SCIS 2010 The 2010 Symposium on Cryptography and Information Security
Takamatsu, Japan, Jan. 19-22, 2010
The Institute of Electronics, Information and Communication Engineers

文書依存再リンク可能リング署名
Message Dependently Relinkable 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 再リンク可能リング署名 [SHK09] とは, 署名生成能力からリング生成能力を分離できる特殊なリング署名である. この署名を用いると, 署名者から特別な秘密 (再リンク鍵) を得た第三者 (代理人) が, 再リンクと呼ばれる手続きにより, 既存のリング署名からメンバーを変更したリング署名を生成する事が出来る. 本論文ではこの署名系が持つ様々な制約を緩和するため, 文書依存再リンク可能リング署名の概念を提案し, その汎用的構成の方法論を与え, 2 つの具体的方式を得た.

キーワード Relinkable Ring Signature, Perfect Anonymity, ID-based Signature

1 はじめに

再リンク可能リング署名 [SHK09] とは, 署名生成能力からリング生成能力を分離できる特殊なリング署名である. この署名を用いると, 署名者から特別な秘密 (再リンク鍵) を得た第三者 (代理人) が, 再リンクと呼ばれる手続きにより, 既存のリング署名からメンバーを変更したリング署名を生成する事が出来る. この署名系は, 通常のリング署名のように高レベルの匿名性を要するアプリケーションに必ずしも向いているとは言えないが, リング署名の依頼計算, 署名者自身の墨塗り, 動的グループのリング署名, 秘密鍵暴露攻撃への対応, 普通の署名への段階的変換, リング署名におけるグループ管理等, 様々なアプリケーションを持つ [SHK09]. ところで, 再リンク可能リング署名の定義では, 再リンク鍵は公開鍵 1 個につき 1 つであると定められている. 実は, この定義が再リンク可能リング署名に様々な制約を課している. 例えば, 代理人は署名者の作る全ての署名を再リンクすることが可能なため, 署名者が署名した文書の価値に応じて代理人を選ぶ事は出来ない. 望まぬ署名が勝手に再リンクされてしまう危険も避けようが無い. さらに, この定義では代理人と検証者の違いが, 鍵生成時に署名者が代理人に与える再リンク鍵のみであり, 代理人にそれ以上の情報を与えない限り, 完全匿名性の実現は困難である. 本論文では, こうした様々な制約を緩和するため, 署名毎に再リンク鍵を構成出来る文書依存再リンク可能リング署名の概念を提案し, その汎用的構成の方法論を与え, 標準的な仮定の下ランダムオラクルモデルで 2 つの具体的方式を得た.

1.1 背景

リング署名 [RST01] を用いると, セットアップ手続きやグループ管理者無しで, 匿名の署名を作成できる. 署名者は自分の秘密鍵とグループ (リング) のメンバーの公開鍵を用い, 文書に関する署名を生成する. メンバーの公開鍵があるならリングは署名生成時に適当に決めて良い.

著者らは, 最近このリング署名の概念を拡張して, リングを構成する能力を, 署名を構成する能力から分離できる, 再リンク可能リング署名 (relinkable ring signature) の概念を提案し, その具体的方式を示した [SHK09, HSK09]. 普通のリング署名とは異なり, 再リンク可能リング署名には再リンクなる手続きが存在し, リング署名生成後に再リンク鍵を使ってリングのメンバーを変更した新しい署名を生成できる. 再リンク鍵は署名鍵よりも弱い鍵で, 署名者により生成され, リングのメンバーを変更する事は出来るが, 新しい署名を作ることは出来ない. 従って署名者は信頼できる代理人に対して, 署名を作成する能力を与えること無く, リングを変更する能力を与えることができる.

この, 再リンク可能リング署名では, 代理人は再リンク鍵を使ってリングを変更することが可能である. メンバーが一人しか居ない正しいリング署名 (普通の署名) を構成できるなら, 代理人は署名者の識別 (または署名偽造) が可能である. 一般に安全な再リンク可能リング署名では, 代理人は署名者の識別が可能となる. 従って代理人があまり信用出来ない場合, 再リンク可能リング署名は公職選挙の秘密投票や組織犯罪の内部告発の様な特に高レベルの匿名

* 独立行政法人情報処理推進機構, 〒 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

性が必要なアプリケーションに必ずしも向いているとは言えない. しかし, 例えばリング署名の依頼計算, 署名者自身の墨塗り, 動的グループのリング署名, 秘密鍵暴露攻撃への対応, 普通の署名への段階的変換, リング署名におけるグループ管理等, 様々なアプリケーションを持っている [SHK09].

