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

2005－ＣＳＥＣ－30 (24)
2005／7／21

追跡可能な部分ブラインド署名の構成法

千田 浩司† 大久保美也子† 塩野入 理† 中村伊智三† 金井 敦†

† NTT 情報流通プラットフォーム研究所
〒 239-0847 神奈川県横須賀市光の丘 1-1
E-mail: †{chida.koji,ookubo.miyako,shionoiri.osamu,nakamura.ichizo,kanai.atsushi}@lab.ntt.co.jp

あらまし ブラインド署名に部分開示機能及び署名／ユーザ追跡の機能を追加した「追跡可能な部分ブラインド署名」(PBST; Partially Blind Signatures with Traceability) の構成については，その実現可能性も含め現在まで十分議論されていない．そこで本稿では，先ず実際に PBST の機能が要求されるアプリケーションを挙げ，その後 PBST 及びそのセキュリティ要件を明確に定義する．そして二種類の PBST 実現プロトコルを与え，それらの安全性について，先に定義したセキュリティ要件に基づいて考察を行う．

キーワード ブラインド署名，部分開示性，追跡可能性，証明書，匿名性

Partially Blind Signatures with Traceability

Koji CHIDA†, Miyako OHKUBO†, Osamu SHIONOIRI†, Ichizo NAKAMURA†, and Atsushi KANAI†

† NTT Information Sharing Platform Laboratories
1-1 Hikarinooka, Yokosuka, Kanagawa, 239-0847 Japan
E-mail: †{chida.koji,ookubo.miyako,shionoiri.osamu,nakamura.ichizo,kanai.atsushi}@lab.ntt.co.jp

Abstract Until now, it is not sufficiently discussed about how to construct a provably secure "partially blind signature with traceability" (PBST) by which functions of both the partially blind signature and the fair blind signature. This paper describes an application that the function of PBST is actually demanded, and specifically defines PBST and some security requirements of it. Subsequently, this paper proposes two kinds of PBST protocols and then considers the security of these according to the security requirements where they are previously defined.

Key words Blind Signature, Partial Blindness, Traceability, Certificate, Anonymity

1. はじめに

ブラインド署名は Chaum によって 1982 年に提案され [4]，アプリケーションとしては電子マネー (電子決済) や電子投票が代表的であり，ブラインド署名はこれらアプリケーションにおけるユーザの匿名性を効果的に高められる事が知られている ([5], [7] 等)．しかし一般に匿名性はユーザのプライバシ保護レベルを高めると同時に，ユーザの不正を誘発する事にもなりかねず，ブラインド署名のアプリケーションは匿名性悪用によるユーザの不正を防止する技術を必要とする場合がある．例えば電子マネーでは不正コピーや重複使用の防止技術が，電子投票では二重投票の防止技術が必要となる．

一方，アプリケーションに特化しない汎用的なブラインド署名の不正防止技術として，部分ブラインド署名 [1], [2] や追跡可能なブラインド署名 (FBS; Fair Blind Signature)(注1) [3], [8] といった拡張方式が提案されている．前者は，メッセージの一部は署名者に開示される特徴を持ち，後者は，管理者だけは署名付きメッセージと署名発行依頼者との対応関係を識別出来る特徴を持つ．しかしながら，ブラインド署名に部分開示機能及び署名／ユーザ追跡の機能を追加した「追跡可能な部分ブラインド署名」(PBST; Partially Blind Signatures with Traceability) の構成については，その実現可能性も含め現在まで十分議論されていない．

PBST の機能が要求されるアプリケーションとしては，FBS を用いた ID エスクロー方式がある [6]．§2.1 で詳しく述べる

(注1)：本稿では FBS において，ユーザの不正防止を目的として，任意の署名付きメッセージに対して管理者だけは該署名の発行依頼者を識別出来る性質を強調するため，FBS を「追跡可能なブラインド署名」と呼ぶ事にする．

が，該 ID エスクロー方式において FBS の代わりに PBST を用いる事で，有効な機能拡張が得られる．そこで本稿では，実用的かつセキュアな PBST を構成する事を目的とし，PBST 及びそのセキュリティ要件を明確に定義した上で，PBST 実現プロトコルを与え，その安全性について先に定義したセキュリティ要件に基づいて考察を行う．

2. 準　　備

2.1 PBST を用いたアプリケーション

[6] では FBS を利用した ID エスクロー方式を提案している．これは簡単に言えば，ユーザは CA (Certificate Authority) から公開鍵証明書を発行してもらう際，FBS を用いる事で，公開鍵を CA に対して秘匿する方式であり，これによりユーザは公開鍵証明書を発行者である CA の監視下で用いたとしても，CA に対して匿名性を確保出来る．従って，CA が該公開鍵を元に秘密裏にユーザの行動を追跡する，あるいは CA が保管している公開鍵とユーザとの対応リストが外部に漏洩するといった被害を防止でき，プライバシ保護や情報漏洩防止の観点から有効な手段であるといえる．一方，ユーザの匿名性悪用による不正を防ぐためには，条件によってはユーザを識別出来る機能も重要であり，[6] では CA を含む一定数以上の管理者が協力した場合に限り，任意の公開鍵に対してその所有者を識別出来る事を特徴としている．

