SCIS 2009 The 2009 Symposium on Cryptography and Information Security
Otsu, Japan, Jan. 20-23, 2009
The Institute of Electronics, Information and Communication Engineers

フレキシブルリング署名
A Flexible Ring Signature

星野 文学* 鈴木 幸太郎† 小林 鉄太郎 †
Fumitaka Hoshino Koutarou Suzuki Tetsutaro Kobayashi

あらまし 署名者の匿名性を守るための署名技術には大別して 2 つの方法がある. 一つは 1991 年に Chaum らが提案したグループ署名 [CH91] の概念で, この方法にはグループ管理者と呼ばれる信頼できる第三者 (TTP) が登場する. もう一つは 2001 年に Rivest らが提案したリング署名 [RST01] の概念で, この方法にはグループ管理者が存在しない. 著者らは, このグループ署名とリング署名の間の中間に位置するような署名を提案している [SHK07]. 本論文では, この中間的な署名方式を改造して署名者がリング署名を生成した後にグループ管理者がリング署名の参加メンバを変更したりリング署名を普通の署名に変換したりできる事を実現する.

キーワード リング署名, 非超特異楕円曲線, フロベニウス写像の固有空間, ペアリング

1 はじめに

署名者の匿名性を守るための署名技術には大別して 2 つの方法がある.

一つは 1991 年に Chaum らが提案したグループ署名 [CH91] の概念で, この方法にはグループ管理者と呼ばれる信頼できる第三者 (TTP) が登場する. グループ管理者はセットアップと呼ばれる手続きによって署名グループを決定し, 署名者はグループ管理者との対話を通じて秘密鍵を決定する. またグループ管理者は署名がメンバーの誰によって作成されたか知る事が出来る. このような強い力を持つ TTP を仮定することは, いわゆるビッグブラザーを生むとされ, 好ましくないと言われる事も多い. またグループ署名では, グループからメンバを排除したり新たにメンバを加えたり, グループメンバの一部だけを含む子グループを作成する場合, 一般にはセットアップが必要であり, それを避けるようなグループ署名は煩雑になりがちである.

一方, もう一つは 2001 年に Rivest らが提案したリング署名 [RST01] の概念で, この方法にはグループ管理者が存在しない. 署名者は, 自身が所有する公開鍵のリストから任意に公開鍵を選び自分の公開鍵, 秘密鍵, および選んだ公開鍵から自分を含む任意のグループ (リング) に関して署名者が匿名となる署名を生成できる. この場合グループ管理者が存在しないので完全に匿名性が保たれてしまい, 例えば悪意を持ったメンバーが勝手にグループを作って署名を発行してしまう等の行為は原理的に防ぎようがない.

グループ署名における TTP の強い能力が何らかの手段により適切に管理されるとすれば, こうした抑止力のあるシステムの方が, 完全に匿名化され全く管理されないシステムより現実的な解になり得ると考えられる.

著者らは, セッティング無しで任意に署名グループを指定可能でありながら信頼できるグループ管理者が署名を行ったメンバーの特定ができるようなグループ署名とリング署名の間の中間に位置するような署名を提案している [SHK07].

本論文では, この方式を改造して, 署名者がリング署名を生成した後にグループ管理者がリング署名の参加メンバを変更したりリング署名を普通の署名に変換したりできる事を実現する. 本提案がリング署名である事を強く意識し, 以降署名グループの事をリングと呼ぶこととする. またリングを変更することを再リンクと呼ぶ.

* 独立行政法人情報処理振興機構, 〒 113-6591 東京都文京区本駒込 2-28-8 文京グリーンコートセンターオフィス 16 階, Information-technology Promotion Agency, Japan, 16th Floor Bunkyo Green Court Center Office 2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591 Japan
† NTT 情報流通プラットフォーム研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11 NTT Information Sharing Platform Laboratories, 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan

2 準備

2.1 ペアリング可能な非超特異楕円曲線

ペアリング可能な非超特異楕円曲線においてフロベニウス写像の固有空間を考慮すると次のような概念をみたす同型の巡回群の組 G_1, G_2, G_3 を考えることが出来る [SHUK03, HSK05].

- G_2, G_3 上の DDH 問題が計算量的に困難である.
- G_1 上の DH 問題が計算量的に困難である.
- 多項式時間で計算可能な非退化な双線形写像 $e : G_2 \times G_1 \to G_3$ が存在する.

