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

2005－ＣＳＥＣ－30（23）
2005／7／21

オブリビアス署名の構成手法

椎名　信行†　岡本　健†　岡本　栄司†

† 筑波大学大学院システム情報工学研究科　〒305-8573 茨城県つくば市天王台 1-1-1
E-mail: †senna@cipher.risk.tsukuba.ac.jp, {ken,okamoto}@risk.tsukuba.ac.jp

あらまし　オブリビアス署名の暗号系は，署名者 $\mathcal{S}$，受取人 $\mathcal{R}$，検証者 $\mathcal{V}$ という 3 つのエンティティから構成される．この暗号系では，n 個のメッセージに対して $\mathcal{R}$ は任意のメッセージの署名を得られる一方，$\mathcal{S}$ はどのメッセージに署名したかわからないという性質があり，$\mathcal{R}$ のプライバシを保護するのに有効である．そこで，本稿ではオブリビアス署名の明確な定義を示し，実用性に優れた方式を提案する．提案方式は 2 種類あり，それぞれ電子署名標準である DSA 及び ECDSA に基づく．また，オブリビアス署名はオブリビアス通信の署名版と考えることができるため，両者の関係について詳しく述べる．最後に，提案方式について種々の観点から評価を行い，従来方式との比較，検討をすることで，各方式の特徴を示す．

キーワード　オブリビアス署名，オブリビアス通信，DSA，ECDSA，電子署名標準

Oblivious Signature, Revised

Nobuyuki SHIINA†, Takeshi OKAMOTO†, and Eiji OKAMOTO†

† Graduate School of Systems and Information Engineering, University of Tsukuba　Tennodai 1-1-1, Tsukuba, Ibaraki, 305-8573 Japan
E-mail: †senna@cipher.risk.tsukuba.ac.jp, {ken,okamoto}@risk.tsukuba.ac.jp

Abstract　An oblivious signature scheme consists of three entities: a signer $\mathcal{S}$, a recipient $\mathcal{R}$ and a verifier $\mathcal{V}$. In this scheme, $\mathcal{R}$ can obtain k signatures from n messages whereas $\mathcal{S}$ cannot know which messages $\mathcal{R}$ chose. Therefore, such a scheme can be used to keep the user's privacy. In this paper, we formalize the notion of oblivious signature and propose two efficient schemes: DSA and ECDSA based schemes. We also give the relation between oblivious signatures and oblivious transfer. Finally, we discuss the properties of our schemes by evaluating communication cost, computational cost and so on.

Key words　oblivious signatures, oblivious transfer, DSA, ECDSA, digital signature standard

1. まえがき

オブリビアス署名は Chen [5] により提案された特殊な電子署名方式である．オブリビアス署名の暗号系は，署名者 $\mathcal{S}$，受取人 $\mathcal{R}$，検証者 $\mathcal{V}$ という 3 つのエンティティから構成され，n 個のメッセージに対して，

- $\mathcal{R}$ は任意のメッセージの署名を得られる
- $\mathcal{S}$ はどのメッセージに署名したかわからない

という特徴を有する(注1)．したがって，$\mathcal{R}$ はどのメッセージに対して署名を得たかを秘密にしたまま任意のメッセージの署名を得ることができるため，$\mathcal{R}$ のプライバシを保護するのに有効である．

具体的な例として，オンラインショッピングを利用してデジタルコンテンツを購入する場合が挙げられる．この場合，$\mathcal{S}$ は売り手，$\mathcal{R}$ は買い手，メッセージはデジタルコンテンツと対応づけることができ，署名は実社会における領収書に相当する．ここで，$\mathcal{R}$ は $\mathcal{S}$ により署名がなされた署名付きデジタルコンテンツを購入したいが，昨今の個人情報漏洩事件の多発から，どのデジタルコンテンツを購入したかについては秘密にしたいという要望があったとする．このような場合，オブリビアス署名を用いれば問題を解決することができる．

また，オブリビアス署名はオブリビアス通信の署名版と考えることができる．オブリビアス通信には大きく分けて 2 種類あり，1 つは単にオブリビアス通信 (OT) と呼ばれる次のような通信 [16] を意味する．送信者 $\mathcal{A}$ がメッセージを受信者 $\mathcal{B}$ に送