1.2 問題点

ところで [SHK09] にある再リンク可能リング署名の定義では, 再リンク鍵は鍵生成時に公開鍵と一緒に生成され, 公開鍵 1 個につき 1 つであると定められている. 署名者は一度でも再リンク鍵を代理人に与えてしまうと, その再リンク鍵は公開鍵が破棄されるまで有効であり続ける. この定義が再リンク可能リング署名に様々な制約を課している. 例えば, 代理人は署名者の作る全ての署名を再リンクすることが可能である. 署名者が署名した文書の価値に応じて代理人を選ぶ事は出来ない. 署名者の望まぬ署名が再リンクされてしまう危険も避けようが無い.

また, リング署名が完全匿名性を達成する為には, 検証者は真の署名者に関する知識を一切持つ事が許されない. 一方, 代理人がリング署名から真の署名者を除外しない為には, 代理人が真の署名者に関する知識を持たなくてはならない. ところが [SHK09] の定義では, 代理人と検証者の知識の差分は代理人に一度しか与えられない再リンク鍵に限られてしまう. 署名者と代理人が共有する秘密の情報量を超えて署名者の情報を情報理論的に秘匿することは不可能であるから, この定義では発行可能な署名の数に強い制限を与えるか, または代理人に追加の情報を与えない限りは完全匿名性を達成する事は不可能である.

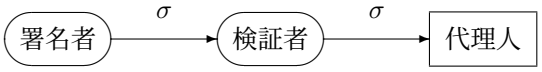

図 1: 再リンク可能リング署名 (σ は署名)

従って, この定義で実用的な方式を設計する場合は, より低い匿名性を甘受する必要があり, 実際, [SHK09] で提案された具体的方式では計算量的匿名性しか達成出来ていない. 仮に代理人が正直であったとしても, 攻撃者が想定外の計算能力を持った場合に, この方式ではリング署名から直接署名者が特定されてしまう危険性がある.

また, [SHK09] の定義には 5 つもの安全性概念が提示されており, 代理人と検証者の知識の差が限定される状況下でこれらの複雑な安全性定義を満足するため, 具体的方式の計算量的仮定に特殊なペアリングの設定を利用していた.

1.3 本論文について

こうした再リンク可能リング署名のさまざまな問題点は, 全てこの定義の欠陥に原因がある. 本論文ではこれらの制約を緩和するため, 署名毎に再リンク鍵を構成出来る文書依存再リンク可能リング署名の概念を提案する.

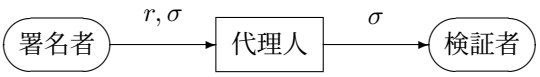

図 2: 文書依存再リンク可能リング署名 (r は再リンク鍵)

この署名系は, 署名者が署名毎にその匿名性を無効化する鍵を構成できる, コンバーチブルリング署名 [LWH05] の拡張とみなす事も出来る. また, この署名系は, ID ベース署名 (IBS) [Sha84] の拡張と考えることも出来る. その参加者の役割は幾分異なるが, 構成アルゴリズムは IBS と非常に良く似ている. この事実は, 文書依存再リンク可能リング署名の汎用的構成の方法論を与える. 本論文では, この方法論に従って 2 通りの文書依存再リンク可能リング署名の具体的方式を与える.

2 定義

$k \in \mathbb{N}$ をセキュリティパラメタとする. 再リンク可能リング署名と同様に, 文書依存再リンク可能リング署名にも二種類の秘密鍵が存在している. 即ち署名鍵 x および再リンク鍵 r である. 以下, 署名者の集合を $N = \{0, 1, \ldots\}$, その部分集合を $L \subset N$ 等とする. 特定の署名者の公開鍵等を記述する際は署名者を添え字として付すこととする. 例えば署名者 $j \in N$ の公開鍵は y_j 等とする. また簡単のため, 公開鍵のリスト $(y_j)_{j \in L}$ 等を y_L 等と記述する. また 1 個の公開鍵からなるリスト (y_j) は誤解の余地が無ければ y_j と略記する.

