SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

エージェント指定匿名化可能署名
Designated Agent Anonymizable Signature

小林 鉄太郎 *　　星野 文学 *
Tetsutaro Kobayashi　　Fumitaka Hoshino

あらまし 匿名化可能署名 (Anonymizable Signature) とはリング署名の拡張であり, 匿名化可能署名を用いると署名されたメッセージを持つ者は, 誰でも後からその署名を匿名署名に変換できる. 本発表では, 匿名化可能署名を匿名化する前の時点で検証できる者を限定化する, という拡張を行った. この拡張により, 匿名化前の署名が流出した場合のリスクを軽減することが可能となる.

キーワード キーワード

1 Introduction

匿名化可能署名 (Anonymizable Signature) とは リング署名 (Ring Signature) [4, 5] の拡張である.

匿名化可能署名を用いることで, 任意のエンティティが通常の署名から匿名署名に変換することができる. 言い換えると, 署名を代理人に託し, 匿名化を依頼することが可能である.

類似の研究に, 再リンク可能リング署名 (Relinkable Ring Signature) [3] という, リング署名の拡張となる署名方式があった. 再リンク可能リング署名は, 特殊な鍵を持つ代理人がリング署名の構成員（リング）を変更可能であり, 匿名性を必要とするプロトコルへの応用を想定したものである. この方式の欠点は, 公開鍵を作成した時点でリング構成員を変更する特殊な鍵も生成されるため, 署名者が署名ごとに代理人を選択することが出来ない点と, 代理人が正直であったとしても完全な匿名性を達成することが出来ない点である.

これに対し, 匿名化可能署名 [1] が, 再リンク可能リング署名の問題点を解決する方式として提案されている. 一切の秘密情報を用いずに署名を匿名署名に変換することが出来る. 匿名化可能署名は無条件の匿名性を保証することができるため, 電子投票などの高い匿名性が求められる用途に用いることが出来る.

匿名化可能署名に残存する課題として, 匿名化する前の署名が通常の署名であるため, 誰でも検証可能という点がある. 匿名化可能署名の典型的な利用法に電子投票の利用法があり, 以下の手順となる.

1. 投票者が投票内容に署名を行い, 投票箱に送信する
2. 投票箱は署名検証を行い, 投票を蓄積する
3. 投票が締め切られた時点で, 投票箱が匿名化を行い, 掲示板に掲示する
4. 集計者が匿名署名の検証および票の集計を行う

この際, Step 2 の段階で蓄積してある署名が漏洩した場合, 投票の秘密が暴露されてしまうという問題がある. この問題は投票の署名は投票箱のみが検証できるだけで十分であるのに, 他のエンティティが検証できてしまうことが原因で発生している. そこで, 検証者を限定できれば, 投票が漏洩した際のリスクを減らすことができる.

このような問題を解決するため, 本稿ではエージェント指定匿名化可能署名を定義し, Decisional Diffie-Hellman 仮定のもとで安全な方式を示す.

基本的なアイデアとしては, 匿名化可能署名 [1] を拡張し, Trapdoor-DDH 群 [2] を応用することで, 署名部分を検証者指定可能署名に変更することで実現している.

1.1 Related Works

1.1.1 匿名化可能署名

匿名化可能署名 [1] はリング署名の拡張であり, 匿名化可能署名を用いると署名されたメッセージを持つ者は, 誰でも後からその署名を匿名署名に変換できる. 即ち, 署名者は適切なエージェントに署名を渡しておけば, 後で自分が匿名化に関与する必要が無い. $k \in \mathbb{N}$ を安全パラメタとし, $N = \{0, 1, \cdots\}$ を署名者集合とする. 署

* NTT セキュア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. NTTSecure Platform Laboratories 3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, Japan. kobayashi.tetsutaro@lab.ntt.co.jp

名者 i の秘密鍵を x_i, 公開鍵を y_i とする. 署名者の部分集合 $L \subset N$ はリングと呼ばれる. 記述を簡単にするため, リング L に対して a_L を $a_L = (a_i)_{i \in L}$ と定義する. 匿名化可能署名方式 Σ は次の構文を満たす 4 つの確率的多項式時間アルゴリズム ($\mathtt{KeyGen}, \mathtt{Sign}, \mathtt{Anonymize}, \mathtt{Verify}$) により構成される.