(注1)：[5] では，ここで取り上げた特徴を持つ方式以外に，複数の署名者に対するオブリビアス署名方式を定義している．また複数の受取人に対する方式，さらにはメッセージ，署名者，受取人が同時に複数となる方式も当然考えられる．しかしながら，いずれの方式もここで取り上げた方式を拡張することで簡単に実現できる．したがって，本稿では煩雑さを避けるため説明を省略する．

るとき，1/2の確率で$\mathcal{B}$に伝わるが，伝わったかどうかを$\mathcal{A}$は一切知ることはできない．しかし，暗号プロトコルにおいてオブリビアス通信が使われる場合，1-out-of-2 オブリビアス通信 (OT_1^2) の形 [7] で使われることが多い．OT_1^2 では，$\mathcal{A}$ が 2 つのメッセージを $\mathcal{B}$ に送るとき，どちらか 1 つのみが $\mathcal{B}$ に伝わるが，どちらを受け取ったかを $\mathcal{A}$ は知ることができない．オブリビアス署名はオブリビアス通信の署名版であることから，これら 2 種類の方式はオブリビアス署名にも当てはまる．すなわち，オブリビアス署名も

- $\mathcal{R}$ は確率 1/2 で署名を得られる
- $\mathcal{R}$ は 2 つの署名のどちらか 1 つだけを得られる

の 2 つに大別できる．ここで，前者を単に OS，後者を OS_1^2 と表記することにする．同様に，1-out-of-n OT を OT_1^n，k-out-of-n OT を OT_k^n，1-out-of-n OS を OS_1^n，k-out-of-n OS を OS_k^n と表記する．本稿では最も一般的な OS_k^n を扱う．

ここで注意しなくてはならない点は，オブリビアス署名は単にオブリビアス通信を使用して署名を送ることとは全く違うという点である．もちろん，オブリビアス通信におけるメッセージを署名とみなすことで，両者が実現することは同じになる．また，オブリビアス通信を使用した場合，どのような署名方式にも適用できるという利点がある．しかしながら，この場合，署名とオブリビアス通信という 2 つの操作をそれぞれ独立に行わなくてはならないため，計算コストが増大し，効率が悪いという問題が生じる．オブリビアス通信自体の計算コストも大きいため，なおさら効率が悪い．それに対し，オブリビアス署名ではこれら 2 つの操作を同時に行うため，単にオブリビアス通信を使用するのに比べて効率が良い．

また，同じく $\mathcal{R}$ のプライバシを保護する手法としてブラインド署名 [4] が存在する．ブラインド署名とオブリビアス署名の明確な違いは，前者が $\mathcal{S}$ はメッセージの内容が一切わからないのに対し(注2)，後者は n 個のどのメッセージに署名するかはわからないがメッセージの内容はわかるという点である．したがって，前述したオンラインショッピングの例を考えたとき，ブラインド署名を用いて実現するとなると，$\mathcal{S}$ は全く不明なデジタルコンテンツに領収書を発行することになり，$\mathcal{S}$ の負担が大きすぎるため実用的ではない．

これまでの研究から，オブリビアス署名にはいくつかの方式が存在する．[5] ではハッシュ関数の一方向性を利用した Fiat-Shamir の暗号系に基づく方式，[20] ではべき乗剰余演算の一方向性を利用した Schnorr，RSA の暗号系に基づく方式がそれぞれ提案されている．しかしながら，これらの論文ではオブリビアス署名の明確な定義が与えられていなかった．そこで，本稿ではオブリビアス署名の明確な定義を示し，さらに，オブリビアス性を構築するのに [20] のアプローチを利用した方式を提案する．提案方式は 2 種類あり，それぞれ電子署名標準である DSA 及び ECDSA に基づく．提案方式の利点としては，署名生成，検証時において，国際的に規格化されている署名方式を容易に適用できることが挙げられる．これは最終的に作成された署名構造がこれらの規格と同一になるということを意味している．オンラインショッピングやオンラインバンキングの運用を想定して暗号プロトコルを実装する場合，通常はこれらの規格に基づいてプログラムを構築するのが一般的である．したがって，提案方式がこのような性質を有していることは実用性という点で優れていると言える．

本稿の構成としては，2 節でオブリビアス署名の定義を与える．3 節では，DSA 及び ECDSA に基づくオブリビアス署名方式を提案する．4 節では，提案方式について種々の観点から評価を行い，従来方式との比較，検討をすることで，各方式の特徴を示す．最後に 5 節でまとめる．