確率的チューリング機械 X に Y を入力することを $X(Y)$ 等と記述する. ランダムテープの入力引数は特に必要な場合以外は省略する. 変数 X に値 Y を代入することを $X \leftarrow Y$ と記述する. 変数 X に集合 Y から一様ランダムに元を選んで代入することを $X \xleftarrow{\$} Y$ と記述する. 一様ランダムに選んだランダムテープを入力した確率的チューリング機械 Y の出力を, 変数 X に代入することを $X \xleftarrow{\$} Y()$ 等と記述する. 出力変数または出力値 Y を持つ確率的チューリング機械 X を $X() \xrightarrow{\$} Y$ 等と記述する. 任意の二項演算子 $\circ$ に関して, 変数 X に値 $X \circ Y$ を代入することを $X \xleftarrow{\circ} Y$ 等と記述する. 例えば, X, Y を集合として, 変数 X に値 $X \cup Y$ を代入することを $X \xleftarrow{\cup} Y$ と記述する.

PPT_k を k に関する確率的多項式時間アルゴリズムの集合, TM を計算量無制限の確率的アルゴリズムの集合, neg_k を k に関する無視可能関数 (negligible function) の集合とする.

Exp は系の攻撃環境を抽象し, 安全性を記述するため定義されるチューリング機械で, 攻撃者の抽象アルゴリズム $\mathcal{A}$ が与えられる時, 必要なら k の多項式回呼び出し可能な適当な神託機械 $\mathcal{O}$ を $\mathcal{A}$ に与え, 安全性が破られたか否か ($\mathcal{A}$ が勝利したか否かを) を判定するとする. また Exp は署名者 ID により参照できるテープの記録領域を持ちそこに有効な秘密鍵, 公開鍵, 再リンク鍵の組、またはその

一部を記録するとする. $\mathcal{O}$ はこのテープの領域に入出力可能であるとし, $\mathcal{A}$ はこのテープの領域を参照出来ないが, 必要なら有効な秘密鍵, 公開鍵, 再リンク鍵の組, またはその一部を任意に追記出来るとする. (即ち $\mathcal{A}$ はオラクル $\mathcal{O}$ にこの鍵を使わせる事ができるとする). 但し, $\mathcal{A}, \mathcal{O}$ または *Exp* により, 既に記録された秘密鍵, 公開鍵, 再リンク鍵を上書きすることは禁止する. また首尾一貫しない秘密鍵, 公開鍵, 再リンク鍵の組, またはその一部をテープに追記する事は禁止する (秘密鍵で作成した署名が公開鍵で検証失敗する場合など).

2.1 文書依存再リンク可能リング署名

本論文では安全な文書依存再リンク可能リング署名系を次のように定義する.

構文. 文書依存再リンク可能リング署名系 Σ とは下記のような四つのアルゴリズムの組

$$\Sigma = (\mathtt{KeyGen}, \mathtt{Sign}, \mathtt{Relink}, \mathtt{Verify})$$

の事である.

– **鍵生成アルゴリズム**

$\mathtt{KeyGen}(1^k) \xrightarrow{\$} (x, y)$ は, セキュリティパラメタ k に対して秘密鍵 x, 公開鍵 y, 再リンク鍵の一部 r' を出力とする確率的多項式時間アルゴリズムである.

– **署名アルゴリズム**

$\mathtt{Sign}(x, m) \xrightarrow{\$} r$ は, 秘密鍵 x, および文書 m を入力とし, 再リンク鍵 r を出力とする確率的多項式時間アルゴリズムである.

– **再リンクアルゴリズム**

$\mathtt{Relink}(r, L, y_L, m) \xrightarrow{\$} \sigma / \perp$ は, 再リンク鍵 r, リング L, 公開鍵のリスト y_L, および文書 m を入力とし, 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である.

– **検証アルゴリズム**

$\mathtt{Verify}(L, y_L, m, \sigma) \xrightarrow{\$} 0/1$ は, リング L, 公開鍵のリスト y_L, 文書 m, および署名 σ を入力とし, 検証結果 $0/1$ を出力とする確率的多項式時間アルゴリズムである.

安全性.

– **署名オラクル**

$\mathcal{O}_s(i, m) \xrightarrow{\$} \mu$ は攻撃者の指定する署名者 i, 文書 m, に対して, *Exp* 内で設定された文書カウンター $\nu \in \mathbb{N}$, 秘密鍵 x_i, 照会履歴 Q_s, を用いて

$\mathcal{O}_s(i, m) :=$

$\mu \leftarrow \nu\mathtt{++}$;
if (i, m) is valid input then
  $r \xleftarrow{\$} \mathtt{Sign}(x_i, m)$;
otherwise $r \leftarrow \perp$;
$Q_s \xleftarrow{\cup} \{(\mu, i, m, r)\}$;
return μ ;

を実行し, 文書番号 $\mu \in \mathbb{N}$ を出力する神託機械である.

