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

2005－DPS－122（68）
2005－CSEC－28（68）
2005／3／23

署名長が署名者数に比例しない RSA ベース Sequencial Aggregate 署名方式

寺西勇 †, 佐古和恵 †, 野田潤 ‡, 田口大悟 ‡

{teranisi@ah, k-sako@ab,j-noda@cw, d-taguchi@bp}.jp.nec.com
NEC インターネットシステム研究所
† 〒 211-8666 神奈川県川崎市中原区下沼部 1753
‡ 〒 630-0101 奈良県生駒市高山町 8916-47

本論文では、署名長が署名者数に比例しない RSA ベースのシーケンシャル・アグリゲート署名を提案する。RSA ベースの従来方式の場合、署名者数ひ比例して 1 ビットずつ署名長が伸びてしまうという問題点があった。提案方式は、署名者数や署名した順番によらず署名長が不変である効率的なシーケンシャル・アグリケート署名になっている。また、提案方式は書き換え可能 RFID タグの経路認証にもちいることができる。RFID タグのメモリ容量には制限があるが、RFID タグが多数の各 RFID リーダを通過した証拠として、各 RFID リーダの署名文を RFID タグに書き込んでも一定長のメモリでよいという特長がある。

A New Length invariant Aggregate Signature Scheme Based on RSA

Isamu Teranishi†, Kazue Sako†, Jun Noda‡, Daigo Taguchi‡

{teranisi@ah, k-sako@ab,j-noda@cw, d-taguchi@bp}.jp.nec.com
Internet Systems Research Laboratories, NEC Corporation
†1753 Shimonumabe, Nakahara-Ku, Kawasaki 211-8666, Japan
‡8916-47 Takayama-Chou, Ikoma-Shi Nara 630-0101, Japan

Abstract In this paper, we present a new aggregate signature scheme suitable for authorizing a path of a rewritable RFID tag. We allow each RFID reader to write in its signature to a target RFID tag, as a proof that the tag has passed that reader. The restriction laid on a rewritable RFID tag is that it has bounded size memory. However, a signature length of known schemes based on RSA algorithm will be lengthened at least one bit, each times RFID tag pass a RFID reader. We present a new practical aggregate signature based on RSA algorithm whose signature size is constant regardless of the number of readers it has passed or their order.

1　イントロダクション

ユビキタス時代の到来により、電子デバイスの用途がこれまでとは大きく変る。近年 RFID (Radio Frequency IDentification) タグという新たな電子デバイスが注目されている。RFID タグの一つの用途として商品在庫の物流管理が挙げられる。各在庫に RFID タグをつけ、商品在庫の位置や帳簿情報を RFID タグに記憶させる事で、商品流通の管理を容易にする事ができる。

また、商品が正しい経路を通って流通したかどうかを確認するのに RFID タグを使う事ができる。例えばある機械部品が市場に並ぶ前に 3 つの検査を行なったかどうかの確認に RFID タグを使う事ができる。典型的な実装方法は、各検査を行なう度に RFID リーダが RFID タグの

ID を読み込み、検査を通過したら、データベースセンターに検査結果を送り、データベースセンターが全ての検査結果を記憶しておく、というものである。しかしこの実装の場合、検査を行なう度に RFID リーダはデータベースセンターにアクセスして、データを読み書きしなければならない。RFID が再書き込み可能であれば、RFID リーダは電子署名を生成して、検査を通過した証拠として電子署名を RFID タグに書き込む事ができる。この方法を用いれば、RFID リーダはデータベースセンターにアクセスする必要が無くなる上、データベースセンターに情報を記憶する必要がそもそも無くなる。

この実装方法の問題は RFID タグに記憶できるデータ量が限られている事である。例えば 100 回の検査をすれば 100 個の署名文を記憶する必要があるので、記憶領域をすぐに使い果たしてしまう。