(注2)：[1] では，メッセージの一部がわかるブラインド署名方式が提案されている．

2. オブリビアス署名の定義

本節では，k-out-of-n オブリビアス署名 (OS_k^n) の定義を与え，OS_k^n が満たすべき要件を示す．オブリビアス署名はブラインド署名と類似しているため，[2], [9] に従って定義する．

[Definition 1] (オブリビアス署名) OS_k^n とは，$(\mathcal{G}, \mathcal{S}, \mathcal{R}, \mathcal{V})$ の組で，以下を満たすものである．

- $(pk, sk) \leftarrow \mathcal{G}(1^t)$: $\mathcal{G}$ は確率的多項式時間アルゴリズムであり，セキュリティパラメータ t を入力に取り，公開鍵 pk とそれに対応する秘密鍵 sk を出力する．
- $(< \text{完了/未完了} >, (< (\sigma_1, \cdots, \sigma_k) \text{/失敗} >) \leftarrow interact(\mathcal{S}(pk, sk, m_1, \cdots, m_n), \mathcal{R}(pk, \ell_1, \cdots, \ell_k))$: $\mathcal{S}$ と $\mathcal{R}$ は確率的多項式時間 Turing 機械 (PPTM) であり，どちらも read-only 入力テープ，write-only 出力テープ，read/write 記録テープ，read-only 乱数テープ，read-only 伝達テープ，write-only 伝達テープを持つ．$\mathcal{S}$ の入力テープには $\mathcal{G}(1^t)$ により生成された (pk, sk) のペアと n 個のメッセージ $m_1, \cdots, m_n$ が入力されており，$\mathcal{R}$ の入力テープには pk と $\{\ell_1, \cdots, \ell_k\} \subseteq \{1, \cdots, n\}$ を満たす $\ell_1, \cdots, \ell_k$ が入力されている．$\mathcal{S}$ と $\mathcal{R}$ は出力テープ，乱数テープ，伝達テープを用いて相互にやり取りし，多項式時間で結果を出力テープに出力する．最終的には，$\mathcal{S}$ の出力テープには完了あるいは未完了が書き込まれ，$\mathcal{R}$ の出力テープには $m_{l_1}, \cdots, m_{l_k}$ に対する署名 $\sigma_1, \cdots, \sigma_k$ あるいは失敗が書き込まれる．
- $< accept/reject > \leftarrow \mathcal{V}(pk, m_{l_i}, \sigma_i)$: $\mathcal{V}$ は確定的多項式時間アルゴリズムであり，公開鍵 pk，メッセージ m_{l_i}，署名 σ_i $(1 \leqq i \leqq k)$ を入力に取り，*accept* あるいは *reject* を出力する．

[Definition 2] (完全性) 正しく $\mathcal{G}$, $\mathcal{S}$, $\mathcal{R}$ を行なえば，$Pr[\mathcal{V}(pk, m_{l_i}, \sigma_i) = accept] = 1$ $(1 \leqq i \leqq k)$ が成り立つ．

安全性の定義は，オブリビアス通信同様，受取人 $\mathcal{R}$ と署名者 $\mathcal{S}$ で分かれる [6], [11], [13], [14]．以下では，$view_{\tilde{\mathcal{S}}}(\tilde{\mathcal{S}}, \mathcal{R})$ は攻撃者 $\tilde{\mathcal{S}}$ が $\mathcal{S}$ の代わりに $\mathcal{R}$ とやり取りをし，$\mathcal{R}$ が選択した $\{\ell_1, \cdots, \ell_k\} \subseteq \{1, \cdots, n\}$ を導き出す試行を表す．同様に，$view_{\tilde{\mathcal{R}}}(\mathcal{S}, \tilde{\mathcal{R}})$ は攻撃者 $\tilde{\mathcal{R}}$ が $\mathcal{R}$ の代わりに $\mathcal{S}$ とやり取りをし，$\tilde{\mathcal{R}}$ が選択した $m_{\ell_1}, \cdots, m_{\ell_k}$ 以外のメッセージに対する署名を

導き出す試行を表す.