FBS に部分開示機能が加われば，上述の公開鍵証明書に CA が有効期限や属性等を埋め込む事が出来る．これらの情報を埋め込む事で一般にユーザの匿名性は低下するが，運用の柔軟性が高まる事は明らかであり，有効期限を埋め込む事でセキュリティ上の効果も期待出来る．従って，埋め込み情報が実用上匿名性を著しく損ねるものでなければ，[6] において PBST の機能は特に有効であると考えられる．

2.2 定　　義

ここでは PBST，及びそのセキュリティ要件について定義する．先ず概要を述べる．PBST における主要なセキュリティ要件は

（1） 署名／ユーザの追跡可能性 (定義 3, 4)
（2） メッセージの部分開示性 (定義 5)
（3） 署名の偽造困難性 (定義 6)

に関するものであり，それぞれ

（1） 管理者が (署名者との協力の下で) 署名付きメッセージと署名発行依頼者 (＝ユーザ) との対応関係を正しく識別出来ないような署名を (ある一定の条件下で) ユーザが生成する事は出来ない，
（2） メッセージの非開示部分に関する情報を (ある一定の条件下で) 署名者が知る事は出来ない，
（3） 署名者の意図しない署名を (ある一定の条件下で) ユーザは作成出来ない，

事を要件としている．

以下で与える定義は，基本的には阿部らが [2] 及び [3] で与えた定義の組み合わせである．なお [2] では部分ブラインド署名，そして [3] では FBS に対するセキュリティ要件を与えている．

[定義 1] (追跡可能な部分ブラインド署名 (PBST))　$\mathcal{G}, \mathcal{G}_T, \mathcal{S}, \mathcal{U}, \mathcal{V}, \mathcal{R}_{sig}, \mathcal{R}_{sid}, \mathcal{M}_{sig}, \mathcal{M}_{sid}$ がそれぞれ以下であるとき，$(\mathcal{G}, \mathcal{G}_T, \mathcal{S}, \mathcal{U}, \mathcal{V}, \mathcal{R}_{sig}, \mathcal{R}_{sid}, \mathcal{M}_{sig}, \mathcal{M}_{sid})$ は PBST であるという．

- $\mathcal{G}$([2]): セキュリティパラメータ n を入力として，署名公開鍵，秘密鍵の組 (pk, sk) を出力するような，n に対する確率的多項式時間アルゴリズム．
- $\mathcal{G}_T$([3]): pk を入力として，追跡用公開鍵，秘密鍵の組 (rpk, rsk) を出力するような，n に対する確率的多項式時間アルゴリズム．
- $\mathcal{S}, \mathcal{U}$([2] の変形): それぞれ署名者，ユーザの役割を担う対話型 Turing マシン．$\mathcal{S}$ は sk, pk, rpk, 及び開示情報 info を入力として，$\mathcal{U}$ は pk, rpk, info, 及びメッセージ msg を入力として，署名発行プロトコルを n に対する多項式時間内で実行し，$\mathcal{U}$ は署名 sig を出力する．
- $\mathcal{V}$([2]): pk 及び $(\mathsf{info}, \mathsf{msg}, sig)$ を入力として，署名検証結果 *accept* / *reject* を返すような，n に対する多項式時間アルゴリズム．
- $\mathcal{R}_{sig}$([3]): pk, rsk, 及び $\mathcal{S}, \mathcal{U}$ 間のあるセッション時における $\mathcal{S}$ の公開入出力テープの情報 $view$ を入力として，該セッションで $\mathcal{U}$ が出力した署名 sig の識別子 I_{sig} を出力するような，n に対する多項式時間アルゴリズム．
- $\mathcal{R}_{sid}$([3] の変形): pk, rsk, 及び $(\mathsf{info}, \mathsf{msg}, sig)$ を入力として，$\mathcal{U}$ が sig を出力したセッションの識別子 I_{sid} を出力するような，n に対する多項式時間アルゴリズム．
- $\mathcal{M}_{sig}$([3] の変形): I_{sig} 及び $(\mathsf{info}, \mathsf{msg}, sig)$ を入力として，sig の識別子が I_{sig} であるか否かを示す結果 *match* / *not_match* を出力するような，n に対する多項式時間アルゴリズム．
- $\mathcal{M}_{sid}$([3]): I_{sid} 及び $view$ を入力として，$view$ に対応するセッションの識別子が I_{sid} であるか否かを示す結果 *match* / *not_match* を出力するような，n に対する多項式時間アルゴリズム．

[定義 2] (完全性)　ある PBST について，$\mathcal{S}, \mathcal{U}$ が正しく署名発行プロトコルを実行した際の $\mathcal{U}$ の入出力の一部 $(\mathsf{info}, \mathsf{msg}, sig)$, $\mathcal{S}$ の公開入出力テープの情報 $view$, 及び pk に対して，

$$\begin{cases} \mathcal{V}(pk; \mathsf{info}, \mathsf{msg}, sig) = accept, \\ \mathcal{M}_{sig}(\mathcal{R}_{sig}(rsk, pk; view), \mathsf{info}, \mathsf{msg}, sig) = match, \\ \mathcal{M}_{sid}(\mathcal{R}_{sid}(rsk, pk; \mathsf{info}, \mathsf{msg}, sig), view) = match \end{cases} \quad (1)$$

となる確率が，十分大きな数 n に対して $1 - 1/n^c$ (c は定数) 以上であるとき，その PBST は完全であるという．

[定義 3] (署名の追跡可能性 ([3] の変形))　ある PBST について，正しく動作する $\mathcal{S}$ に対して適応的かつ自由に交互配置 (interleaving) しながら ℓ 回まで対話可能な，n に対する任意の確率的多項式時間アルゴリズム $\mathcal{U}^*$ が，$i = 1, \ldots, \ell$ につ