群 G_2 がフロベニウス写像の固有空間に相当する. このような曲線は例えば Miyaji らの方法 [MNT01] を使えば得ることができる. $\mathcal{G}$ を G_1 の生成元, g を G_2 の生成元とする.

さらに、以下の問題が計算量的に困難であることを仮定する.

G_2 から G_1 へのスキュー CDH 問題: $(g, g^\alpha, \mathcal{G})$ から $\mathcal{G}^\alpha$ を求める問題.

ヒント付きの G_2 上の CDH 問題: $(g, g^\alpha, g^\beta, \mathcal{G}, \mathcal{G}^\alpha, \mathcal{G}^\beta)$ から $g^{\alpha\beta}$ を求める問題.

G_2 上の DDH 問題: $(g, g^\alpha, g^\beta, g^\gamma)$ と $(g, g^\alpha, g^\beta, g^{\alpha\beta})$ を見分ける問題.

2.2 DDH-tuple への所属証明

ある $g, y, h, w \in G_2$ が DDH-tuple に属する事を離散対数を明かさずに証明する典型的な方法が 2 通り存在する. ひとつは

$$e(y, \mathcal{G}) = e(g, \mathcal{X})$$
$$e(w, \mathcal{G}) = e(h, \mathcal{X})$$

なる $\mathcal{G}, \mathcal{X} \in G_1$ を検証者に与える Joux-Nguyen の方法 [JN01] である. (あるいは Boneh-Lynn-Shacham の short signature[BLS01] の方法と言うべきかもしれない). もうひとつは離散対数 x を知る者が証明者となって知識の対話証明を実行する Chaum-Pederson のプロトコル [CP92] で, Fiat-Shamir Heuristic[FS86] を用いて非対話化することもできる. 後の便宜の為 Camenisch らの形式的記法 [CS97] (と同様のもの) を導入しておく. この記法によれば Chaum-Pederson のプロトコルは

$$PK\{(x) : y = g^x \wedge w = h^x\}$$

と記述される. 中括弧内の : の右側の命題 $y = g^x \wedge w = h^x$ を満たすような : の左側 (x) に関する Proof of Knowledge (PK) を意味する. さらに, この知識証明の非対話版の証明生成アルゴリズムおよび検証アルゴリズムをそれぞれ

$$P\{(x) : y = g^x \wedge w = h^x\}$$
$$V\{(x) : y = g^x \wedge w = h^x\}(\sigma)$$

等と記述することとする.

2.3 [SHK07] の基本署名方式

上記 2 通りの DDH-tuple への所属証明をあえて両方用いる事によって, 2 通りの検証方法を持つ署名を構成できる. この署名方式には署名者と検証者の他に, 第三の参加者として TTP が登場する. 後にこの署名を拡張してリング署名を構成する際に, この TTP がグループ管理者となる.

セキュリティパラメタ k に応じて G_1, G_2 を選び, 生成元 $\mathcal{G} \in G_1$ および $g \in G_2$ を選んで公開する. また, ハッシュ関数 $H : \{0,1\}^* \to G_2$ を公開する.

鍵生成:

- $x \in_U \mathbb{Z}/\ell\mathbb{Z}$
- $\mathcal{X} \leftarrow \mathcal{G}^x$
- $y \leftarrow g^x$

とし, $(x, \mathcal{X}, y)$ を出力する. 署名者は秘密鍵 x を保持し, TTP 用鍵 $\mathcal{X}$ を TTP に預け, 公開鍵 y は公開する. TTP は必要に応じて $e(y, \mathcal{G}) = e(g, \mathcal{X})$ を確認し, 必要に応じて公開鍵証明書の付与等を行う.

署名生成: 文書 m, 秘密鍵 $x \in \mathbb{Z}/\ell\mathbb{Z}$.

- $h \leftarrow H(m)$
- $w \leftarrow h^x$
- $\sigma \leftarrow P\{(x) : y = g^x \wedge w = h^x\}$

とし, 署名 (w, σ) を出力する.

署名検証 1: 文書 m, 署名 (w, σ), TTP 用鍵 $\mathcal{X}$.

- $h \leftarrow H(m)$
- $b \leftarrow (e(h, \mathcal{X}) \stackrel{?}{=} e(w, \mathcal{G}))$

とし, b を出力する.