– **再リンクオラクル**

$\mathcal{O}_r(\mu, L) \xrightarrow{\$} \sigma$ は攻撃者の指定する文書番号 μ, リング L, に対して, *Exp* 内で設定された照会履歴 Q_s, Q_r, 公開鍵のリスト y_L を用いて

$\mathcal{O}_r(\mu, L) :=$

if (μ, L) is valid input then
  find (i, m, r) s.t. $(\mu, i, m, r) \in Q_s$;
  $\sigma \xleftarrow{\$} \mathtt{Relink}(r, L, y_L, m)$;
otherwise $\sigma \leftarrow \perp$;
$Q_r \xleftarrow{\cup} \{(\mu, L, \sigma)\}$;
return σ ;

を実行し, リング署名 σ を出力する神託機械である.

– **再リンク鍵暴露オラクル**

$\mathcal{O}_e(\mu) \xrightarrow{\$} r$ は攻撃者の指定する文書番号 μ に対して, *Exp* 内で設定された照会履歴 Q_s, Q_e を用いて

$\mathcal{O}_e(\mu) :=$

if (μ) is valid input then
  find (i, m, r) s.t. $(\mu, i, m, r) \in Q_s$;
otherwise $r \leftarrow \perp$;
$Q_e \xleftarrow{\cup} \{(\mu, r)\}$;
return r ;

を実行し, 再リンク鍵 r を出力する神託機械である.

– **チャレンジオラクル**

$\mathcal{O}_c(L^*, m^*) \xrightarrow{\$} \sigma^*$ は攻撃者の指定するリング $L^* \supset \{0, 1\}$, 文書 m^*, に対して *Exp* 内で設定された照会履歴 Q_c, 署名者 $b \in \{0, 1\}$, オラクル $\mathcal{O}_s, \mathcal{O}_r$, を用いて

$\mathcal{O}_c(L^*, m^*) :=$

if $Q_c \neq \emptyset$ then return $\perp$;
$\mu^* \xleftarrow{\$} \mathcal{O}_s(b, m^*)$;
if (L^*, m^*) is valid then
  $\sigma^* \xleftarrow{\$} \mathcal{O}_r(\mu^*, L^*)$;
otherwise $\sigma^* \leftarrow \perp$;
$Q_c \xleftarrow{\cup} \{(\mu^*, L^*, m^*, \sigma^*)\}$;
return (μ^*, σ^*) ;

を実行し, 再リンク鍵 (μ^*, σ^*) を出力する神託機械である. $\mathcal{O}_c$ が一度でも呼ばれた後は, 照会履歴 Q_c に記録された μ^* は $\mathcal{O}_e$ の正当な引数ではないとする. 同様に $L \not\supset \{0, 1\}$ なる L に関して (μ^*, L) は $\mathcal{O}_r$ の正当な引数ではないとする.

安全な再リンク可能リング署名系 Σ とは下記のような三つの安全性概念を満たす.

– **完全性**

正しく作成された署名は検証にて圧倒的確率で受理される.

即ち, 任意の多項式長の文書 $m \in \{0,1\}^*$, 任意の多項式長の署名者集合 $L \subset N$, 任意の署名者 $i \in L$ に対して

$$\begin{aligned}&\Pr[\\&\quad \forall j \in L, (x_j, y_j) \xleftarrow{\$} \mathtt{KeyGen}(1^k);\\&\quad r \xleftarrow{\$} \mathtt{Sign}(x_i, m);\\&\quad \sigma \xleftarrow{\$} \mathtt{Relink}(r, L, y_L, m);\\&\quad \mathtt{Verify}(L, y_L, m, \sigma) = 0\\&] \in neg_k\end{aligned}$$

なるとき, およびその時に限り, 再リンク可能リング署名 Σ は完全性を持つという.

– **匿名性**

秘密鍵も再リンク鍵も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. 即ち,

$Exp^{\mathrm{anon}}_{k,\Sigma}(\mathcal{A}) :=$

$$\begin{aligned}&\text{clear } \nu, Q_s, Q_r, Q_e, Q_c\ ;\\&b \xleftarrow{\$} \{0,1\}\ ;\\&\forall i \in \{0,1\}, (x_i, y_i) \xleftarrow{\$} \mathtt{KeyGen}(1^k)\ ;\\&b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_s, \mathcal{O}_r, \mathcal{O}_e, \mathcal{O}_c}(y_0, y_1)\ ;\\&\text{return } b \stackrel{?}{=} b'\end{aligned}$$