いて，

$$\begin{cases} I_{sig} = \mathcal{R}_{sig}(rsk, pk; view_i), \\ \mathcal{M}_{sig}(I_{sig}, \mathsf{info}, \mathsf{msg}, sig) = not\_match, \\ \mathcal{V}(pk; \mathsf{info}, \mathsf{msg}, sig) = accept \end{cases}$$

となる (info, msg, sig) を出力する確率，あるいは $i = 1, \ldots, \ell$ について，

$$\begin{cases} I_{sig} = \mathcal{R}_{sig}(rsk; view_i), \\ \mathcal{M}_{sig}(I_{sig}, \mathsf{info}, \mathsf{msg}, sig) = \mathcal{M}_{sig}(I_{sig}, \mathsf{info}', \mathsf{msg}', sig'), \\ \mathcal{V}(pk; \mathsf{info}, \mathsf{msg}, sig) = accept, \\ \mathcal{V}(pk; \mathsf{info}', \mathsf{msg}', sig') = accept \end{cases}$$

となる二つの異なる組 (info, msg, sig), (info′, msg′, sig') を出力する確率が，十分大きな数 n に対して高々 $1/n^c$ (c は定数) であるとき，その PBST は署名の追跡が可能であるという．

[定義 4] (ユーザ (セッション) の追跡可能性 ([3] の変形))
ある PBST について，正しく動作する $\mathcal{S}$ に対して適応的かつ自由に交互配置 (interleaving) しながら ℓ 回まで対話可能な，n に対する任意の確率的多項式時間アルゴリズム $\mathcal{U}^*$ が，$i = 1, \ldots, \ell$ について，

$$\begin{cases} I_{sid} = \mathcal{R}_{sig}(rsk, pk; \mathsf{info}, \mathsf{msg}, sig), \\ \mathcal{M}_{sid}(I_{sid}, view_i) = not\_match \end{cases}$$

となる (info, msg, sig) を出力する確率，あるいは

$$\mathcal{M}_{sid}(I_{sid}, view_i) = \mathcal{M}_{sid}(I_{sid}, view_j) = match$$

となる i, j ($i \neq j$) が存在するような (info, msg, sig) を出力する確率が，十分大きな数 n に対して高々 $1/n^c$ (c は定数) であるとき，その PBST はユーザの追跡が可能であるという．

[定義 5] (部分開示性 ([2] の変形)) ある PBST について，$\mathcal{U}_0, \mathcal{U}_1$ を正しく署名発行プロトコルを実行するユーザと仮定したとき，任意の確率的多項式時間アルゴリズム $\mathcal{S}^*$ が以下のプロトコル

(1) $(pk, sk) \leftarrow \mathcal{G}(1^n)$
(2) $(rpk, rsk) \leftarrow \mathcal{G}_T(pk)$
(3) $\mathcal{S}^*$ は (pk, sk), rpk を受け取る
(4) $(\mathsf{msg}_0, \mathsf{msg}_1, \mathsf{info}_0, \mathsf{info}_1) \leftarrow \mathcal{S}^*(sk, rpk)$
(5) msg_b, $\mathsf{msg}_{\bar{b}}$ ($b \in_R \{0,1\}$, $\bar{b} = 1 - b$) をそれぞれ $\mathcal{U}_0$, $\mathcal{U}_1$ のメッセージとする
(6) $\mathcal{S}^*$ は $\mathcal{U}_0, \mathcal{U}_1$ と署名発行プロトコルを行う
(7) $\mathcal{U}_0, \mathcal{U}_1$ はそれぞれ $(\mathsf{info}_0, \mathsf{msg}_0, sig_b)$, $(\mathsf{info}_1, \mathsf{msg}_1, sig_{\bar{b}})$ を出力する．
(8) $\mathsf{info}_0 = \mathsf{info}_1$ であれば，$\mathcal{S}^*$ は $(\mathsf{info}_0, \mathsf{msg}_0, sig_b)$, $(\mathsf{info}_1, \mathsf{msg}_1, sig_{\bar{b}})$ を受け取る
(9) $\mathcal{S}^*$ は $b' \in \{0,1\}$ を出力する

を行ったとき，$b' = b$ となる確率が，十分大きな数 n に対して高々 $1/2 + 1/n^c$ (c は定数) であるとき，その PBST は部分開示機能を持つという．

[定義 6] (偽造困難性 ([2] の変形)) ある PBST について，正しく動作する $\mathcal{S}$ に対して適応的かつ自由に交互配置 (interleaving) しながら各 info に対して ℓ_{info} 回まで対話可能な，n に対する任意の確率的多項式時間アルゴリズム $\mathcal{U}^*$ が，任意の $j = 1, \ldots, \ell_{\mathsf{info}} + 1$ に対して $\mathcal{V}(pk; \mathsf{info}, \mathsf{msg}_j, sig_j) = accept$ となる確率が，十分大きな数 n に対して高々 $1/n^c$ (c は定数) であるとき，その PBST は偽造困難であるという．