署名検証 2: 文書 m, 署名 (w, σ), 公開鍵 y.

- $h \leftarrow H(m)$
- $b \leftarrow V\{(x) : y = g^x \wedge w = h^x\}(\sigma)$

とし, b を出力する.

2.4 [SHK07] のリング署名方式

著者らは [SHK07] にてグループ署名とリング署名の中間的な特徴を持った署名を提案している. このリング署名は 鍵生成, 署名, 検証, オープンの 4 つのアルゴリズムで構成される. その概要は以下のようになる.

鍵生成: 基本署名方式と同じ.

署名生成: 同じメッセージに対する複数のリング署名から, リング署名の匿名性が壊れる事を防ぐ為, 署名者は署名すべき文書に乱数を付加し m を決める[1]. さらに署名者は, 自分を含むリング L を決め, L, m および秘密鍵 x_j, および公開鍵 $\{y_i\}_{i\in L}$ を入力とし, 基本署名方式で知識証明を実行している部分に Cramer-Damgård-Schoenmakers の部分知識証明 [CDS94] を組み合わせリング署名 (w, σ) を生成する. 即ち

$$\sigma \leftarrow P\{(x_i)_{i\in L} : \vee_{i\in L}(y_i = g^{x_i} \wedge w = h^{x_i})\}$$

署名検証: 検証者はリング L, 乱数を含む文書 m, 公開鍵 $\{y_j\}_{j\in L}$ およびリング署名 (w, σ) を入力として, $b \in \{0, 1\}$ を出力する ($b = 0$ は拒絶, $b = 1$ は受理の意味).

$$b \leftarrow V\{(x_i)_{i\in L} : \vee_{i\in L}(y_i = g^{x_i} \wedge w = h^{x_i})\}(\sigma)$$

オープン: グループ管理者はメッセージ m , リング L , 公開鍵 $\{y_j\}_{j\in L}$, グループ管理鍵 $\{\mathcal{X}_j\}_{j\in L}$, およびリング署名 σ を入力として, 署名者

$$j \in L \text{ s.t. } e(w, \mathcal{G}) = e(h, \mathcal{X}_j)$$

を出力する.

このグループ管理者付きリング署名について次の安全性が示された [SHK07].

correctness: リングに含まれる者が正しく作成した署名は検証にて圧倒的確率で受理される.

unforgeability: リングに含まれない者が現実的な時間の内に作成した署名は検証にて圧倒的確率で拒絶される.

anonymity: グループ管理鍵を持たない者がリングの誰が署名を作成したかに関する非自明な情報を現実的な時間の内に取得できる確率は無視しうる.

exculpability: 受理されるリング署名に対してオープンの出力が署名作成者と異なる確率は無視しうる.

[1] リングのメンバによる対話的あるいは非対話的な deniability は許容する.

3 フレキシブルリング署名

本論文で提案するフレキシブルリング署名は, 以下の 4 つのアルゴリズムの組 $\Sigma = (\text{KeyGen}, \text{Sign}, \text{Relink}, \text{Verify})$ で, correctness と, 以下の 4 つの安全性の条件, unforgeability, relinker unforgeability, traceability, anonymity, を満たすものである.

以下では, リングメンバー集合 L は全署名者の集合 $P = \{0, 1, ...\}$ の部分集合, PK は全署名者の公開鍵の集合 $\{pk_0, pk_1, ...\}$, とする.

鍵生成 $\text{KeyGen}(k) \rightarrow (pk_i, rk_i, sk_i)$**:** 鍵生成アルゴリズム KeyGen は, セキュリティパラメタ k を入力され, 署名者 i の署名鍵 sk_i と再リンク鍵 rk_i と公開鍵鍵 pk_i を出力する.

署名生成 $\text{Sign}(PK, sk_i, L, m) \rightarrow s$**:** 署名生成アルゴリズム Sign は, 全署名者の公開鍵の集合 PK と署名者 i の署名鍵 sk_i とリングメンバー集合 L $(i \in L)$ とメッセージ m を入力され, 署名 s を出力する.