本論文ではこの問題を解決する為、新しい効率的なシーケンシャル・アグリゲート署名方式を提案する。マルチ署名方式 [4, 6] と (シーケンシャル・) アグリゲート署名方式 [2, 3] は署名者が複数人いる状況で署名長を短くするのに使われる方式である。マルチ署名方式は全署名者が同じメッセージに対して署名する場合にしか用いる事ができないが、(シーケンシャル・) アグリゲート署名方式は署名者毎に署名文が異なる場合にも用いる事ができる。しかし我々の要件を全て満たす効率的な既存方式はない。RSA ベースの方式 [3, 6] の場合は署名する度に 1 ビットずつ署名長が伸びるし、ペアリングベースの方式 [2] の場合は我々の要件を全て満たすものの、RSA ベースの方式ほど効率的ではない。我々は署名長が全く伸びないシーケンシャル・アグリゲート署名方式で、署名長が全く伸びないものを提案する。

2 モデル

シーケンシャル・アグリゲート署名方式のモデルを述べる。

2.1 エンティティ

三種類のエンティティがいる：RFID タグの**所有者**、**RFID リーダ**、**検証者**。所有者は RFID タグを持って各 RFID リーダへと移動する。RFID タグは再書き込み可能な記憶領域を持っており、そこには初期値もしくは署名文が記憶される。

シーケンシャル・アグリゲート署名は以下の４つのアルゴリズムからなる：**鍵生成**、**初期化**、**アグリゲート署名**、**検証**.

各 RFID リーダはまず鍵生成を行ない、自分の公開鍵・秘密鍵ペアを作成する。RFID タグの所有者は初期化アルゴリズムに従い、RFID タグを初期化する。

RFID タグが RFID リーダに近づいたら、RFID リーダは RFID タグに書き込まれた情報を読み込み、その情報と自分の鍵ペアを用いてメッセージにアグリゲート署名し、署名文を RFID タグに書き込む。

RFID リーダ $R_{i_1}, \ldots, R_{i_m}$ がそれぞれ公開鍵 $pk_1, \ldots, pk_i$ を用いてメッセージ $M_1, \ldots, M_m$ に順にアグリゲート署名した場合、最終的にできあがった署名文を、$(pk_1, \ldots, pk_i)$ を使った $(M_1, \ldots, M_m)$ に対する署名文と呼ぶ。

検証者は検証アルゴリズムに従う事で、署名文の正当性を検証できる。

2.2 要件

安全なシーケンシャル・アグリゲート署名は以下の要件を満たさねばならない：

1. **健全性**: 正しい方法で生成された署名文は正直な検証者に受理される。

2. **存在的偽造不能性**: いかなる偽造者も、組 $(u, (M_1, \ldots, M_m), (pk_1, \ldots, pk_m))$ で、次の性質を満たすものは作成できない：u は公開鍵 $(pk_1, \ldots, pk_m)$ を用いた $(M_1, \ldots, M_m)$ の署名文であり、しかもある l に対し pk_l は正直な RFID リーダの公開鍵で、その RFID リーダは $(M_1, \ldots, M_l)$ に対して署名していない。この性質はたとえ偽造者が pk_k の所有者以外の全ての RFID リーダと結託し、偽造者と結託した RFID リーダ達の公開鍵を不正に作成したとしても成立する。

存在的偽造不能性の定義をより形式的に述べる。偽造者はまず正直な RFID リーダの公開鍵 pk を与えられる。また偽造者はその RFID リーダのアグリゲート署名を実行してくれるオラクル $\mathcal{O}$ に任意回アクセスできる。すなわち、偽造者が任意に選んだ $(m, (pk_1, \ldots, pk_m), (M_1, \ldots, M_m))$ を $\mathcal{O}$ に送ると、もし $pk_m = pk$ なら、$\mathcal{O}$ は $(pk_1, \ldots, pk_m)$ を用いた $(M_1, \ldots, M_m)$ への署名文を出力する。偽造者の目標は、組 $(u, l, (pk_1, \ldots, pk_l), (M_1, \ldots, M_l))$ で 1) u は $(pk_1, \ldots, pk_l)$

を用いた $(M_1, \ldots, M_l)$ への署名文で、2) $pk_l = pk$ であり、しかも 3) 偽造者は $\mathcal{O}$ に $(u, l, (pk_1, \ldots, pk_l), (M_1, \ldots, M_l))$ を送っていないものを作成する事である。偽造者がこの目標を達成する確率が無視できるほど小さいとき、シーケンシャル・アグリゲート署名方式は存在的偽造不能であるという。