注意：定義 5, 6 は署名者 $\mathcal{S}$ と管理者 $\mathcal{R}$(注2) の結託を考慮していない．即ち $\mathcal{S}$ が rsk を得た場合のセキュリティは対象外としている．従って，$\mathcal{S}$ と $\mathcal{R}$ の結託を考慮した [3] で定義したセキュリティ要件 ([3] 定義 3, 4) は，定義 5, 6 のそれよりも強い要件といえる．

2.3 既存の FBS [3]

提案方式の基本技術となる既存の FBS [3] のプロトコルについて説明する．

署名用鍵生成 ($\mathcal{G}$) 署名者 $\mathcal{S}$ は以下を実行する．

$$((p, q, g, h, y, z, \mathcal{F}, \mathcal{H}), x) \leftarrow \mathcal{G}(1^n).$$

ここで p, q を素数，$\langle g \rangle$ を g によって生成される $\mathbb{Z}_p^\times$ の位数 q の部分群，そして $h (\neq 1) \in \langle g \rangle$, $\mathcal{F} : \{0,1\}^* \to \langle g \rangle$, $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{|q|}$, $x \in_R \mathbb{Z}_q^*$, $y = g^x \pmod p$, $z = \mathcal{F}(p \| q \| g \| h \| y)$ とする．x は $\mathcal{S}$ が秘密に保持する．

追跡用鍵生成 ($\mathcal{G}_T$) 管理者 $\mathcal{R}$ は以下を実行する．

$$((y_t, ek), (x_t, dk)) \leftarrow \mathcal{G}_T(p, q, g, h, y, z).$$

ここで $x_t \in_R \mathbb{Z}_q$, $y_t = g^{x_t} \pmod p$, そして (ek, dk) はある検証可能暗号 $\mathcal{E}$ ([3] §3.2 等を参照) の公開鍵，秘密鍵の組とする．$rsk = (x_t, dk)$ は $\mathcal{R}$ が秘密に保持する．

署名発行 ($\mathcal{S}$, $\mathcal{U}$)

署名者 $\mathcal{S}$ 及びユーザ $\mathcal{U}$ は図 1 に示す署名発行プロトコルを実行する．ここで $pk = (p, q, g, h, y, z)$, $sk = x$, $rpk = (y_t, ek)$, そして $\mathsf{msg} (\in \{0,1\}^*)$ はメッセージとする．E, P, P_s の記法については [3] を参照されたい．

署名検証 ($\mathcal{V}$)

pk, msg, $sig = (\zeta_1, \rho, \varpi, \sigma_1, \sigma_2, \delta)$ を入力として，

$$\varpi + \delta \stackrel{?}{=} \mathcal{H}(\zeta_1 \| g^\rho y^\varpi \| g^{\sigma_1} \zeta_1^\delta \| h^{\sigma_2} (z/\zeta_1)^\delta \| \mathsf{msg}) \qquad (2)$$

の結果 *accept* / *reject* を出力する．

追跡 ($\mathcal{R}_{sig}$, $\mathcal{R}_{sid}$, $\mathcal{M}_{sig}$, $\mathcal{R}_{sid}$)

(注2) : $\mathcal{R}$ は $\mathcal{G}_T$, $\mathcal{R}_{sig}$, $\mathcal{R}_{sid}$, $\mathcal{M}_{sig}$, $\mathcal{R}_{sid}$ を実行する．

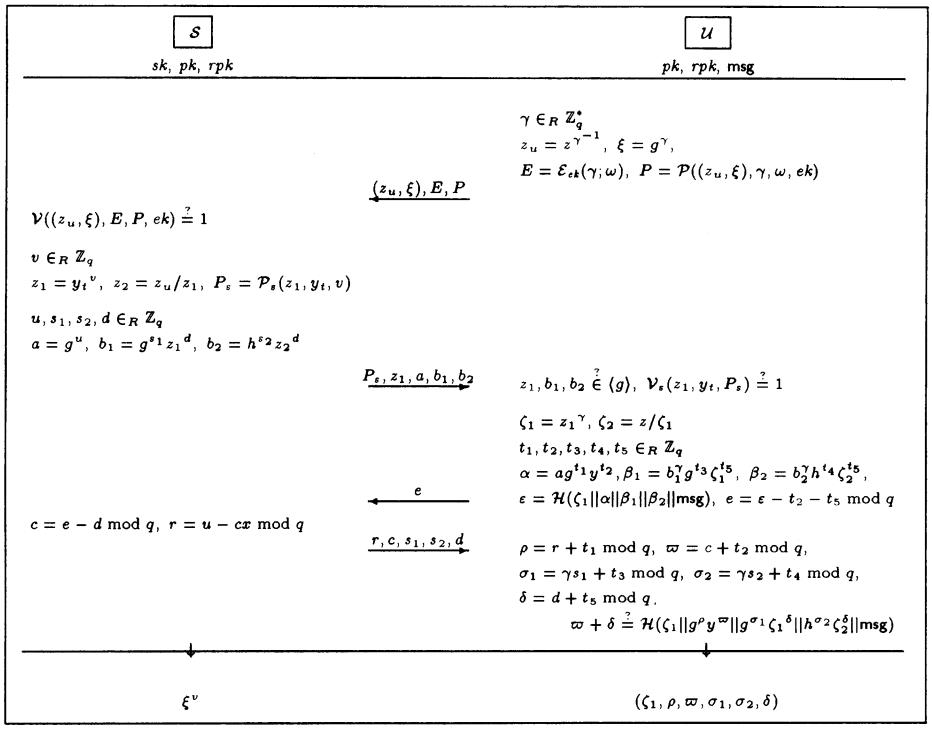

図 1　[3] の署名発行

- 署名の追跡：管理者 $\mathcal{R}$ は $view = \xi^v$ 及び $\zeta_1^{(i)}$ $(i = 1,2,\ldots)$ を入力として，$I_{sig} = (\xi^v)^{x_t}$ を計算し，$i = 1,2,\ldots$ について，

$$\begin{cases} match & if \quad I_{sig} = \zeta_1^{(i)} \\ not\_match & otherwise \end{cases}$$