とし, Exp^{anon} のランダムテープ (従って, b, 各鍵, 各オラクルのランダムテープ, $\mathcal{A}$ のランダムテープ) を標本空間として攻撃者 $\mathcal{A}$ の利得 Adv^{anon} を

$$Adv^{\mathrm{anon}}_{k,\Sigma}(\mathcal{A}) := \left|\Pr\left[Exp^{\mathrm{anon}}_{k,\Sigma}(\mathcal{A}) = 1\right] - \frac{1}{2}\right|$$

とすると, $\forall \mathcal{A}_k \in PPT_k, Adv^{\mathrm{anon}}_{k,\Sigma}(\mathcal{A}_k) \in neg_k$ なるとき, およびその時に限り, 再リンク可能リング署名 Σ は (計算量的) 匿名性を持つという. 特に, 如何なるセキュリティパラメタ k, 正当な鍵ペア (x_0, y_0) および (x_1, y_1), 文書 m, および $L \supset \{0,1\}$ なる正当なリング署名 σ に対しても,

$$\begin{aligned}&|\Pr[\mathtt{Relink}(\mathtt{Sign}(x_0, m), L, y_L, m) = \sigma]\\&\quad -\Pr[\mathtt{Relink}(\mathtt{Sign}(x_1, m), L, y_L, m) = \sigma]| = 0\end{aligned}$$

なるとき, およびその時に限り, 再リンク可能リング署名 Σ は完全匿名性を持つという.

– **偽造不可能性**

文書に対応する再リンク鍵を一つも持たない (従って秘密鍵も持たない) リングでその文書のリング署名を現実的な時間の内に作成できる確率は無視しうる. 即ち,

$Exp^{\mathrm{unforge}}_{k,\Sigma}(\mathcal{A}) :=$

$$\begin{aligned}&\text{clear } \nu, Q_s, Q_r, Q_e\ ;\\&\forall i \in L, (x_i, y_i) \xleftarrow{\$} \mathtt{KeyGen}(1^k)\ ;\\&(L^*, m^*, \sigma^*) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_s, \mathcal{O}_r, \mathcal{O}_e}(y_L)\ ;\\&\text{return } [\ \forall(\mu, i, r) \text{ s.t. } (\mu, i, m^*, r) \in Q_s,\\&\qquad\qquad (\mu, L^*, \sigma^*) \notin Q_r\ \wedge\ (\mu, r) \notin Q_e]\ \wedge\\&\quad (L^* \subset L)\ \wedge\ \mathtt{Verify}(L^*, y_{L^*}, m^*, \sigma^*)\ ;\end{aligned}$$

と定義し, Exp^{unforge} のランダムテープを標本空間として攻撃者 $\mathcal{A}$ の利得 Adv^{unforge} を

$$Adv^{\mathrm{unforge}}_{k,\Sigma}(\mathcal{A}) := \Pr\left[Exp^{\mathrm{unforge}}_{k,\Sigma}(\mathcal{A}) = 1\right]$$

とすると, $\forall \mathcal{A}_k \in PPT_k, Adv^{\mathrm{unforge}}_{k,\Sigma}(\mathcal{A}_k) \in neg_k$ なるとき, およびその時に限り, 再リンク可能リング署名 Σ は偽造不可能性を持つという.

3 汎用的構成の方法論

本節では, ID ベース署名 (IBS) に基づいて文書依存再リンク可能リング署名を得る汎用的な構成法を考察する. ID ベース署名は, 任意の文字列を公開鍵として指定することが可能な電子署名系で, 80 年代前半に国内外でその概念および具体的方式が提案されている [Sha84, Oka84]. 同時期に概念が提案された ID ベース暗号 (IBE) が, 安全な方式を確立するまで 15 年程度の歳月を要したのに対して, IBS は PKI ベースの電子署名系と構文的にはほとんど違いが無く, 比較的簡単に構成できる. そのため, この概念は暗号学において IBE ほどは注目されていない. IBS は概ね次のような四つのアルゴリズムの組 ($\mathtt{Setup}_{\Sigma_i}$, $\mathtt{Extract}_{\Sigma_i}$, $\mathtt{Sign}_{\Sigma_i}$, $\mathtt{Verify}_{\Sigma_i}$) により定義される [BNN04].

– **マスター鍵生成アルゴリズム** $\mathtt{Setup}_{\Sigma_i}(1^k) \xrightarrow{\$} (x, y)$ は, $k \in \mathbb{N}$ をセキュリティパラメタとし, マスター秘密鍵 x, 公開パラメタ y を出力とする確率的多項式時間アルゴリズムである.