鍵生成アルゴリズム $\mathtt{KeyGen}(1^k) \xrightarrow{\$} (x, y)$: は安全パラメタ 1^k を入力とし秘密鍵 x および公開鍵 y を出力とする確率的多項式時間アルゴリズム.

署名アルゴリズム $\mathtt{Sign}(x, m) \xrightarrow{\$} r$: は秘密鍵 x およびメッセージ m を入力とし署名 r を出力とする確率的多項式時間アルゴリズム.

匿名化アルゴリズム $\mathtt{Anonymize}(i, r, L, y_L, m) \xrightarrow{\$} \sigma/\perp$: は署名者 ID i, 署名 r, リング $L \subset N$, 公開鍵リスト y_L, およびメッセージ m を入力とし, リング署名 σ または拒絶 $\perp$ を出力とする確率的多項式時間アルゴリズム.

検証アルゴリズム $\mathtt{Verify}(L, y_L, m, \sigma) \xrightarrow{\$} 0/1$: はリング $L \subset N$, 公開鍵リスト y_L, メッセージ m, およびリング署名 σ, を入力とし, 単一ビット $b \in \{0, 1\}$ を出力とする確率的多項式時間アルゴリズム.

構文 : 如何なる (多項式長の) メッセージ $m \in \{0,1\}^*$, 如何なる (多項式長の) リング $L \subset N$, および如何なる署名者 $i \in L$ に対しても

$$\Pr[\mathtt{Verify}(L, y_L, m, \mathtt{Anonymize}(\mathtt{Sign}(x_i, m), L, y_L, m)) = 0 \mid \forall j \in L, (x_j, y_j) \xleftarrow{\$} \mathtt{KeyGen}(1^k)]$$

が k に関して無視可能.

署名者の匿名性を壊さないよう署名 r は署名者とエージェントの間の秘密としなければならない.

1.1.2 匿名化可能署名の具体的構成

文献 [1] では次のようなペアリングを用いた匿名化可能署名の具体的構成が与えられている.

$\mathbb{G}$ および $\mathbb{G}_T$ を素数位数 p を持つ巡回群とし $\mathbb{G}^*$ を $\mathbb{G}$ の生成元全体とし $g \in \mathbb{G}^*$ とする. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ を非退化双順同型, $H : \{0,1\}^* \to \mathbb{G}^*$ および $H' : \{0,1\}^* \to \mathbb{F}_p$ を互いに独立なランダムオラクルとする. $\rho = (\mathbb{G}, \mathbb{G}_T, e, g, H, H')$ をシステムパラメタと呼ぶ. システムパラメタは方式に参加するすべての参加者が知っている共通参照文字列で, 例えば匿名化エージェントが設定して良い.

$\mathtt{KeyGen}(1^k)$: $x \xleftarrow{\$} \mathbb{F}_p$, $y \leftarrow g^x$ return (x, y)

$\mathtt{Sign}(x, m)$: return $\sigma \leftarrow H(\rho, m)^x$

$\mathtt{Anonymize}(i, r, L, y_L, m)$: $h \leftarrow H(\rho, m)$ if $e(g, r) \neq e(y_i, h)$ return $\perp$ $(\exists j \in L, r = h^{x_j})$ なる r の知識証明を次のように生成する: $t \xleftarrow{\$} \mathbb{F}_p$ $\tilde{a}_i \leftarrow e(g, h)^t$ $\forall j \in L \setminus \{i\}$ $c_j \xleftarrow{\$} \mathbb{F}_p$ $z_j \xleftarrow{\$} \mathbb{G}$ $\tilde{a}_j \xleftarrow{\$} e(g, z_j)e(h, y_j)^{c_j}$ $c_i \leftarrow H'(\rho, L, m, y_L, \tilde{a}_L) - \sum_{j \neq i} c_j$ $z_i \xleftarrow{\$} h^t r^{-c_i}$ return $\sigma \leftarrow (c_L, z_L)$