を出力する．

- ユーザ (セッション) の追跡：管理者 $\mathcal{R}$ は ζ_1 及び $view = \xi_i^v$ $(i = 1,2,\ldots)$ を入力として，$I_{sid} = \zeta_1^{1/x_t}$ を計算し，$i = 1,2,\ldots$ について，

$$\begin{cases} match & if \quad I_{sid} = \xi_i^v \\ not\_match & otherwise \end{cases}$$

を出力する．

3. 提案方式

本稿で提案する方式は，[3] で提案された FBS プロトコルが info を用いて行われるように拡張したものである．その際，正しい開示情報 info を用いない限りは署名検証に合格しないような署名発行プロトコルを構成する必要があり，今回は以下の二種類のアプローチについて検討を行った．

(A1)　info を $\langle g \rangle$ または $\mathbb{Z}_q$ の元とし，署名発行及び署名検証で共通の info を利用する必要があるようにプロトコルを変更する．

(A2)　[2] で提案された部分ブラインド署名の技法を用いる．即ち，署名発行及び署名検証で共通して用いられる何れかの基底 (公開鍵) を，info を入力としたハッシュ関数を用いて構成する．

次に上記アプローチに基づいた具体的なプロトコルを与える．先ず (A1) については，図 1 ([3]) において，

[拡張 1]

$$\begin{aligned} z_2 &= z_u/z_1 \to z_u/z_1^{\mathsf{info}}, \\ \zeta_2 &= z/\zeta_1 \to z/\zeta_1^{\mathsf{info}}, \\ \varpi + \delta &\stackrel{?}{=} \mathcal{H}(\zeta_1 \| g^\rho y^\varpi \| g^{\sigma_1} \zeta_1^\delta \| h^{\delta_2} (z/\zeta_1)^\delta \| \mathrm{msg}) \\ &\to \mathcal{H}(\zeta_1 \| g^\rho y^\varpi \| g^{\sigma_1} \zeta_1^\delta \| h^{\delta_2} (z/\zeta_1^{\mathsf{info}})^\delta \| \mathrm{msg}) \end{aligned}$$

とする．続いて (A2) については，図 1 ([3]) において，

[拡張 2]

$$z = \mathcal{F}(p \| q \| g \| h \| y) \to \mathcal{F}(p \| q \| g \| h \| y \| \mathsf{info})$$

とする．

なお拡張 1, 2 何れにおいても署名発行，署名検証の入力に info (拡張 1 であれば $\mathsf{info} \in \{0,1\}^*$, 拡張 2 であれば $\mathsf{info} \in \mathbb{Z}_q$) を追加する．

4. 考　　察

§2.2 の定義を元に，拡張 1, 2 の考察を行う．先ず定義 1, 2

から容易に以下の補題が成り立つ.

[補題 1] 拡張 1 は PBST である.
[補題 2] 拡張 2 は PBST である.
[補題 3] 拡張 1 は完全である.
[補題 4] 拡張 2 は完全である.

実際, 補題 3, 4 について確率 1 で定義 2 の式 (1) が成り立つ事が分かる.

続いて定義 6 に基づいた偽造困難性について考察する. 拡張 1, 2 の偽造困難性については以下が成り立つ.

[定理 1] $\mathcal{H}$ がランダムオラクル, $\sum_{\mathsf{info}} \ell_{\mathsf{info}} = 1$ のとき, $\langle g \rangle$ 上の離散対数問題を解く事が困難であれば, 拡張 1 は偽造困難である.

[定理 2] $\mathcal{F}$, $\mathcal{H}$ がランダムオラクル, $\sum_{\mathsf{info}} \ell_{\mathsf{info}} = 1$ のとき, $\langle g \rangle$ 上の離散対数問題を解く事が困難であれば, 拡張 2 は偽造困難である.

(定理 1 の証明) $\ell_{\mathsf{info}} = 1$ となる開示情報 info を入力とした $\mathcal{U}^*$ が $\mathcal{S}$ と一度だけ対話可能なとき, 以下の攻撃 (A), (B) が困難である事を示す.

(A) 同一の info に対して異なる二つの署名付きメッセージ $(\zeta_1, \rho, \varpi, \sigma_1, \sigma_2, \delta, \mathsf{msg})$, $(\zeta_1', \rho', \varpi', \sigma_1', \sigma_2', \delta', \mathsf{msg}')$ を生成する.

(B) info' ($\neq \mathsf{info}$) に対する署名付きメッセージ $(\zeta_1', \rho', \varpi', \sigma_1', \sigma_2', \delta', \mathsf{msg}')$ を生成する.