[Definition 3] (識別不可能性)

– $\mathcal{R}$ の安全性 : 任意の PPTM 攻撃者 $\tilde{\mathcal{S}}$ は, 任意の公開鍵 pk, 相異なる二つの集合 $L = \{\ell_1, \cdots, \ell_k\}, L' = \{\ell_1', \cdots, \ell_k'\}$, $L, L' \subseteqq \{1, \cdots, n\}$ に対して, $\mathcal{R}$ が L を選んだ場合と L' を選んだ場合の識別が統計学的に不可能である. すなわち,

$$view_{\tilde{\mathcal{S}}}\left(\tilde{\mathcal{S}}, \mathcal{R}(pk, L)\right) \stackrel{s}{\equiv} view_{\tilde{\mathcal{S}}}\left(\tilde{\mathcal{S}}, \mathcal{R}(pk, L')\right)$$

が成り立つ. ただし, $\stackrel{s}{\equiv}$ は統計学的に同一であることを表す. これは直感的には $\tilde{\mathcal{S}}$ は $\mathcal{R}$ がどの $\{\ell_1, \cdots, \ell_k\} \subseteqq \{1, \cdots, n\}$ を選んだかわからないことを意味する.

– $\mathcal{S}$ の安全性 : 任意の PPTM 攻撃者 $\tilde{\mathcal{R}}$ は, 任意の公開鍵 pk, 秘密鍵 sk, メッセージ $m_1, \cdots, m_n$, 乱数 $\gamma_1, \cdots, \gamma_{n-k}$, $\{\ell_1, \cdots, \ell_k\} \subseteqq \{1, \cdots, n\}$ に対して, $\mathcal{S}$ が $m_1, \cdots, m_n$ を選んだ場合と $m_{\ell_1}, \cdots, m_{\ell_k}, \gamma_1, \cdots, \gamma_{n-k}$ を選んだ場合の識別が計算量的に不可能である. すなわち,

$$view_{\tilde{R}}\left(\mathcal{S}(pk, sk, m_1, \cdots, m_n), \tilde{\mathcal{R}}\right) \stackrel{c}{\equiv} view_{\tilde{R}}\left(\mathcal{S}(pk, sk, m_{\ell_1}, \cdots, m_{\ell_k}, \gamma_1, \cdots, \gamma_{n-k}), \tilde{\mathcal{R}}\right)$$

が成り立つ. ただし, $\stackrel{c}{\equiv}$ は計算量的に同一であることを表す. これは直感的には $\tilde{\mathcal{R}}$ は $m_{\ell_1}, \cdots, m_{\ell_k}$ に対する署名以外得られないことを意味する.

提案方式は 2 種類あり, それぞれ DSA 及び ECDSA に基づき, $\mathcal{S}$ の安全性は DLP と ECDLP の困難性の仮定に帰着する.

[Assumption 1] (DLP) p を素数とし, $\mathbb{Z}_p^*$ の原始元を g としたとき, 任意の $y \in \mathbb{Z}_p^*$ に対して,

$$y = g^x \bmod p$$

を満たす x を求めることは計算量的に不可能である.

[Assumption 2] (ECDLP) p を素数とし, 有限体 $\mathbb{F}_p$ 上の楕円曲線を E としたとき, $Y, G \in E(\mathbb{F}_p)$ に対して,

$$Y = xG = \sum_{i=1}^{x} G$$

を満たす x を求めることは計算量的に不可能である.

3. 提案方式

本節では, k-out-of-n オブリビアス署名 (OS_k^n) 方式を提案する. 提案方式は 2 種類あり, それぞれ電子署名標準である DSA 及び ECDSA に基づく.

3.1 DSA 型

【鍵生成】

$\mathcal{S}$ は $q \mid p-1$ を満たす素数 p, q を生成し, 乗法群 $\mathbb{Z}_p^*$ の位数 q の部分群の生成元 $g, \tilde{g}$ を定める. また, 乱数 $x \in_R \mathbb{Z}_q$ を生成し, $y = g^x \bmod p$ を計算する. 最後に, $(y, g, \tilde{g}, p, q)$ を公開鍵とし, x を秘密鍵とする.