$\mathtt{Verify}(L, y_L, m, \sigma)$: $(c_L, z_L) \leftarrow \sigma$ $h \leftarrow H(\rho, m)$ $\forall j \in L, \tilde{a}_j \leftarrow e(g, z_j)e(h, y_j)^{c_j}$ return

1 if $H'(\rho, L, m, y_L, \tilde{a}_L) = \sum_{j \in L} c_j$,

0 otherwise.

2 Definition

2.1 Trapdoor DDH

[2] にはペアリングを拡張した特殊な trapdoor DDH 群の具体的構成が示されている. 本稿ではエージェント指定匿名化可能署名の具体的構成を与えるためこれを用いる.[2] の trapdoor DDH 群の具体的構成を要約すると, およそ次のようになる.

- p を十分大きい素数とする.
- E を $\mathbb{F}_p$ 上の超特異楕円曲線とし, 位数が十分大きい素数 q で割り切れる.
- α を $E(\mathbb{F}_p)[q]$ の生成元とする.
- $\mathbb{G} := \mathbb{GL}(n, \langle\alpha\rangle) \subseteq \langle\alpha\rangle^{n \times n}$.
- Ł $:= \mathbb{GL}(n, \mathbb{F}_q) \subseteq \mathbb{F}_q^{n \times n}$.
- $\mathbb{G}$ は成分毎の楕円加算を群演算とするアーベル群で, これを trapdoor DDH 群と見なす.
- 非可換環 Ł を $\mathbb{G}$ に関する離散対数と見なし, 鍵交換が可能である (後述).
- $\mathbb{G}$ 上で自然なペアリングが定義される (後述).

2.2 離散対数

本稿で使用する特殊な離散対数問題を定義する.

- 巡回群 $\langle\alpha\rangle$, 位数 q (素数) とする.
- $h := (\alpha^{r_{ij}})$ に対する離散対数 $r := (r_{ij})$ を以下のように定義する. $\langle\alpha\rangle^{n \times n} \to \mathbb{F}_q^{n \times n}$

$$\begin{pmatrix} \alpha^{r_{11}} & \dots & \alpha^{r_{1n}} \\ \vdots & \ddots & \vdots \\ \alpha^{r_{n1}} & \dots & \alpha^{r_{nn}} \end{pmatrix} \mapsto \begin{pmatrix} r_{11} & \dots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \dots & r_{nn} \end{pmatrix}$$

- この場合, h を α^r と書く.
- r が $n \times n$ 単位行列の時は α^r を I_n と書く.

- $\mathbb{GL}(n, \langle\alpha\rangle)$: 離散対数が正則な $\langle\alpha\rangle^{n\times n}$ の部分群と定義する.

  例: $n = 2$ の場合, G の元の加算は以下のように表現できる.

- $g := \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathbb{G},\ h := \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \in \mathbb{G}$

- $g + h = h + g = \begin{pmatrix} g_{11}+h_{11} & g_{12}+h_{12} \\ g_{21}+h_{21} & g_{22}+h_{22} \end{pmatrix} \in \mathbb{G},$

- 本稿では, 今後アーベル群 G を乗法表記を行い, 上記の加算を以下のような表現で表す

  $$gh = hg = \begin{pmatrix} g_{11}h_{11} & g_{12}h_{12} \\ g_{21}h_{21} & g_{22}h_{22} \end{pmatrix} \in \mathbb{G},$$

2.3 右冪乗・左冪乗

- Ł が非可換環
- Ł と $\mathbb{G}$ との間の対応

$$\begin{array}{ccccccc} x & = & x_1x_2 & = & x_1x_2 & \in & Ł \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ g & = & {}^{x_1}g_2 & = & g_1^{x_2} & \in & \mathbb{G} \end{array}$$

Definition 1 左冪乗・右冪乗 $Ł$ が非可換環の時, $[\mathbb{G}, Ł]$ は `pow` の代わりに下記の確率的多項式時間アルゴリズムを含むとする.