再リンク $\text{Relink}(PK, rk_i, L, m, s, L') \rightarrow s'$**:** 再リンクアルゴリズム Sign は, 全署名者の公開鍵の集合 PK と署名者 i の再リンク鍵 rk_i とリングメンバー集合 L $(i \in L)$ とメッセージ m と署名 s とリングメンバー集合 L' $(i \in L')$ を入力され, 署名 s' を出力する.

署名検証 $\text{Verify}(PK, L, m, s) \rightarrow OK/NG$**:** 署名検証アルゴリズム Verify は, 全署名者の公開鍵の集合 PK とリングメンバー集合 L とメッセージ m と署名 s を入力され, OK または NG を出力する.

フレキシブルリング署名は, 正しく生成し再リンクした署名は正しく検証されるという以下の性質を満たす.

correctness: 鍵生成 $\text{KeyGen}(k) \rightarrow (pk, rk, sk)$ を行い, 署名生成 $\text{Sign}(PK, sk_i, L, m) \rightarrow s$ s.t. $i \in L$ を行い, 再リンク $\text{Relink}(PK, rk_i, L, m, s, L') \rightarrow s'$ s.t. $i \in L, i \in L'$ を 0 回以上を行うと, $\text{Verify}(PK, L', m, s') \rightarrow OK$ となる.

フレキシブルリング署名は, 部外者による新しいリングもしくは新しいメッセージに対する署名偽造攻撃をモデル化した以下の性質を満たす.

unforgeability: 攻撃者 A が行う以下のゲームを考える. 攻撃者 A は, pk_i $(i = 0, 1, ..., n-1)$ を与えられる. 攻撃者 A は, 鍵生成 $\text{KeyGen}(k) \rightarrow (pk_i, rk_i, sk_i)$ $(i = n, n+1, ...)$ を行い, 全署名者の集合 P に i を, 全署名者の公開鍵の集合 PK に生成した公開鍵 pk_i を, 追加することができる. 攻撃者 A は,$i = 0, 1, ..., n-1$ について, signing oracle $\text{SO}(PK, i, L, m)$ $i \in L$ と

relink oracle $\mathrm{RO}(PK, i, L, m, s, L')$ $i \in L, i \in L'$ とに質問し回答を得ることができる.

攻撃者 A が, 署名 (L^*, m^*, s^*) を出力し, 1.Verify $(PK, L^*, m^*, s^*) \to OK$ であり, 2.(L^*, m^*, s^*) は SO, RO の回答でなく, 3.$L^* \subset \{0, ..., n-1\}$ である, 確率を $Adv^{\mathrm{uf}}_{\Sigma,A}$ とする.

全ての確率的多項式時間攻撃者 A に対して, $Adv^{\mathrm{uf}}_{\Sigma,A}$ が無視できるとき, Σ は unforgeable であるという.

フレキシブルリング署名は, 再リンク者による新しいメッセージに対する署名偽造攻撃をモデル化した以下の性質を満たす.

relinker unforgeability: 攻撃者 A が行う以下のゲームを考える. 攻撃者 A は, pk_i, rk_i $(i = 0, 1, ..., n-1)$ を与えられる. 攻撃者 A は, 鍵生成 $\mathrm{KeyGen}(k) \to (pk_i, rk_i, sk_i)$ $(i = n, n+1, ...)$ を行い, 全署名者の集合 P に i を, 全署名者の公開鍵の集合 PK に生成した公開鍵 pk_i を, 追加することができる. 攻撃者 A は,$i = 0, 1, ..., n-1$ について, signing oracle $\mathrm{SO}(PK, i, L, m)$ $i \in L$ に質問し回答を得ることができる.

攻撃者 A が, 署名 (L^*, m^*, s^*) を出力し, 1.Verify $(PK, L^*, m^*, s^*) \to OK$ であり, 2.m^* は SO への質問でなく, 3.$L^* \subset \{0, ..., n-1\}$ である, 確率を $Adv^{\text{r-uf}}_{\Sigma,A}$ とする.

全ての確率的多項式時間攻撃者 A に対して, $Adv^{\text{r-uf}}_{\Sigma,A}$ が無視できるとき, Σ は relinker unforgeable であるという.