【署名生成】

step 1 $\mathcal{R}$ は $\{\ell_1, \cdots, \ell_k\} \subseteqq \{1, \cdots, n\}$ を満たす $\{\ell_1, \cdots, \ell_k\}$ を選択する.

step 2 $\mathcal{R}$ は $i = 1, \cdots, k$ に対して, 乱数 $r_i \in_R \mathbb{Z}_q$ を生成し,

$$c_i = g^{r_i} \tilde{g}^{\ell_i} \bmod p$$

を計算して, c_i を $\mathcal{S}$ に送る.

step 3 $\mathcal{S}$ は $i = 1, \cdots, k$, $j = 1, \cdots, n$ に対して, 乱数 $\tilde{r}_{i,j} \in_R \mathbb{Z}_q$ を生成し,

$$\begin{cases} \tilde{u}_{i,j} = \left(\left(c_i / \tilde{g}^j\right)^{\tilde{r}_{i,j}} \bmod p\right) \bmod q \\ \tilde{v}_{i,j} = (\mathcal{H}(\tilde{m}_j) + x\tilde{u}_{i,j})/\tilde{r}_{i,j} \bmod q \end{cases}$$

を計算して, $\tilde{m}_j, \tilde{u}_{i,j}, \tilde{v}_{i,j}$ を $\mathcal{R}$ に送る.

step 4 $\mathcal{R}$ は $i = 1, \cdots, k$ に対して,

$$\begin{cases} m_i = \tilde{m}_{\ell_i} \\ u_i = \tilde{u}_{i,\ell_i} \\ v_i = \tilde{v}_{i,\ell_i}/r_i \bmod q \end{cases}$$

を計算する.

【署名文】

メッセージ m_i に対する署名文は (u_i, v_i).

【署名検証】

$\mathcal{V}$ は,

$$u_i \stackrel{?}{=} \left(g^{\mathcal{H}(m_i)v_i^{-1}} y^{u_i v_i^{-1}} \bmod p\right) \bmod q$$

が成り立つかどうか確認する. 成り立つならば受理し, そうでなければ棄却する.

[Theorem 1] DSA 型 OS_k^n は, 完全性を満たす.

(証明)

$$\begin{aligned} g^{\mathcal{H}(m_i)v_i^{-1}} y^{u_i v_i^{-1}} &= g^{\mathcal{H}(\tilde{m}_{l_i})v_i^{-1}} (g^x)^{\tilde{u}_{i,l_i} v_i^{-1}} \\ &= g^{v_i^{-1}\left(\mathcal{H}(\tilde{m}_{l_i}) + x\tilde{u}_{i,l_i}\right)} \\ &= g^{(\tilde{v}_{i,\ell_i}/r_i)^{-1}\tilde{v}_{i,l_i}\tilde{r}_{i,l_i}} \\ &= g^{r_i \tilde{r}_{i,l_i}} \\ &= u_i \qquad \square \end{aligned}$$

[Theorem 2] DSA 型 OS_k^n において, $\mathcal{R}$ の選択 $\{\ell_1, \cdots, \ell_k\}$ は情報理論的に安全である.

(証明) $\mathcal{R}$ の選択 $\{\ell_1, \cdots, \ell_k\} \subseteqq \{1, \cdots, n\}$ とそれとは異なる任意の $\{\ell_1', \cdots, \ell_k'\} \subseteqq \{1, \cdots, n\}$ に対して,

$$c_i = g^{r_i} \tilde{g}^{\ell_i} = g^{r_i'} \tilde{g}^{\ell_i'} \bmod p \quad (1 \leqq i \leqq k)$$

を満たす r_i, r_i' $(1 \leqq i \leqq k)$ が必ず存在する. したがって, $\mathcal{S}$ は $\mathcal{R}$ の選択 $\{\ell_1, \cdots, \ell_k\}$ について, 無限の計算資源を持っていたとしても一切の情報を得ることができない. $\square$

[Theorem 3] DSA 型 OS_k^n において, DLP が困難であると仮定すると, $\mathcal{R}$ は選択していないメッセージ m_{l_α} $(l_\alpha \notin \{\ell_1, \cdots, \ell_k\})$ に対する署名を得ることはできない.