- $\mathbb{G}, Ł$ に関する非退化双準同型
  - `rpow` : $\mathbb{G} \times Ł \to \mathbb{G}$, 右冪乗, および
  - `lpow` : $Ł \times \mathbb{G} \to \mathbb{G}$, 左冪乗 *(*どちらも結合律を満たす*)*.

2.4 左冪乗・右冪乗の具体例

- 離散対数上の行列乗算と考える $({}^x(\alpha^y) = \alpha^{xy},\ (\alpha^y)^x = \alpha^{yx})$
- $x := \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in Ł \subseteq \mathbb{F}_q^{2\times 2}$
- $g := \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathbb{G} \subseteq \langle\alpha\rangle^{2\times 2}$
- 乗法表示すると
- ${}^xg := \begin{pmatrix} g_{11}^{x_{11}}g_{21}^{x_{12}} & g_{12}^{x_{11}}g_{22}^{x_{12}} \\ g_{11}^{x_{21}}g_{21}^{x_{22}} & g_{12}^{x_{21}}g_{22}^{x_{22}} \end{pmatrix} \in \mathbb{G}$
- $g^x := \begin{pmatrix} g_{11}^{x_{11}}g_{12}^{x_{21}} & g_{11}^{x_{12}}g_{12}^{x_{22}} \\ g_{21}^{x_{11}}g_{22}^{x_{21}} & g_{21}^{x_{12}}g_{22}^{x_{22}} \end{pmatrix} \in \mathbb{G}$
- ${}^xI_n = I_n^x = \alpha^x$

2.5 鍵交換

- Alice が $x \in Ł$ を生成し, ${}^xg$ を Bob に送信
- Bob が $y \in Ł$ を生成し, g^y を Alice に送信
- Alice は $K_A = {}^x(g^y)$ を計算
- Bob は $K_B = ({}^xg)^y$ を計算
- K_A と K_B は同じ値となる

2.6 ペアリング

自然なペアリング $e : \langle\alpha\rangle^{n\times n} \times \langle\alpha\rangle^{n\times n} \to \mu_q^{n\times n}$

- 離散対数上の行列乗算と考える $(e(\alpha^x, \alpha^y) = \xi^{xy})$
- $g := \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathbb{G},\ h := \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \in \mathbb{G}$
- ペアリングの定義は $e(g, h) :=$

$$\begin{pmatrix} e(g_{11},h_{11})e(g_{12},h_{21}) & e(g_{11},h_{12})e(g_{12},h_{22}) \\ e(g_{21},h_{11})e(g_{22},h_{21}) & e(g_{21},h_{12})e(g_{22},h_{22}) \end{pmatrix} \in \mu_q^{2\times 2}$$

2.7 Security

エージェント指定匿名化可能署名の安全性は,

- 検証者指定署名としての安全性
- 匿名化可能署名としての安全性

の 2 つに分けて定義される.

検証者指定署名の安全性は [6] で定義されており, 匿名化可能署名の安全性は [1] で定義されている.

検証者指定署名は署名時に検証者を指定する方式であるのに対し, エージェント指定匿名化可能署名は公開鍵生成時にあらかじめ検証者を指定する方式であるため, 似ているが異なる. おおむね同様の安全性評価を行うことができる.

3 Proposed Scheme

3.1 エージェント指定匿名化可能署名

[1] においては署名者がエージェントに渡す署名は通常の署名で誰でもこれが検証出来る事が問題であった. 提案方式は, 匿名化可能署名 [1] の署名方式の定義に `Setup` 関数を追加し, この関数で事前に証明者がエージェント

を指定し, 指定されたエージェントのみが署名検証および匿名化を出来るものとする.