$\mathcal{H}$ は $\mathcal{U}^*$ から問い合わせがあれば任意入力に対して $\mathbb{Z}_q$ 上の乱数を生成, 出力するものとする. すると $\mathcal{U}^*$ が $\mathcal{S}$ と対話しない場合, または e を $\mathcal{S}$ に送信する前に $\mathcal{H}$ へ問い合わせを行っていない場合は, $\mathcal{U}^*$ が §2.3 の検証式 (2) に合格する開示情報及び署名付きメッセージの組を生成する事は, 無作為に選んだ開示情報及び署名付きメッセージの組が検証式 (2) に合格する無視出来る確率 $1-(\frac{q-1}{q})^{q_H}$ ($< \frac{q_H}{q}$) を除き, (g,h) または (g,y) の離散対数問題を解く事に帰着される (ここで q_H は $\mathcal{U}^*$ の $\mathcal{H}$ への問い合わせ最大回数). 即ち, $\mathcal{U}^*$ は少なくとも α, β_1, β_2 を正しく生成した後, $\tilde{\varepsilon} = \mathcal{H}(\tilde{\zeta}_1 \| \alpha \| \beta_1 \| \beta_2 \| \mathsf{msg})$, $\tilde{e} = \tilde{\varepsilon} - t_2 - t_5$ を生成し(注3), $\tilde{e}$ を送信後 $r = \rho - t_1$, $c = \varpi - t_2$, $s_1 = (\sigma_1 - t_3)\gamma$, $s_2 = (\sigma_2 - t_4)\gamma$, $d = \delta - t_5$ を $\mathcal{S}$ から受信しない限りは, 検証式 (2) に合格する開示情報及び署名付きメッセージの組を生成出来ない. 従ってもし攻撃 (A) が可能であれば,

$$(\alpha =)\ g^{\rho} y^{\varpi} = g^{\rho'} y^{\varpi'} \tag{3}$$
$$(\beta_1 =)\ g^{\sigma_1} \zeta_1^{\delta} = g^{\sigma_1'} \zeta_1'^{\delta'} \tag{4}$$
$$(\beta_2 =)\ h^{\sigma_2} (z/\zeta_1^{\mathsf{info}})^{\delta} = h^{\sigma_2'} (z/\zeta_1'^{\mathsf{info}})^{\delta'} \tag{5}$$
$$(\tilde{\varepsilon} =)\ \varpi + \delta = \varpi' + \delta' \tag{6}$$

(注3) : 検証式 (2) では, ζ_1 ($\in \langle g \rangle$) 及び msg に対する言語は制限していないため任意で良い.)

が成り立つような $(\zeta_1, \rho, \varpi, \sigma_1, \sigma_2, \delta, \mathsf{msg})$, $(\zeta_1', \rho', \varpi', \sigma_1', \sigma_2', \delta', \mathsf{msg}')$ を生成出来る事になる. 以下ではこれが困難である事を示す.

先ず $\mathcal{H}$ の衝突困難性から, $\zeta_1 = \zeta_1' = \tilde{\zeta}_1$, $\mathsf{msg} = \mathsf{msg}'$ がいえる. 次に式 (3) を

$$g^{\rho'-\rho} y^{\varpi'-\varpi} = 1 \tag{7}$$

と変形すれば, $\rho = \rho' \Leftrightarrow \varpi = \varpi'$ が成り立つ事が分かる. そしてもし $\varpi \neq \varpi'$ であれば, $x = \log_g y = (\rho - \rho')/(\varpi' - \varpi)$ となる事から, (g, y) の離散対数問題を解く事ができ仮定に反する. 即ち $\varpi = \varpi'$, $\rho = \rho'$ となる. すると式 (6) から直ちに $\delta = \delta'$ がいえ, 更に式 (4), (5) を式 (7) 同様の変形をする事で $\sigma_1 = \sigma_1'$, $\sigma_2 = \sigma_2'$ となる事が分かる. 従って $(\zeta_1, \rho, \varpi, \sigma_1, \sigma_2, \delta, \mathsf{msg}) = (\zeta_1', \rho', \varpi', \sigma_1', \sigma_2', \delta', \mathsf{msg}')$ となり, 攻撃 (A) が困難である事が示せた.

次に攻撃 (B) が困難である事を示す. 先の考察により $\mathcal{U}^*$ は α, β_1, β_2 を正しく生成する事から, 攻撃 (B) について, $\mathcal{H}$ の衝突困難性より

$$(\alpha =)\ a g^{t_1} y^{t_2} = g^{\tilde{\rho}} y^{\tilde{\varpi}} \tag{8}$$
$$(\beta_1 =)\ b_1^{\gamma} g^{t_3} \zeta_1^{t_5} = g^{\tilde{\sigma}_1} \tilde{\zeta}_1^{\tilde{\delta}} \tag{9}$$
$$(\beta_2 =)\ b_2^{\gamma} h^{t_4} \zeta_2^{t_5} = h^{\tilde{\sigma}_2} (z/\tilde{\zeta}_1^{\mathsf{info}'})^{\tilde{\delta}} \tag{10}$$
$$\tilde{\varepsilon} = \tilde{\varpi} + \tilde{\delta} \tag{11}$$

を満たす $\mathsf{fg} = (\tilde{\zeta}_1, \tilde{\rho}, \tilde{\varpi}, \tilde{\sigma}_1, \tilde{\sigma}_2, \tilde{\delta}, \mathsf{msg}, \mathsf{info}')$ のみ生成可能となる. 以下では $\mathsf{info}' \neq \mathsf{info}$ となるような fg の生成が困難である事を示す.