以下で我々は次の記号を用いる：$\mathbb{N}$ で自然数全体の集合を表し、Σ で集合 $\{0,1\}$ を表し、Σ^* でビット列全体の集合 $\bigcup_i \{0,1\}^i$ を表す。我々は Σ^κ と Σ^* とを、$\{0, \ldots, 2^\kappa - 1\}$ と $\mathbb{N}$ とを同一視する。

3 構成方法の概略

提案方式の構成方法の概略を、[3] のそれに従って説明する。二つの関数 E_{pk} と D_{sk} とが方式の構成に本質的な役割を果たす。これらの関数は任意の $u \in \Sigma^*$ に対し、$D_{sk}(E_{pk}(u)) = u$ を満たす。ここで (pk, sk) は公開鍵・秘密鍵ペアとする。

まず関数 E_{pk}、D_{sk} を使って提案方式の概略を説明し、4 章で E_{pk} と D_{sk} の詳細な記述を述べる。提案方式が [3] の方式よりも優位性をもつのは、E_{pk} と D_{sk} との選び方の違いによる。

3.1 初期化

RFID タグの所有者は、RFID タグの記憶領域を 0 にセットする。

3.2 鍵生成

各 RFID リーダ R_i は公開鍵･秘密鍵ペア (pk_i, sk_i) を生成する。

3.3 アグリゲート署名

RFID リーダ R_{i_1} が最初に署名を行なうリーダであれば、$u = D_{sk_{i_1}}(H(M_1||pk_{i_1}) \oplus 0)$ を RFID タグに書き込む。ここで M_1 は署名対象のメッセージ。この結果 RFID タグは、公開鍵 pk_1 を用いた M_1 に対する署名文 u を記憶した事になる。この署名文は $H(M_1||pk_{i_1}) \oplus E_{pk_i}(u) = 0$ が成立するかどうかを確認する事で検証できる事に注意されたい。

RFID リーダ $R_{i_1}, \ldots, R_{i_{m-1}}$ による公開鍵 $pk_{i_1}, \ldots, pk_{i_{m-1}}$ を用いた $(M_1, \ldots M_{m-1})$ の署名文 u を RFID タグが保持していたら、RFID リーダ R_{i_m} はまず署名文 u の正当性を 3.4 の方法で検証し、次に $T_m = M_1||\cdots||M_m||pk_{i_1}||\cdots||pk_{i_m}$ を計算して、$D_{sk_i}(\mathcal{H}(T_m) \oplus u)$ を RFID タグに書き込む。

3.4 検証

検証者はまず、公開鍵 $pk_{i_1}, \ldots, pk_{i_{m-1}}$ の正当性を検証し、さらにこれらの公開鍵が互いに異なる事を確認する。そして検証者は $T_1, \ldots, T_m$ を計算し、

$$\mathcal{H}(T_{i_1}) \oplus E_{pk_{i_1}}(\mathcal{H}(T_{i_2}) \oplus (E_{pk_{i_2}}(\cdots E_{pk_{i_m}}(u))\cdots)) = 0$$

が成立するかどうかを確認する。この式が成立すれば検証者は署名文 u を受理し、そうでなければ棄却する。

4 提案方式

4.1 従来方式の E、D

κ をセキュリティ・パラメータとする。[3] の方式では、各 RFID リーダ R_i は公開鍵・秘密鍵ペアを以下の方法で生成する。R_i はまず κ ビットの RSA モジュラス n_i を生成し、素数 e_i で $\gcd(e_i, \phi(n_i)) = 1$ と $e_i > n_i$ とを満たすものを選ぶ。そしてさらに非負整数 d_i で $e_i d_i = 1 \bmod \phi(n_i)$ を満たすものを計算する。RFID リーダ R_i の公開鍵 pk_i、秘密鍵 sk_i はそれぞれ (n_i, e_i)、d_i である。

検証アルゴリズム中の pk_i の正当性を確認する部分で、検証者は $e_i > n_i$ である事と e_i が素数である事とを確認する。

集合 Σ^* 上の関数関数 E を次のように定義する：

$$E_{pk_i}(u) = \begin{cases} (a^{e_i} \bmod n_i, s||0) & \text{if } a < n_i \\ ((a - n_i)^{e_i} \bmod n_i, s||1) & \text{if } a \geq n_i \end{cases}$$