フレキシブルリング署名は, 署名者特定のできない署名偽造攻撃をモデル化した以下の性質を満たす.

traceability: 攻撃者 A が行う以下のゲームを考える. 攻撃者 A は, pk_i, rk_i $(i = 0, 1, ..., n-1)$ を与えられる. 攻撃者 A は, 鍵生成 $\mathrm{KeyGen}(k) \to (pk_i, rk_i, sk_i)$ $(i = n, n+1, ...)$ を行い, 全署名者の集合 P に i を, 全署名者の公開鍵の集合 PK に生成した公開鍵 pk_i を, 追加することができる.

攻撃者 A が, 署名 (L^*, m^*, s^*) を出力し, 1.Verify $(PK, L^*, m^*, s^*) \to OK$ であり, 2. すべての $i \in L \cap \{n, n+1, ...\}$ に対して $\mathrm{Relink}(PK, rk_i, L^*, m^*, s^*, \{i\}) \to s_i^*$ かつ Verify $(PK, \{i\}, m^*, s_i^*) \to NG$ である, 確率を $Adv^{\mathrm{trace}}_{\Sigma,A}$ とする.

全ての確率的多項式時間攻撃者 A に対して, $Adv^{\mathrm{trace}}_{\Sigma,A}$ が無視できるとき, Σ は traceable であるという.

フレキシブルリング署名は, 部外者による署名者特定攻撃をモデル化した以下の性質を満たす.

anonymity: 攻撃者 A が行う以下のゲームを考える. 攻撃者 A は, pk_i $(i = 0, 1, ..., n-1)$ を与えられる. 攻撃者 A は, 鍵生成 $\mathrm{KeyGen}(k) \to (pk_i, rk_i, sk_i)$ $(i = n, ...)$ を行い, 全署名者の集合 P に i を, 全署名者の公開鍵の集合 PK に生成した公開鍵 pk_i を, 追加することができる. 攻撃者 A は,$i = 0, 1, ..., n-1$ について, signing oracle $\mathrm{SO}(PK, i, L, m)$ $i \in L$ と relink oracle $\mathrm{RO}(PK, i, L, m, s, L')$ $i \in L, i \in L'$ とに質問し回答を得ることができる.

攻撃者 A は, i_0, i_1, L^* s.t. $i_0, i_1 \in L^* \subset \{0, 1, ..., n-1\}$) と m^* を選んで, $s_b = \mathrm{Sign}(PK, sk_{i_b}, L^*, m^*)$ $b \in_U \{0, 1\}$ を与えられる.

以降, 攻撃者 A は, relink oracle $\mathrm{RO}(PK, i, L, m, s, L')$ に, $\{i_0, i_1\} \not\subset L^*$ となる L^* と m^* と s_b を質問できない.

攻撃者 A が, b' を出力し, $Adv^{\mathrm{anon}}_{\Sigma,A} = |Pr[b' = b] - 1/2|$ とする.

全ての確率的多項式時間攻撃者 A に対して, $Adv^{\mathrm{anon}}_{\Sigma,A}$ が無視できるとき, Σ は anonymous であるという.

4 提案方式

[SHK07] では秘密鍵を持つ署名者だけが 2 通りの DDH-tuple への所属証明を行う事が出来た. 本提案法では, この制限を少し緩和し Chaum-Pederson のプロトコル [CP92] を署名者だけでなく, TTP も実行可能であるように改造する. 即ち, 離散対数 x を知る者が証明者となる知識の証明

$$PK\{(x) : y = g^x \wedge w = h^x\}$$

を実行する代わりに, $\mathcal{X} = \mathcal{G}^x$ を知る者が証明者となり知識の証明

$$PK\{(\mathcal{X}) : e(y, \mathcal{G}) = e(g, \mathcal{X}) \wedge e(w, \mathcal{G}) = e(h, \mathcal{X})\}$$

を実行するのである. 公開鍵 $pk = y = g^x$ から証明作成鍵 $rk = \mathcal{X} = \mathcal{G}^x$ を, 証明作成鍵 $rk = \mathcal{X} = \mathcal{G}^x$ から秘密鍵 $sk = x$ を, 求めることは計算量的に困難なので, リングを作成する能力を署名を作成する能力から完全に分離でき, リングを編集する能力だけをグループ管理者に渡すことが可能となる.

以下では, $\mathcal{G} \in G_1$ および $g \in G_2$ を生成元, $H, H' : \{0,1\}^* \to G_2$ をハッシュ関数とする.

4.1 提案方式の基本署名方式

提案基本署名方式は, 以下の非対話証明を用いる.