改良された署名方式 Σ は次の構文を満たす 5 つの確率的多項式時間アルゴリズム ($\mathtt{Setup}, \mathtt{KeyGen}, \mathtt{Sign}, \mathtt{Anonymize}, \mathtt{Verify}$) により構成される.

エージェント鍵生成アルゴリズム $\mathtt{Setup}(1^k) \xrightarrow{\$} (w, \rho)$: は安全パラメタ 1^k を入力としエージェント秘密鍵 w およびシステムパラメタ ρ を出力とする確率的多項式時間アルゴリズム.

鍵生成アルゴリズム $\mathtt{KeyGen}(\rho) \xrightarrow{\$} (x, y)$: はシステムパラメタ ρ を入力とし秘密鍵 x および公開鍵 y を出力とする確率的多項式時間アルゴリズム.

署名アルゴリズム $\mathtt{Sign}(x, m) \xrightarrow{\$} r$: は秘密鍵 x およびメッセージ m を入力とし署名 r を出力とする確率的多項式時間アルゴリズム.

匿名化アルゴリズム $\mathtt{Anonymize}(i, r, L, y_L, m) \xrightarrow{\$} \sigma/\perp$: は署名者 ID i, 署名 r, リング $L \subset N$, 公開鍵リスト y_L, およびメッセージ m を入力とし, リング署名 σ または拒絶 $\perp$ を出力とする確率的多項式時間アルゴリズム.

検証アルゴリズム $\mathtt{Verify}(L, y_L, m, \sigma) \xrightarrow{\$} 0/1$: はリング $L \subset N$, 公開鍵リスト y_L, メッセージ m, およびリング署名 σ, を入力とし, 単一ビット $b \in \{0,1\}$ を出力とする確率的多項式時間アルゴリズム.

構文 : 如何なる (多項式長の) メッセージ $m \in \{0,1\}^*$, 如何なる (多項式長の) リング $L \subset N$, および如何なる署名者 $i \in L$ に対しても

$$\Pr\left[\begin{array}{l|l} \mathtt{Verify}(L, y_L, m, \sigma) = 0 & \begin{array}{l}(w,\rho) \xleftarrow{\$} \mathtt{Setup}(1^k),\\ \forall j \in L, (x_j, y_j) \xleftarrow{\$} \mathtt{KeyGen}(\rho),\\ r \xleftarrow{\$} \mathtt{Sign}(x_i, m),\\ \sigma \xleftarrow{\$} \mathtt{Anonymize}(w, r, L, y_L, m),\end{array}\end{array}\right]$$

が k に関して無視可能.

署名者の匿名性を壊さないよう署名 r は署名者とエージェントの間の秘密としなければならないが, r が攻撃者に漏洩しても, エージェント秘密鍵 w が漏洩していなければ r が どの x_i によって作成された署名なのかは計算量的に識別困難とする.

3.2 構成例

$\mathbb{G}$ を上記 Trapdoor-DDH 群とし Ł をその離散対数とし, $\mathbb{G}_T = \mathbb{GL}(n, \langle e(\alpha, \alpha)\rangle)$ とする. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ を上記 Trapdoor-DDH 群のペアリングとする. $H : \{0,1\}^* \to \mathbb{G}$ および $H' : \{0,1\}^* \to$ Ł を互いに独立なランダムオラクルとする. $\rho = (\text{Ł}, \mathbb{G}, \mathbb{G}_T, e, g, H, H')$ をシステムパラメタと呼ぶ.

$\mathtt{Setup}(1^k) : w \xleftarrow{\$} \text{Ł}\ g \leftarrow I_n^w\ \rho \leftarrow (\text{Ł}, \mathbb{G}, \mathbb{G}_T, e, g, H, H')$
return (w, ρ)

$\mathtt{KeyGen}(\rho) : (\text{Ł}, \mathbb{G}, \mathbb{G}_T, e, g, H, H') \leftarrow \rho\ x \xleftarrow{\$} \text{Ł},\ y \leftarrow {}^x g$ return (x, y)

