依存する計算量が必要になる．

表 2 は削除情報更新にかかる計算量である．[5] の方式は，削除時に情報を更新しない方式であるので表 2 では省略する．[7] の方式では，メンバーが削除されると GM が残ったメンバーの証明書を更新する必要があり，残ったメンバー数に依存する．提案方式では，GM が公開鍵の一部と削除情報の更新を行うので削除メンバー数に依存する．

表 2 削除更新時の計算量

	削除更新の計算量
MNF06	$GM : 2(n - r)S_{\mathbb{G}_1}$
提案方式	$GM : (36 + r)S_{\mathbb{G}_1}$

n : メンバー数, r : 削除メンバー数

5. ま と め

本稿では，双線形写像を用いたグループ署名においてメンバーを分割する方式を提案した．従来方式は検証時に削除されたメンバー数に依存する計算量が必要であったが，提案方式ではメンバーを分割することにより検証時に削除メンバー数に依存しない計算量で行うことができる．今後の課題として，署名生成と署名検証の計算コストの削減が挙げられる．

文 献

[1] D. Chaum and E. van Heyst; Group Signatures, Advances in Cryptology-Proceedings of EUROCRYPT, LNCS 547, pp. 257-365, (1991)

[2] Jan Camenisch, Jens Groth; Group Signatures: Better Efficiency and New Theoretical Aspect, SCN 2004, LNCS 3352, pp. 120-133, (2005)

[3] Dan Boneh, Xavier Boyen, Hovav Shacham: Short Group Signature. CRYPT 2004, Volume 3152 of Lecture Notes in Computer Science, pages 41-55, (2004)

[4] Mihir Bellare, Daniele Micciancio, Bogdan Warinschi; Foundations of Group Signature: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions, EUROCRYPT 2003, LNCS 2656, pp. 614-629, (2003)

[5] Toru Nanishi, Nobuo Funabiki:A Verifier-Local Revocation Group Signature Scheme with Backward Unlinkability from Bilinear Maps, SCIS2005, Volume of . pp.1141-1146,Full paper, (2005)

[6] Jun Furukawa, Hideki Imai: An Efficient Group Signature Scheme from Bilinear Maps. ACISP 2005, LNCS 3574, pp. 455-467, (2005)

[7] 三谷 千恵, 中西 透, 舩曳 信生: 木構造により所属無効化を効率的にした双線形写像に基づくグループ署名方式. SCIS 2006, 4A2-4, (2006)