$P\{(\mathcal{X}) : e(y, \mathcal{G}) = e(g, \mathcal{X}) \wedge e(w, \mathcal{G}) = e(h, \mathcal{X})\}$: $g, y, h, w \in G_2, \mathcal{X} \in G_1$ を入力として,

- $t \in_U \mathbb{Z}/\ell\mathbb{Z}, T \leftarrow (e(g^t, \mathcal{G}), e(h^t, \mathcal{G}))$,
- $c \leftarrow H'(g, y, h, w, T)$,
- $\mathcal{Z} \leftarrow \mathcal{G}^t \mathcal{X}^{-c}$,

を計算し, 証明 $\sigma = (c, \mathcal{Z})$ を出力する.

$V\{(\mathcal{X}) : e(y,\mathcal{G}) = e(g,\mathcal{X}) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X})\}$**:** 証明 $\sigma = (c, \mathcal{Z})$ を入力として,

- $(c, \mathcal{Z}) \leftarrow \sigma, T \leftarrow (e(g,\mathcal{Z})e(y,\mathcal{G})^c, e(h,\mathcal{Z})e(w,\mathcal{G})^c)$
- $b \leftarrow (c \stackrel{?}{=} H'(g,y,h,w,T))$,

を計算し, 検証結果 b を出力する.

提案基本署名方式は, 以下のようになる.

鍵生成: 署名生成鍵 $sk = x \in_U \mathbb{Z}/\ell\mathbb{Z}$, 証明生成鍵 $rk = \mathcal{X} = \mathcal{G}^x \in G_1$, 公開鍵 $pk = y = g^x \in G_2$ を計算し, 出力する.

署名生成: 文書 m, 秘密鍵 $x \in \mathbb{Z}/\ell\mathbb{Z}$ を入力とし,

- $h \leftarrow H(m)$
- $w \leftarrow h^x$
- $\sigma \leftarrow P\{(\mathcal{X}) : e(y,\mathcal{G}) = e(g,\mathcal{X}) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X})\}$

を計算し, 署名 $s = (w, \sigma)$ を出力する.

署名検証: 文書 m, 署名 $s = (w, \sigma)$, 公開鍵 $y = g^x$ を入力とし,

- $h \leftarrow H(m)$
- $b \leftarrow V\{(\mathcal{X}) : e(y,\mathcal{G}) = e(g,\mathcal{X}) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X})\}(\sigma)$

を計算し, 署名検証結果 b を出力する.

4.2 提案方式のリング署名方式

つぎに, 上記方法をリング署名に適用することにより, 以下のように提案フレキシブルリング署名方式を構成することができる. 基本的には上記の [SHK07] の方法と全く同様に, 基本署名方式で知識証明を実行している部分に Cramer-Damgård-Schoenmakers の部分知識証明 [CDS94] を組み合わせリング署名 (w, σ) を生成する. 但しこの方式にはグループ管理者がリング署名の参加メンバを変更したり, リング署名を普通の署名に変換したりできる “再リンク” なる手続きが存在する.

提案フレキシブルリング署名方式は, 以下の非対話証明を用いる.

$P\{(\mathcal{X}_i)_{i\in L} : \vee_{i\in L}(e(y_i,\mathcal{G}) = e(g,\mathcal{X}_i) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X}_i))\}$**:** $g, (y_i)_{i\in L}, h, w \in G_2, \mathcal{X}_j \in G_1$ を入力として,

- $t \in_U \mathbb{Z}/\ell\mathbb{Z}, T_j \leftarrow (e(g^t,\mathcal{G}), e(h^t,\mathcal{G}))$,
- $\forall i \in L \setminus \{j\}, c_i \in_U \mathbb{Z}/\ell\mathbb{Z}, \mathcal{Z}_i \in_U G_1$, $T_i \leftarrow (e(g,\mathcal{Z}_i)e(y,\mathcal{G})^{c_i}, e(h,\mathcal{Z}_i)e(w,\mathcal{G})^{c_i})$,
- $c_j \leftarrow H'(g,h,w,(y_i,T_i)_{i\in L}) - \Sigma_{i\in L\setminus\{j\}} c_i$,
- $\mathcal{Z}_j \leftarrow \mathcal{G}^t \mathcal{X}^{-c_j}$,

を計算し, 証明 $\sigma = (c_i, \mathcal{Z}_i)_{i\in L}$ を出力する.