– **秘密鍵生成アルゴリズム** $\mathtt{Extract}_{\Sigma_i}(x, i) \xrightarrow{\$} r_i$ は, マスター秘密鍵 x, および署名者 ID i を入力とし, 署名者の秘密鍵 r_i を出力とする確率的多項式時間アルゴリズムである.

– **署名生成アルゴリズム** $\mathtt{Sign}_{\Sigma_i}(y, r_i, m) \xrightarrow{\$} \sigma$ は, 公開パラメタ y, 秘密鍵 r_i, 文書 m を入力とし, 署名 σ を出力とする確率的多項式時間アルゴリズムである.

– **検証アルゴリズム** $\mathtt{Verify}_{\Sigma_i}(y, i, m, \sigma) \xrightarrow{\$} 0/1$ は, 公開パラメタ y, 署名者 ID i, 文書 m, 署名 σ を入力とし, 検証結果 $0/1$ を出力とする確率的多項式時間アルゴリズムである.

安全な IBS は, 完全性, および偽造不可能性の 2 つの安全性要件を満たす [BNN04].

図 3 に示すように, この ID ベース署名の定義は上記の文書依存再リンク可能リング署名の定義と非常に良く似ている. この事実を利用して文書依存再リンク可能リング署名の汎用的構成の方法論を得ることが出来る. 即ち、Σ_i を IBS, Σ を文書依存再リンク可能リング署名として,

- Σ_i の PKG を Σ の署名者と思う.
- Σ_i の署名者を Σ の代理人と思う.
- Σ_i の検証者を Σ の検証者と思う.
- Σ_i の署名者 ID i を Σ の文書 m と思う.
- $\mathtt{KeyGen}(1^k) := \mathtt{Setup}_{\Sigma_i}(1^k)$ とする.

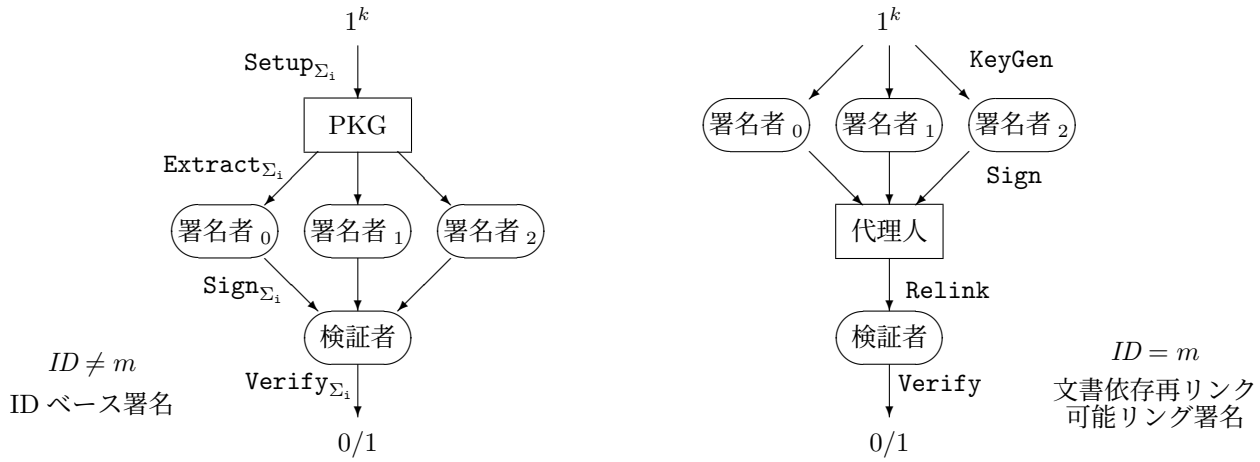

図 3: ID ベース署名と文書依存再リンク可能リング署名

- $\mathtt{Sign}(x, m) := \mathtt{Extract}_{\Sigma_i}(x, m)$ とする.
- 単署名者の Relink を $\mathtt{Sign}_{\Sigma_i}$ と思う.
- 単署名者の Verify を $\mathtt{Verify}_{\Sigma_i}$ と思う.
- Σ_i を PKG に関してリング化する.

この方法論に従うなら, PKG をリング化出来る ID ベース署名があるなら文書依存再リンク可能リング署名を得ることが出来る.

4 具体的方式

4.1 方式 1

以下に ID ベース Schnorr 署名 [SK03] に基づく方法を示す.