(証明) $\mathcal{R}$ は任意の $1 \leqq i \leqq k$ に対して,

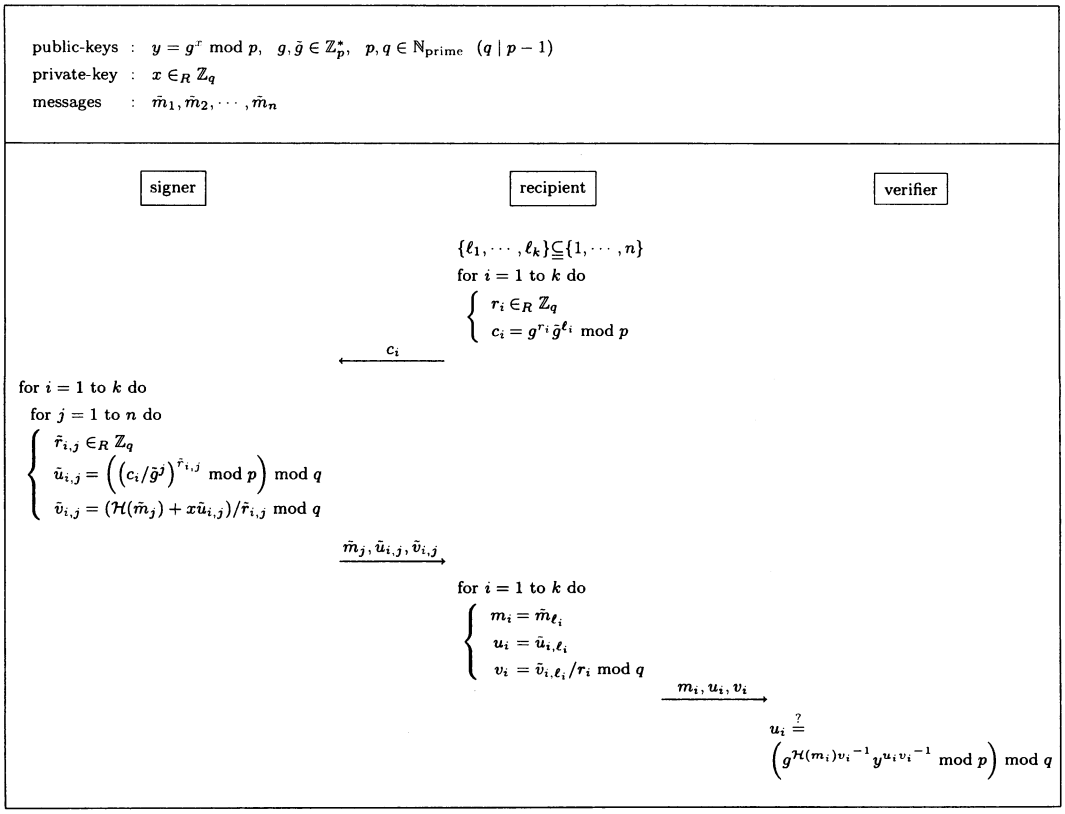

図 1　オブリビアス署名方式 (DSA 型)

Fig. 1　Oblivious Signature Scheme (DSA type)

$$c_i = g^{r_i}\tilde{g}^{l_i} = g^{r_\alpha}\tilde{g}^{l_\alpha} \bmod p$$

を満たす (r_i, l_i) と (r_α, l_α) の組を求めることはできない．さもなければ，$\mathcal{R}$ は $\log_g \tilde{g} = (r_\alpha - r_i)/(l_i - l_\alpha)$ から $\log_g \tilde{g}$ を求めることができ，DLP の困難性に矛盾する．したがって，$\mathcal{R}$ は $m_{\ell_1}, \cdots, m_{\ell_k}$ に対する署名以外得ることはできない．　□

3.2 ECDSA 型

【鍵生成】

$\mathcal{S}$ は素数 p を生成し，$4a^3 + 27b^2 \neq 0$ を満たす $a, b \in \mathbb{F}_p$ を選択して，有限体 $\mathbb{F}_p$ 上の楕円曲線 $E : y^2 = x^3 + ax + b$ を定義する．次に，位数 q のベースポイント $G, \tilde{G} \in E(\mathbb{F}_p)$ を定める．また，乱数 $d \in_R \mathbb{Z}_q$ を生成し，$Q = dG$ を計算する．最後に，$(Q, p, a, b, G, \tilde{G}, q)$ を公開鍵とし，d を秘密鍵とする．

【署名生成】

step 1　$\mathcal{R}$ は $\{\ell_1, \cdots, \ell_k\} \subseteqq \{1, \cdots, n\}$ を満たす $\{\ell_1, \cdots, \ell_k\}$ を選択する．

step 2　$\mathcal{R}$ は $i = 1, \cdots, k$ に対して，乱数 $r_i \in_R \mathbb{Z}_q$ を生成し，

$$C_i = r_i G + \ell_i \tilde{G}$$

を計算して，C_i を $\mathcal{S}$ に送る．

step 3　$\mathcal{S}$ は $i = 1, \cdots, k$，$j = 1, \cdots, n$ に対して，乱数 $\tilde{r}_{i,j} \in_R \mathbb{Z}_q$ を生成し，

$$\begin{cases} (x_{i,j}, y_{i,j}) = \tilde{r}_{i,j}(C_i - j\tilde{G}) \\ \tilde{s}_{i,j} = x_{i,j} \bmod q \\ \tilde{t}_{i,j} = (\mathcal{H}(\tilde{m}_j) + d\tilde{s}_{i,j})/\tilde{r}_{i,j} \bmod q \end{cases}$$