ここで a は u の最初の κ ビット、s は u の残りの部分を表す。すなわち $u = a||s$ かつ $|a| = \kappa$ である。

また、Σ^* 上の関数 D を次のように定義する：

$$D_{sk_i}(u) = \begin{cases} (a^{d_i} \bmod n_i, s) & \text{if } b = 0 \\ ((a^{d_i} \bmod n_i) + n_i, s) & \text{if } b = 1 \end{cases}$$

ここで a は u の最初の κ ビット、b は u の最後のビット、s は u の残りの部分を表す。すなわち $u = a||s||b$、$|a| = \kappa$、かつ $|b| = 1$ である。

任意の $u \in \Sigma^*$ に対し $D_{sk_i}(E_{pk_i}(u)) = u$ が成立する事を簡単に示す事ができる。

この構成方法には、RFID リーダが署名を行なう度に署名長が 1 ビットずつ伸びてしまうという欠点がある。

4.2 提案関数

RFID タグは限られた量の記憶領域しか持たないので、署名を行なっても署名長が伸びない事が望まれる。そのような性質を持つ方式を実現する為、我々は関数 E'_{pk_i}、D'_{sk_i} を定義する。これらの関数をそれぞれ既存方式 [3] の関数 E_{pk_i}、D_{sk_i} と置き換える事で、署名長が全く伸びないシーケンシャル・アグリゲート署名方式を実現する。

関数 E'_{pk_i} と D'_{pk_i} を定義するため、まず我々は二つの関数 f_i, $g_i : \Sigma^\kappa \to \Sigma^\kappa$ を次のように定義する：

$$f_i(u) = \begin{cases} u^{e_i} \bmod n_i & \text{if } u < n_i \\ u & \text{if } u \geq n_i \end{cases}$$

$$g_i(u) = \begin{cases} u^{d_i} \bmod n_i & \text{if } u < n_i \\ u & \text{if } u \geq n_i \end{cases}$$

任意の $u \in \Sigma^\kappa$ に対し $g_i(f_i(u)) = u$ が成立する事が容易に分かる。

関数 $\phi : \Sigma^\kappa \to \Sigma^\kappa$ を $\phi(u) = u + n_i \bmod 2^\kappa$ により定義する。この時 $\phi(\{2^\kappa - n_i, \ldots, 2^\kappa - 1\}) = \{0, \ldots, n_i - 1\}$ が成立する事を容易に示す事ができる。

さらに $\tilde{f}$、$\tilde{g}$ をそれぞれ $\phi^{-1} \circ f_i \circ \phi$、$\phi^{-1} \circ g \circ \phi$ により定義し、E'_{pk_i}、D'_{sk_i} をそれぞれ $\tilde{f} \circ f$、$g \circ \tilde{g}$ により定義する。

5 効率

以下の表は方式 [3] と提案方式の署名長、署名に必要な計算量、検証に必要な計算量を比較したものである。ここで m は RFID リーダの数、$C(\kappa)$ は κ ビット RSA モジュラス上で κ ビットの巾乗剰余を計算するのに必要なステップ数である。

	Bit Length	Sign	Verify
[3]	$\kappa + m$	$C(\kappa)$	$mC(\kappa)$
Ours	κ	$2C(\kappa)$	$2mC(\kappa)$

6 安全性

Theorem 6.1. ランダムオラクル仮定と *RSA* 仮定のもと、提案方式は安全である。

Proof. 文献 [3] の定理 4.1 より、E'_{pk_i} がトラップドアつき一方向性置換な事を示せば十分である。攻撃者 $\mathcal{A}$ が E'_{pk_i} の逆像を無視できない確率で計算できる、すなわち $\Pr(u \leftarrow_U \Sigma^\kappa, c \leftarrow F_i(u), \dot{u} \leftarrow \mathcal{A}(n_i, c, 1^\kappa) : u = \dot{u})$ は無視できないほど大きいと仮定して矛盾を導く。ここで確率は n_i、u の選び方、および $\mathcal{A}$ のランダムテープの取り方によって定義している。この攻撃者 $\mathcal{A}$ を用いる事で、RSA 問題を多項式時間で解く事ができるアルゴリズム $\mathcal{B}$ が存在する事を示す。仮定より次の二つの確率の少なくとも一方は無視できないほど大きい：