4.1.1 設定

群 G, G_T をそれぞれ位数 p の素数位数巡回群とする. $e : G \times G \to G_T$ を非退化双線形写像とする. $g \in G$, を生成元とする. $H : \{0,1\}^* \to G$ および $H' : \{0,1\}^* \to \mathbb{Z}_p$ をそれぞれ独立なランダムオラクルとする. 共有参照文字列 $\rho = (p, G, G_T, e, g, H, H')$ をシステムパラメタと呼ぶ. セキュリティパラメタ k を決めれば k の多項式時間で適切なシステムパラメタが決まり, ρ は k の多項式サイズで符号化されるとする. 系のすべての参加者が同じ ρ を使用するとする. G 上の Gap Diffie-Hellmal 問題 (GDH) の困難性を仮定する [OP01, BLS01].

4.1.2 方式

$\mathtt{KeyGen}(1^k)$:

- $x \xleftarrow{\$} \mathbb{Z}_p,\ y \leftarrow g^x \in G.$
- (x, y) を出力.

$\mathtt{Sign}(x, m)$:

- $h \leftarrow H(m) \in G,\ r \leftarrow h^x \in G.$
- r を出力.

$\mathtt{Relink}(r, L, y_L, m)$:

- i を署名者とし, もし $i \notin L$ なら拒絶し終了.
- $h \leftarrow H(m) \in G.$
- $\exists j \in L, r = h^{x_j}$ なる r の知識証明.
  - $t \xleftarrow{\$} \mathbb{Z}_p.$
  - $\tilde{a}_i \leftarrow e(g, h)^t \in G_T.$
  - $\forall j \in L \setminus \{i\},$
    $c_j \xleftarrow{\$} \mathbb{Z}_p,\ z_j \xleftarrow{\$} G,$
    $\tilde{a}_j \leftarrow e(g, z_j)e(h, y_j)^{c_j} \in G_T.$
  - $c_i \leftarrow H'(\rho, L, m, y_L, \tilde{a}_L) - \sum_{j \neq i} c_j.$
  - $z_i \leftarrow h^t r^{-c_i} \in G.$
- $\sigma \leftarrow (c_L, z_L)$ を出力.

$\mathtt{Verify}(L, y_L, m, \sigma)$:

- $(c_L, z_L) \leftarrow \sigma.$
- $h \leftarrow H(m) \in G.$
- $\forall j \in L,\ \tilde{a}_j \leftarrow e(g, z_j)e(h, y_j)^{c_j} \in G_T.$
- $H'(\rho, L, m, y_L, \tilde{a}_L) \stackrel{?}{=} \sum_{j \in L} c_j$ を出力.

4.2 方式 2

以下に Schnorr 署名 [Sch91, GG09] に基づく方法を示す.

4.2.1 設定

群 G を位数 p の素数位数巡回群とし, $g \in G$ を生成元とする. $H : \{0,1\}^* \to \mathbb{Z}_p$ および $H' : \{0,1\}^* \to \mathbb{Z}_p$ をそれぞれ独立なランダムオラクルとする. 共有参照文字列 $\rho = (p, G, g, H, H')$ をシステムパラメタと呼ぶ. セキュリティパラメタ k を決めれば k の多項式時間で適切なシステムパラメタが決まり, ρ は k の多項式サイズで符号化されるとする. また系のすべての参加者が同じ ρ を使用するとする. G 上の離散対数問題 (DL) の困難性を仮定する.

4.2.2 方式

$\mathtt{KeyGen}(1^k)$:

- $x \xleftarrow{\$} \mathbb{Z}_p,\ y \leftarrow g^x \in G.$
- (x, y) を出力.

$\mathtt{Sign}(x, m)$:

- $t \xleftarrow{\$} \mathbb{Z}_p,\ T \leftarrow g^t \in G.$

– $c \leftarrow H(T, m) \in G$.
– $z \leftarrow t + xc$
– $r \leftarrow (T, z) \in G \times \mathbb{Z}_p$.
– r を出力.

$\texttt{Relink}(r, L, y_L, m)$:

– i を署名者とし, もし $i \notin L$ なら拒絶し終了.
– $(T, z) \leftarrow r \in G \times \mathbb{Z}_p$.
– $c \leftarrow H(T, m) \in G$.
– z の知識証明.
  – $t_i \overset{\$}{\leftarrow} \mathbb{Z}_p$.
  – $T_i \leftarrow g^{t_i} \in G$.
  – $\forall j \in L \setminus \{i\}$,
    $c_j \overset{\$}{\leftarrow} \mathbb{Z}_p,\ z_j \overset{\$}{\leftarrow} \mathbb{Z}_p,$
    $T_j \leftarrow g^{z_j}(Ty_j^c)^{c_j}$
  – $c_i \leftarrow H'(T, T_L, m, y_L) - \sum_{j \neq i} c_j$.
  – $z_i \leftarrow t_i - zc_i$.
– $\sigma \leftarrow (T, c_L, z_L)$ を出力.