を計算して，$\tilde{m}_j, \tilde{s}_{i,j}, \tilde{t}_{i,j}$ を $\mathcal{R}$ に送る．

step 4　$\mathcal{R}$ は $i = 1, \cdots, k$ に対して，

$$\begin{cases} m_i = \tilde{m}_{\ell_i} \\ s_i = \tilde{s}_{i,\ell_i} \\ t_i = \tilde{t}_{i,\ell_i}/r_i \bmod q \end{cases}$$

を計算する．

【署名文】

メッセージ m_i に対する署名文は (s_i, t_i)．

【署名検証】

$\mathcal{V}$ は，$(x_i, y_i) = \mathcal{H}(m_i)t_i^{-1}G + s_i t_i^{-1} Q$ を計算し，

$$x_i \bmod q \stackrel{?}{=} s_i$$

が成り立つかどうか確認する．成り立つならば受理し，そうでなければ棄却する．

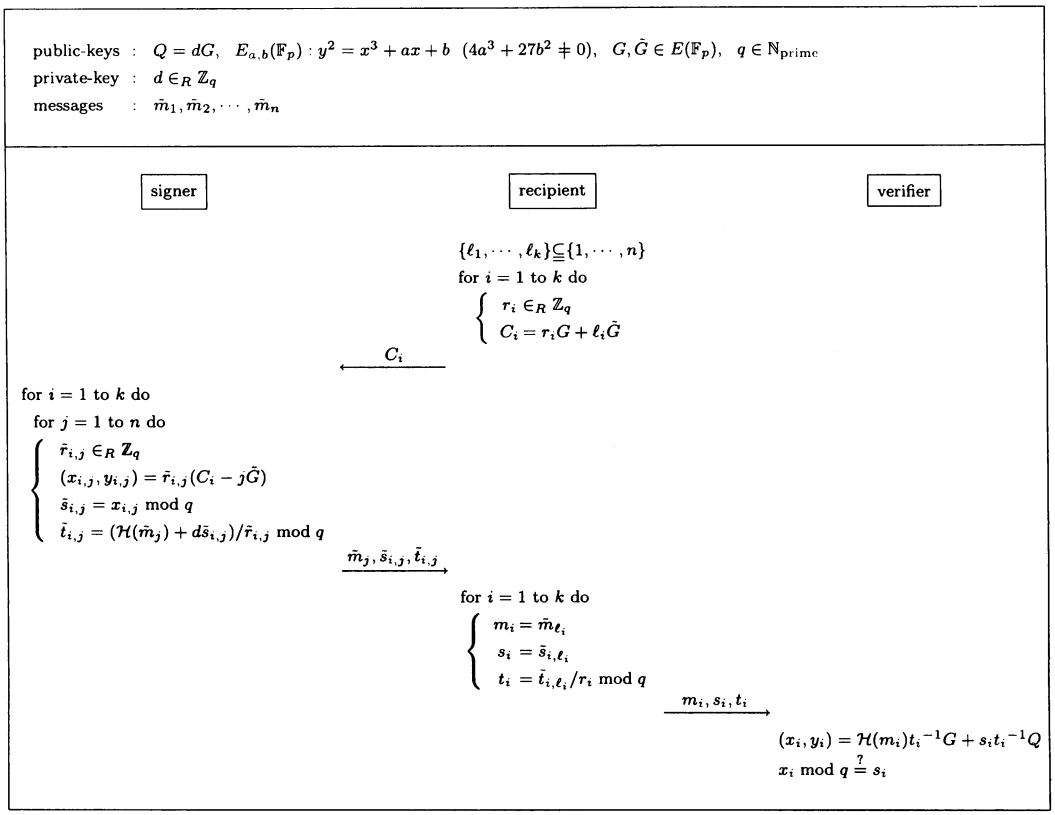

図 2 オブリビアス署名方式 (ECDSA 型)
Fig. 2 Oblivious Signature Scheme (ECDSA type)