$V\{(\mathcal{X}_i)_{i\in L} : \vee_{i\in L}(e(y_i,\mathcal{G}) = e(g,\mathcal{X}_i) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X}_i))\}$**:** 証明 $\sigma = (c_i, \mathcal{Z}_i)_{i\in L}$ を入力として,

- $\forall i \in L, T_i \leftarrow (e(g,\mathcal{Z}_i)e(y,\mathcal{G})^{c_i}, e(h,\mathcal{Z}_i)e(w,\mathcal{G})^{c_i})$,
- $b \leftarrow (\Sigma_{i\in L} c_i \stackrel{?}{=} H'(g,h,w,(y_i,T_i)_{i\in L}))$,

を計算し, 検証結果 b を出力する.

提案フレキシブルリング署名方式は, 以下のようになる.

鍵生成: 署名生成鍵 $sk_i = x_i \in_U \mathbb{Z}/\ell\mathbb{Z}$, 再リンク鍵 $rk_i = \mathcal{X}_i = \mathcal{G}^{x_i} \in G_1$, 公開鍵 $pk_i = y_i = g^{x_i} \in G_2$ を計算し, 出力する.

署名生成: 文書 m, 秘密鍵 $sk_j = x_j$ を入力とし,

- $r \in_U \{0,1\}^k$, $h \leftarrow H(m||r)$,
- $w \leftarrow h^{x_j}$,
- $\sigma \leftarrow P\{(\mathcal{X}_i)_{i\in L} : \vee_{i\in L}(e(y_i,\mathcal{G}) = e(g,\mathcal{X}_i) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X}_i))\}$,

を計算し, 署名 $s = (r, w, \sigma)$ を出力する.

署名検証: 文書 m, 署名 $s = (r, w, \sigma)$, 公開鍵 $\{pk_0, pk_1, ...\}$ を入力とし,

- $h \leftarrow H(m||r)$,
- $b \leftarrow V\{(\mathcal{X}_i)_{i\in L} : \vee_{i\in L}(e(y_i,\mathcal{G}) = e(g,\mathcal{X}_i) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X}_i))\}$,

を計算し, 署名検証結果 b を出力する.

再リンク: 文書 m, 署名 $s = (r, w, \sigma)$, 新しいリング L', 再リンク鍵 $rk_j = \mathcal{G}^{x_j}$ を入力とし,

- $h \leftarrow H(m||r)$,
- $\sigma' \leftarrow P\{(\mathcal{X}_j) : \vee_{i\in L'}(e(y_i,\mathcal{G}) = e(g,\mathcal{X}_i) \wedge e(w,\mathcal{G}) = e(h,\mathcal{X}_i))\}$

を計算し, 署名 $s' = (r, w, \sigma')$ を出力する.

提案フレキシブルリング署名方式は, correctness を満たし, 以下のように 4 つの安全性の条件をみたす.

定理 (unforgeability): G_2 から G_1 へのスキュー CDH 問題が困難であるなら, ランダムオラクルモデルにおいて, 本論文で提案したリング署名は強偽造不可能性を満足する.

定理 (relinker unforgeability): ヒント付きの G_2 上の CDH 問題が困難であるなら, ランダムオラクルモデルにおいて, 本論文で提案したリング署名は弱偽造不可能性を満足する.

定理 (traceability): ランダムオラクルモデルにおいて, 本論文で提案したリング署名は追跡不可能性を満足する.

定理 (anonymity): G_2 上の DDH 問題が困難であるなら, ランダムオラクルモデルにおいて, 本論文で提案したリング署名は匿名性を満足する. [2]

5 アプリケーション

リング署名のリングを作成する為の鍵 $\mathcal{X}$ を署名を作成できる鍵 x から分離する事が出来た. これにより x は持たないが $\mathcal{X}$ を持つ信頼できるグループ管理者がリング署名の参加メンバを変更したりリング署名を普通の署名に変換する事が可能となる.

例えば, ある部署でメンバが変更になった場合,$\mathcal{X}$ を持つ管理者は, 既に生成されたリング署名を再リンクすることにより, その部署の現在のメンバに合わせてリングメンバを修正することができる. しかし,x を持たない管理者は, 新しいメッセージにリング署名を打つことはできないので, 署名作成権限を与えずに, メンバ変更に対応することができる.