$\texttt{Verify}(L, y_L, m, \sigma)$:

– $(T, c_L, z_L) \leftarrow \sigma$.
– $c \leftarrow H(T, m) \in \mathbb{Z}_p$.
– $\forall j \in L,\ T_j \leftarrow g^{z_j}(Ty_j^c)^{c_j}$
– $H'(T, T_L, m, y_L) \overset{?}{=} \sum_{j \in L} c_j$ を出力.

4.3 安全性

定理 1 *H, H' をランダムオラクルとする. 方式 1, 方式 2 は完全匿名性を持ち, 方式 1 は G 上の GDH 仮定のもと, 方式 2 は G 上の DL 仮定のもと偽造不可能性を満たす.*

証明の概略は次の通り. 完全匿名性は任意の $i \in L$ なる鍵 x_i で正直に作成された任意の署名 σ に対して, 鍵 x_0 および鍵 x_1 で全く同じ署名 σ が作成出来き, その確率分布が等しい事を示せばよい. 偽造不可能性は, リワインドを使って得られる再リンク鍵が, 方式 1 では BLS 署名 [BLS01], 方式 2 では Schnorr 署名 [Sch91], となっているので, それらの健全性に帰着する.

5 追跡可能性 (不可能性)

正直な署名者と代理人および標準的な暗号学的仮定の下, 方式 2(方式 1) は以下の性質を持つ. これらの性質は両立しない. アプリケーションによって使い分けると良い.

– **追跡可能性 (不可能性)**
同じ文書に対する二つのリング署名が同じ再リンク鍵から生成されたか否かを現実的な時間の内に判定できない (できる) 確率は無視しうる.

6 まとめと課題

従来の再リンク可能リング署名では, 代理人と検証者の違いが, 鍵生成時に署名者から代理人に与えられる再リンク鍵のみであり, 代理人にそれ以上の情報を与えない限り, 完全匿名性の実現は困難であった. 本論文では, 再リンク可能リング署名 [SHK09] の定義を改良し, 文書に依存して再リンク鍵を生成できる方式, 即ち文書依存再リンク可能リング署名の概念を提案した. そして, ある種の ID ベース署名を利用した汎用的構成の方法論を与え, 2 つの具体的方法を示した.

今回, 文書依存再リンク可能リング署名において, 一般的なリング署名と同様の完全匿名性を実現した. しかし再リンク鍵の漏洩という事象に関しては一般のリング署名には無い概念であり, 代理人に対する仮定を緩和する事が今後の課題である.

参考文献

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *proc. of ASIACRYPT 2001*, pages 514–532, 2001.

[BNN04] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. In *proc. of EUROCRYPT 2004*, pages 268–286, 2004.

[GG09] David Galindo and Flavio D. Garcia. A schnorr-like lightweight identity-based signature scheme. In *proc. of AFRICACRYPT '09*, pages 135–148, 2009.

[HSK09] Fumitaka Hoshino, Koutarou Suzuki, and Tetsutaro Kobayashi. A Flexible Ring Signature. In *proc. of SCIS 2009*, (written in Japanese), 2009.

[LWH05] K. C. Lee, H. Wei, and T. Hwang. Convertible ring signature. *IEE Proceedings of Communications*, 152(4):411–414, 2005.

[Oka84] Tatsuaki Okamoto. A single public-key authentication scheme for multiple users. *Technical Report of IECE Japan*, IN83-92, 1984.

[OP01] T. Okamoto and D. Pointcheval. The gap problems: A new class of problems for the security of cryptographic primitives. In *proc. of PKC 2001*, pages 104–118, 2001.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *proc. of ASIACRYPT 2001*, pages 552–565, 2001.

[Sch91] Claus-Peter Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4(3):161–174, 1991.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In *proc. of CRYPTO '84*, pages 47–53, 1984.

[SHK09] Koutarou Suzuki, Fumitaka Hoshino, and Tetsutaro Kobayashi. Relinkable Ring Signature. In *proc. of CANS 2009*, (to be appear), 2009.

[SK03] Ryuichi SAKAI and Masao KASAHARA. ID based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive: 2003/054, 2003.