先ず式 (8) について, (g, y) の離散対数問題の困難性を仮定すれば $\tilde{\rho} = r + t_1 (= \rho)$, $\tilde{\varpi} = c + t_2 (= \varpi)$ とそれぞれ一意に定まる. すると式 (11) より $\tilde{\delta} = d + t_5 (= \delta)$ となり, 式 (9), (10) はそれぞれ

$$(\beta_1 =)\ g^{\gamma s_1 + t_3} \zeta_1^{d+t_5} = g^{\tilde{\sigma}_1} \tilde{\zeta}_1^{d+t_5} \tag{12}$$
$$(\beta_2 =)\ h^{\gamma s_2 + t_4} (z/\zeta_1^{\mathsf{info}})^{d+t_5} = h^{\tilde{\sigma}_2} (z/\tilde{\zeta}_1^{\mathsf{info}'})^{d+t_5} \tag{13}$$

と変形出来る. 特に式 (12), (13) からそれぞれ

$$(\tilde{\zeta}_1/\zeta_1)^{d+t_5} = g^{\gamma s_1 + t_3 - \tilde{\sigma}_1} \tag{14}$$
$$(\tilde{\zeta}_1^{\mathsf{info}'}/\zeta_1^{\mathsf{info}})^{d+t_5} = h^{\tilde{\sigma}_2 - \gamma s_2 - t_4} \tag{15}$$

が成り立つ. ここで d は $\mathcal{S}$ が生成した乱数であり, $\mathcal{U}^*$ が t_5 を生成した時点では明らかに d は Statistically-Hiding であるため, 無視出来る確率 $1/q$ を除いて $d + t_5 \neq 0 \bmod q$ となる. すると (15) について, もし $\tilde{\zeta}_1 = \zeta_1$ であれば, (h, ζ_1) の離散対数問題の困難性を仮定すれば $\mathsf{info}' = \mathsf{info}$, $\tilde{\sigma}_2 = \gamma s_2 + t_4 (= \sigma_2)$ と一意に定まる. 一方 $\tilde{\zeta}_1 \neq \zeta_1$ であるときは, $\log_g(\tilde{\zeta}_1/\zeta_1) = m$ ($\neq 0 \bmod q$) としたとき, (14) を満たす $\tilde{\sigma}_1$ を生成するためには $(g, \tilde{\zeta}_1/\zeta_1)$ の離散対数問題より m は既知である事が必要となる. 即ち一般性を失わずに $\tilde{\zeta}_1/\zeta_1 = g^m$ と書ける. すると (15) は

$$(g^{m \times \mathsf{info}'} \zeta_1^{\mathsf{info}' - \mathsf{info}})^{d+t_5} = h^{\tilde{\sigma}_2 - \gamma s_2 - t_4} \tag{16}$$

と変形でき，(g,h) 及び (ζ_1,h) の離散対数問題の困難性を仮定すれば $\tilde{\sigma}_2=\gamma s_2+t_4$ とし (16) の右辺は 1 と出来る．即ち (16) は $g^{m\times \mathsf{info}'}\zeta_1^{\mathsf{info}'-\mathsf{info}}=1$ と変形出来る．従って，(g,ζ_1) の離散対数問題の困難性を仮定すれば $m=0$, $\mathsf{info}'=\mathsf{info}$ となり仮定に反する．
以上から，攻撃 (B) が困難である事が示せた．■

(定理 2 の証明)　定理 1 の証明同様，攻撃 (A), (B) が困難である事を示す．なお証明方針も定理 1 の証明とほぼ同様であるため概要のみ示す．
$\mathcal{F}$, $\mathcal{H}$ は $\mathcal{U}^*$ から問い合わせがあれば任意入力に対してそれぞれ $\langle g\rangle$, $\mathbb{Z}_q$ 上の乱数を生成，出力するものとする．
攻撃 (A) が困難である事については，定理 1 の証明と同様の考察を行えば良い．従って以降では攻撃 (B) のみを考察の対象とする．
定理 1 の証明における考察から，攻撃 (B) について，$\mathcal{U}^*$ は $\mathcal{H}$ の衝突困難性より (8),(9),(11), 及び

$$(\beta_2=)\ b_2^{\gamma}h^{t_4}\zeta_2^{t_5}=h^{\tilde{\sigma}_2}(\tilde{z}/\tilde{\zeta}_1^{\mathsf{info}'})^{\tilde{\delta}} \tag{17}$$

を満たす $\mathsf{fg}=(\tilde{\zeta}_1,\tilde{\rho},\tilde{\varpi},\tilde{\sigma}_1,\tilde{\sigma}_2,\tilde{\delta},\mathsf{msg},\mathsf{info}')$ のみ生成可能となる (ここで $\tilde{z}=\mathcal{F}(p\|q\|g\|h\|y\|\mathsf{info}')$)．以下では $\mathsf{info}'\neq\mathsf{info}$ となるような fg の生成が困難である事を示す．なおここで $\mathcal{F}$ の衝突困難性より $(\mathsf{info}'\neq\mathsf{info})\Leftrightarrow(z\neq\tilde{z})$ と出来る．
先ず式 (8) について，(g,y) の離散対数問題の困難性を仮定すれば $\tilde{\rho}=r+t_1(=\rho)$, $\tilde{\varpi}=c+t_2(=\varpi)$ とそれぞれ一意に定まる．すると式 (11) より $\tilde{\delta}=d+t_5(=\delta)$ となり，式 (9), (17) はそれぞれ (12) 及び

$$(\beta_2=)\ h^{\gamma s_2+t_4}(z/\zeta_1)^{d+t_5}=h^{\tilde{\sigma}_2}(\tilde{z}/\tilde{\zeta}_1)^{d+t_5} \tag{18}$$