6 まとめ

本論文では,[SHK07] の署名方式を改造して署名者がリング署名を生成した後にグループ管理者がリング署名の参加メンバを変更したりリング署名を普通の署名に変換したりできる事を実現した.

参考文献

[CH91] David Chaum and Eugène van Heyst,"Group Signatures," In Proceedings of Donald W. Davies ed., Advances in Cryptology - EUROCRYPT'91, volume 547 of LNCS, pages 257-265, Springer-Verlag, 1991.

[RST01] Ronald L. Rivest, Adi Shamir and Yael Tauman, "How to Leak a Secret," In Proceedings of Colin Boyd (Ed.), Advances in Cryptology - ASIACRYPT 2001, volume 2248 of LNCS, pages 552-565, Springer-Verlag, 2001.

[SHK07] Koutarou Suzuki, Fumitaka Hoshino and Tetsutaro Kobayashi, "Revocable Ring Signature using Revocable DDH Assumption," In Proceedings of SCIS 2007, The 2007 Symposium on Cryptography and Information Security, Sasebo, Japan, Jan. 23-26, 2007, The Institute of Electronics, Information and Communication Engineers.

[CP92] David Chaum and Torben Pryds Pedersen, "Wallet databases with observers," In Proceedings of Advances in Cryptology - CRYPTO'92, volume 740 of LNCS, pages 89-105, Springer-Verlag, 1992.

[CS97] Jan Camenisch and Markus Stadler, "Efficient group signature schemes for large groups," In Proceedings of Advances in Cryptology - CRYPTO'97, volume 1294 of LNCS, pages 410-424, Springer-Verlag, 1997.

[SHUK03] Taiichi Saito, Fumitaka Hoshino, Shigenori Uchiyama and Tetsutaro Kobayashi, "Candidate One-Way Functions on Non-Supersingular Elliptic Curves," 5th Symposium on Algebra and Computation, ftp://tnt.math.metro-u.ac.jp/pub/ac03/Saitoh/saitoh-oneway.pdf

[HSK05] Fumitaka Hoshino, Koutarou Suzuki and Tetsutaro Kobayashi, "Revocable DDH by using Pairing and It's Application," In Proceedings of SCIS 2005, The 2005 Symposium on Cryptography and Information Security, Maiko Kobe, Japan, Jan. 25-28, 2005, The Institute of Electronics, Information and Communication Engineers, (in Japanese).

[MNT01] A.Miyaji, M.Nakabayashi and S.Takano, "New explicit conditions of elliptic curve traces for FRReduction," IEICE Trans. Fundamentals, vol.E84-A, no.5, pp.1234-1243, May 2001

[JN01] A.Joux and K.Nguyen ,"Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups," http://eprint.iacr.org/2001/003/

[BLS01] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," In Proceedings of Colin Boyd ed., Advances in Cryptology - ASIACRYPT 2001, volume 2248 of LNCS, pages 514-532, Springer-Verlag, 2001.

[FS86] Amos Fiat and Adi Shamir, "How to prove yourself: Practical solutions to identification and signature problems," In Proceedings of A.M.Odlyzko ed., Advances in Cryptology - CRYPT0'86, volume 263 of LNCS, pages 186-194, Springer-Verlag, 1986.

[CDS94] Ronald Cramer, Ivan Damgård and Berry Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," In Proceedings of Advances in Cryptology - CRYPTO'94, volume 839 of LNCS, pages 174-187, Springer-Verlag, 1994.

[KOSK06] Yuichi Komano, Kazuo Ohta, Atsushi Shimbo, and Shinichi Kawamura, "Toward the Fair Anonymous Signatures: Deniable Ring Signatures," D. Pointcheval (Ed.): CT-RSA 2006, LNCS 3860, pp.174-191, 2006, Springer-Verlag, Berlin Heidelberg, 2006.

[2] 同じ署名に対して再リンクを何度も繰り返したとき, リングの履歴が $L_0, L_1, ..., L_n$ であるなら, 匿名性は $\cap_i L_i$ 内に限定される. 署名の履歴がすべて記録されるようなモデルでは, 再リンクにより匿名性は必ず減少する. 署名の記憶領域が有限であるようなモデルなら, 匿名性が増加することはあり得る.