$$\Pr(u \leftarrow_U \Sigma^\kappa, w \leftarrow F_i(u), \dot{u} \leftarrow \mathcal{A}(n_i, e_i, w, 1^\kappa) : u = \dot{u} \mid u \in \{0, \ldots, n_i - 1\}) \quad (6.1)$$

$$\Pr(u \leftarrow_U \Sigma^\kappa, w \leftarrow F_i(u), \dot{u} \leftarrow \mathcal{A}(n_i, e_i, w, 1^\kappa) : u = \dot{u} \mid u \in \{n_i, \ldots, 2^\kappa\}) \quad (6.2)$$

(n, e, α) を RSA 問題のインスタンスとする。アルゴリズム $\mathcal{B}$ は (n, e) を i の公開鍵 (n_i, e_i) としてセットする。

まず (6.1) が無視できないほど大きい場合を考える。$\mathcal{B}$ はランダムかつ一様に $\beta \in \mathbb{Z}_n$ を選び、$v_* = \alpha\beta^{e_i} \bmod n_i$ とする。そして $\mathcal{B}$ は $r \in \Sigma^\kappa$ をランダムかつ一様に選び。もし $r \notin \{0, \ldots, n_i\}$ なら、$\mathcal{B}$ は $w_* = \tilde{f}_i(v_*)$ とし、そうでなければ $w_* = \tilde{f}_i(r)$ とする。

β と r はランダムかつ一様に選ばれているので、w_* は Σ^κ 上一様に分布する。すなわち w_* の分布と w の分布は同一分布である。よって $\mathcal{A}(n_i, e_i, w_*, 1^\kappa)$ は $\dot{u}$ で $F_i(\dot{u}) = w_*$ を満たすものを無視できない確率で出力する。

我々は $r \notin \{0, \ldots, n_i\}$ の場合に注目する。$r \notin \{0, \ldots, n_i\}$ となる確率は $n_i/2^\kappa \geq 2^{\kappa-1}/2^\kappa = 1/2$ である。もし $r \in \{0, \ldots, n_i\}$ であれば、$\mathcal{B}$ は $\perp$ を出力して停止する。

今 $r \notin \{0, \ldots, n_i\}$ が成立しているので、$w_* = \tilde{f}_i(v_*)$ が成立する。また w_* は式 $w_* = F_i(\dot{u}) = \tilde{f}_i \circ f_i(\dot{u})$ も満たす。よって $v_* = f_i(\dot{u})$ が成立する。

式 $\alpha\beta^e = v_* \in \{0,\ldots,n_i-1\}$ と $v_* = f_i(\dot{u})$ が成立するので、$\alpha\beta^{e_i} = v_* = \dot{u}^{e_i}$ が従う。すなわち、$\dot{u}\beta^{-1}$ は RSA 問題のインスタンス (n,e,α) に対する解である。

次に我々は (6.2) が無視できないほど大きい場合を考える。アルゴリズム $\mathcal{B}$ は $\beta \in \mathbb{Z}_n$ をランダムかつ一様に選び、$w'_* = \phi(\alpha\beta^{e_i} \bmod n_i)$ とする。そして $\mathcal{B}$ はランダムかつ一様に $r \in \Sigma^\kappa$ を選ぶ。もし $r \notin \{2^\kappa - n_i,\ldots,2^\kappa-1\}$ が成立していれば $\mathcal{B}$ は $w_* = w'_*$ とし、そうでなければ $w_* = r$ とする。

β と r がランダムかつ一様に選ばれているので、w_* は Σ^κ 上一様に分布する。すなわち w_* の分布と w の分布は同一分布である。従って $\mathcal{A}(n_i,e_i,w_*,1^\kappa)$ は $F_i(\dot{u}) = w_*$ を満たす $\dot{u}$ を無視できない確率で出力する。

我々は $r \notin \{0,\ldots,n_i\}$ が成立する場合のみを考える。$r \notin \{0,\ldots,n_i\}$ は確率 $n_i/2^\kappa \geq 2^{\kappa-1}/2^\kappa = 1/2$ で成立する。もし $r \notin \{0,\ldots,n_i\}$ でないなら、$\mathcal{B}$ は $\perp$ を出力して停止する。