と変形出来る．特に式 (12), (18) からそれぞれ (14) 及び

$$(\tilde{\zeta}_1 z/(\zeta_1\tilde{z}))^{d+t_5}=h^{\tilde{\sigma}_2-\gamma s_2-t_4} \tag{19}$$

が成り立つ．ここで (19) について，定理 1 の証明における考察から $d+t_5\neq 0 \bmod q$ と出来るため，もし $\tilde{\zeta}_1=\zeta_1$ であれば，(19) を満たす $\tilde{z}$ $(\neq z)$, $\tilde{\sigma}_2$ を生成する事は $(h,z/\tilde{z})$ の離散対数問題を解く事に帰着される．しかしそれは $\tilde{z}$ が乱数であるため $\langle g\rangle$ 上の離散対数問題と等しい(注4)．従って $\tilde{z}=z$, 即ち $\mathsf{info}'=\mathsf{info}$ が必要条件となり仮定に反する．一方 $\tilde{\zeta}_1\neq\zeta_1$ であるときは，$\log_g(\tilde{\zeta}_1/\zeta_1)=m\ (\neq 0 \bmod q)$ としたとき，定理 1 の証明における考察から m は既知である事が必要となり，一般性を失わずに $\tilde{\zeta}_1/\zeta_1=g^m$ と書ける．すると (19) は

$$(g^m z/\tilde{z})^{d+t_5}=h^{\tilde{\sigma}_2-\gamma s_2-t_4} \tag{20}$$

と変形でき，$\langle g\rangle$ 上の離散対数問題 ($(h,z/\tilde{z})$ の離散対数問題) の困難性を仮定すれば $\tilde{\sigma}_2=\gamma s_2+t_4$, 即ち (20) の右辺は 1 となる．そして (20) の左辺について，$d+t_5\neq 0 \bmod q$ として良いため，結局 (16) は $g^m z/\tilde{z}=1$ と変形出来る．従って，$\langle g\rangle$ 上の離散対数問題 ($(g,z/\tilde{z})$ の離散対数問題) の困難性を仮定すれば $m=0$, $\tilde{z}=z$ となり仮定に反する．
以上から，攻撃 (B) が困難である事が示せた．■

(注4)：実際には $\mathcal{U}^*$ から $\mathcal{F}$ への問い合わせ最大回数を q_{F} としたとき，$\tilde{z}$ は q_{F} 通り存在し，攻撃者はその中から任意に $\tilde{z}$ を選ぶ事が出来る．

定理 1, 2 では，攻撃者のモデルについて「$\sum_{\mathsf{info}}\ell_{\mathsf{info}}=1$」と非常に強い仮定としている．しかし [2] では，「全ての info に対して $\ell_{\mathsf{info}}<poly(\log n)$」であれば偽造困難な事を証明しており，偽造を試みる攻撃者に対する提案方式の仮定を弱めた場合の考察を今後の課題とする．

5. まとめと今後の課題

ブラインド署名に部分開示機能及び追跡の機能を追加した「追跡可能な部分ブラインド署名方式」を提案した．同様の技術は今まで検討されていなかった事から，先ず実際に追跡可能な部分ブラインド署名の機能が要求されるアプリケーションを挙げ，その後，該署名及びそのセキュリティ要件を明確に定義した．そしてそれら要件のうち，今回は特に提案方式の偽造困難性について考察を行った．しかし今回の考察では攻撃者のモデルが非常に限定的であり，今後はより攻撃の仮定を弱めた場合の考察，そして追跡可能性，部分開示性の考察を行っていく予定である．

謝辞

文献 [2], [3] に関してご教示いただいた NTT 情報流通プラットフォーム研究所 阿部正幸氏に感謝いたします．

文　献

[1] M. Abe and E. Fujisaki, "How to date blind signatures," Proc. of ASIACRYPT '96, LNCS 1163, pp. 244–251, Springer-Verlag, 1996.

[2] M. Abe and T. Okamoto, "Provably secure partially blind signatures," Proc. of CRYPTO 2000, LNCS 1880, pp. 271–286, Springer-Verlag, 2000.

[3] M. Abe and M. Ohkubo, "Provably secure fair blind signatures with tight revocation," Proc. of ASIACRYPT '01, LNCS 2248, pp. 583–601, Springer-Verlag, 2001.

[4] D. Chaum, "Blind signatures for untraceable payments," Proc. of CRYPTO '82, pp. 199–204, Prenum Publishing Corporation, 1982.

[5] D. Chaum, "Online cash checks," Proc. of EUROCRYPT '89, LNCS 434, Springer-Verlag, pp. 288–293, 1990.

[6] 千田，谷口，塩野入，金井，"代理アクセスを利用した匿名認証方式" 第 28 回 CSEC 研究発表会予稿集, pp. 235–240, 2005 年 3 月.

[7] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," Proc. of AUSCRYPT '92, LNCS 718, pp. 244–251, Springer-Verlag, 1992.

[8] M. Stadler, J.-M. Piveteau, and J. Camenisch, "Fair blind signatures," Proc. of EUROCRYPT '95, LNCS 921, pp. 209–219, Springer-Verlag, 1995.