$\mathtt{Sign}(x, m)$: return $\sigma \leftarrow {}^x H(\rho, m)$

$\mathtt{Anonymize}(i, r, L, y_L, m) : h \leftarrow H(\rho, m)$ if $e(I_n, r) \neq e(y_i^{w^{-1}}, h)$ return $\perp$ $(\exists j \in L, e(I_n, r) = e(y_j^{w^{-1}}, h))$ なる $r : y_j^{w^{-1}}$ の知識証明を次のように生成する:
$t_1, t_2, \beta \xleftarrow{\$} \text{Ł}\ U \leftarrow {}^{\beta} e(I_n, r)\ T_{1,i} \leftarrow {}^{t_1} e(I_n, I_n)$
$T_{2,i} \leftarrow {}^{t_2} e(I_n, h)$
$\forall j \in L \setminus \{i\}\ c_j \xleftarrow{\$} \text{Ł}\ z_{1,j} \xleftarrow{\$} \mathbb{G}\ z_{2,j} \xleftarrow{\$} \mathbb{G}\ T_{1,j} \leftarrow e(I_n, z_{1,j})\ {}^{c_j}U\ T_{2,j} \leftarrow e(z_{2,j}, h)\ {}^{c_j}U$
$c_i \leftarrow H'(\rho, L, m, y_L, U, T_{1,L}, T_{2,L}) - \sum_{j \neq i} c_j\ z_{1,i} \leftarrow {}^{t_1} I_n / {}^{c_i \beta} r\ z_{2,i} \leftarrow {}^{t_2} I_n / {}^{c_i \beta} y_j^{w^{-1}}$
return $\sigma \leftarrow (U, c_L, z_{1,L}, z_{2,L})$

$\mathtt{Verify}(L, y_L, m, \sigma) : (U, c_L, z_{1,L}, z_{2,L}) \leftarrow \sigma\ h \leftarrow H(\rho, m)$
$\forall j \in L,\ T_{1,j} \leftarrow e(I_n, z_{1,j})\ {}^{c_j}U,\ T_{2,j} \leftarrow e(z_{2,j}, h)\ {}^{c_j}U$
return $\begin{cases} 1 & \text{if } H'(\rho, L, m, y_L, T_{1,L}, T_{2,L}) = \sum_{j \in L} c_j, \\ 0 & \text{otherwise.} \end{cases}$

4 Conclusion and Future Work

本稿では, 匿名化可能署名を拡張したエージェント指定匿名化可能署名の定義を行い, DDH 仮定で安全な方式を示した.

今回提案した方式は, 公開鍵生成時にエージェントを指定しなければならないため, 異なる主催者の電子投票の際には公開鍵の生成からやりなおす必要がある. 今後の課題は, 署名時にエージェントを指定できるように改良することである.

参考文献

[1] F. Hoshino, T. Kobayashi, and K. Suzuki, "Anonymizable signature and its construction from pairings," Pairing-Based Cryptography - Pairing 2010 - 4th International Conference, Yamanaka Hot Spring, Japan, December 2010. Proceedings, ed. M. Joye, A. Miyaji, and A. Otsuka, Lecture Notes in Computer Science, vol.6487, pp.6277, Springer, 2010.

[2] F. Hoshino, "A Variant of Diffie-Hellman Problem and How to Prove Independency." SCIS 2014 The 31st Symposium on Cryptography and Information Security Kagoshima, Japan, Jan. 21 - 24, 2014.

[3] K. Suzuki, F. Hoshino, T. Kobayashi, “Relinkable Ring Signature.”, CANS 2009. LNCS, vol. 5888, pp. 518536.

[4] R. L. Rivest, A. Shamir, Y. Tauman, “How to Leak a Secret.”, ASIACRYPT 2001. LNCS, vol. 2248, pp. 552565.

[5] A. Bender, J. Katz, R. Morselli, “Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles.”, TCC 2006. LNCS, vol. 3876, pp. 6079.

[6] J. Markus, K. Sako, “esignated Verifier Proofs and Their Applications”, EUROCRYPT 1996. pp. 199205.