$r \notin \{0,\ldots,n_i\}$ なので $w_* = w'_*$ が成立する。また $w'_* = w_* = F_i(\dot{u}) = \tilde{f}_i \circ f_i(\dot{u})$ は $w'_* = \phi(\alpha\beta^e \bmod n_i) \in \{2^\kappa - n_i,\ldots,2^\kappa-1\}$ を満たす。$\tilde{f}_i = \phi^{-1}\circ f_i \circ \phi$ が成立するので、$(\alpha\beta^e \bmod n_i) = f_i(\dot{u})$ が成立する。すなわち、$\dot{u}\beta^{-1}$ は RSA 問題のインスタンス (n,e,α) の解である。□

7 提案方式の変種

7.1 方式

[3] の方式も提案方式も、署名作成の計算量が RFID リーダの数に比例して多くなるという問題を抱えている。我々は提案方式を修正する事で、この問題を解決できる。修正版の RFID タグは $(u_{m-1}, \mathcal{H}(u_{m-2}))$ を保管する。ここで u_{m-1} と u_{m-2} はそれぞれ $m-1$ 番目、$m-2$ 番目の RFID リーダの署名文で、$\mathcal{H}$ はハッシュ関数。m 番目の署名文を計算するには、m 番目の RFID リーダは $T_m = M_1||\cdots||M_m||pk_{i_1}||\cdots||pk_{i_m}$ を計算し、RFID タグが保管している (u,v) が $v = \mathcal{H}(\mathcal{H}(T_m) \oplus \mathcal{E}_{pk_{m-1}}u)$ を満たしているかどうかを確認し、満たしていれば RFID タグに $(D_{sk_i}(\mathcal{H}(T_m)\oplus u), \mathcal{H}(u))$ を書き込む。

7.2 安全性

この修正版の方式は 4 章の方式ほど安全ではない。この方式は、より弱いバージョンの存在的偽造不能性しか満たさない。この弱いバージョンでは攻撃者の「勝利条件」がもとのバージョンとは異なる。もとのバージョンでは組 $(u,l,(pk_1,\ldots,pk_l),(M_1,\ldots,M_l))$ で、$\mathcal{O}$ に送った事がないものならなんでも出力してよかったが、弱いバージョンの攻撃者は $(u,l,(pk_1,\ldots,pk_l),(M_1,\ldots,M_l))$ で、$M'_m = M_l$ を満たす $(u,l,(pk'_1,\ldots,pk'_m),(M'_1,\ldots,M'_m))$ を $\mathcal{O}$ に送った事がないものしか出力できない。安全性証明は [3] のそれと同様である。

References

[1] M. Bellare, A. Boldyreva, A Desai, and D. Pointcheval. Key-Privacy in Pubkec-Key encryption. In *Advances in Cryptology – ASIACRYPT 2001*, vol. 2248 of *LNCS*, pp. 566-582. Springer-Verlag, 2001.

[2] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In *Advances in Cryptology – EUROCRYPT 2003*, vol. 2656 of *LNCS*, pp. 416-432. Springer-Verlag, 2003.

[3] Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Hovav Shacham. Sequential Aggregate Signatures from Trapdoor Permutations. In *Advances in Cryptology – EUROCRYPT 2004*, vol. 3027 of *LNCS*, pp. 74-90. Springer-Verlag, 2004.

[4] Silvio Micali, Kazuo Ohta, Leonid Reyzin. Accountable-subgroup multisignatures: extended abstract. In: Proc. of the 8th ACM Conference on Computer and Communications Security (CCS 2001), pp. 245-254. ACM, 2001.

[5] Ryotaro Hayashi, Tatsuaki Okamoto, and Keisuke Tanaka. An RSA Family of Trap-Door Permutations with a Common Domain and Its Applications. In *Advances in Cryptology – Public Key Cryptography 2004*, vol. 2947 of *LNCS*, pp. 291-304. Springer-Verlag, 2004.

[6] Tatsuaki Okamoto. A digital multisignature scheme using bijective public-

key cryptosystem. ACM Transactions on Computer Systems, 1988, 6(8): 432-441.