[Theorem 4] ECDSA 型 OS_k^n は，完全性を満たす．
(証明)

$$\begin{aligned}\mathcal{H}(m_i)t_i^{-1}G + s_i t_i^{-1}Q &= \mathcal{H}(m_i)t_i^{-1}G + s_i t_i^{-1}dG \\ &= t_i^{-1}\left(\mathcal{H}(\tilde{m}_{l_i}) + d\tilde{s}_{i,l_i}\right)G \\ &= \left(\tilde{t}_{i,l_i}/r_i\right)^{-1}\tilde{t}_{i,l_i}\tilde{r}_{i,l_i}G \\ &= r_i\tilde{r}_{i,l_i}G \\ &= (x_{i,l_i}, y_{i,l_i}) \quad \square\end{aligned}$$

[Theorem 5] ECDSA 型 OS_k^n において，$\mathcal{R}$ の選択 $\{\ell_1, \cdots, \ell_k\}$ は情報理論的に安全である．
(証明) $\mathcal{R}$ の選択 $\{\ell_1, \cdots, \ell_k\} \subseteqq \{1, \cdots, n\}$ とそれとは異なる任意の $\{\ell_1', \cdots, \ell_k'\} \subseteqq \{1, \cdots, n\}$ に対して，

$$C_i = r_i G + \ell_i \tilde{G} = r_i' G + \ell_i' \tilde{G} \quad (1 \leqq i \leqq k)$$

を満たす r_i, r_i' $(1 \leqq i \leqq k)$ が必ず存在する．したがって，$\mathcal{S}$ は $\mathcal{R}$ の選択 $\{\ell_1, \cdots, \ell_k\}$ について，無限の計算資源を持っていたとしても一切の情報を得ることができない． $\square$

[Theorem 6] ECDSA 型 OS_k^n において，ECDLP が困難であると仮定すると，$\mathcal{R}$ は選択していないメッセージ m_{l_α} $(l_\alpha \notin \{\ell_1, \cdots, \ell_k\})$ に対する署名を得ることはできない．
(証明) $\mathcal{R}$ は任意の $1 \leqq i \leqq k$ に対して，

$$C_i = r_i G + l_i \tilde{G} = r_\alpha G + l_\alpha \tilde{G}$$

を満たす (r_i, l_i) と (r_α, l_α) の組を求めることはできない．さもなければ，$\mathcal{R}$ は $\log_G \tilde{G} = (r_\alpha - r_i)/(l_i - l_\alpha)$ から $\log_G \tilde{G}$ を求めることができ，ECDLP の困難性に矛盾する．したがって，$\mathcal{R}$ は $m_{\ell_1}, \cdots, m_{\ell_k}$ に対する署名以外得ることはできない． $\square$

4. 考　　察

本節では，提案方式について種々の観点から評価を行い，従来方式との比較，検討をすることで，各方式の特徴を示す．

4.1 性能評価

表 1,2,3 に従来方式 (Fiat-Shamir 型，Schnorr 型，RSA 型)，提案方式 (DSA 型，ECDSA 型)，単にオブリビアス通信を利用した方式 (DSA-OT 型)(注3) の性能評価を示す．ただし，各方式の差異を明らかにするため，表 1 中の通信量にはメッセージのデータサイズは加算しないものとする．また，有限体上の演

(注3)：オブリビアス通信には多くの方式が存在するが，ここでは [18] の方式を利用した場合を考える．また，署名方式は DSA を用いるものとする．

表 1 性能評価 (データサイズ，通信量)

Table 1 Comparison of OS_k^n schemes in data size and communication cost

方式	データサイズ (ビット)			通信量 (ビット)	
	公開鍵	秘密鍵	署名長	署名者→受取人	署名者←受取人
Fiat-Shamir 型	$3\|p\|+\|q\|$	$\|q\|$	$6\|p\|+2\|q\|$	$3n\|p\|+kn\|q\|$	$k\|q\|$
Schnorr 型	$3\|p\|+\|q\|$	$\|q\|$	$2\|q\|$	$2kn\|q\|$	$k\|p\|$
RSA 型	$\|N\|+\|e\|$	$\|N\|$	$\|N\|$	$kn\|N\|$	$k\|N\|$
DSA 型	$3\|p\|+\|q\|$	$\|q\|$	$2\|q\|$	$2kn\|q\|$	$k\|p\|$
ECDSA 型	$7\|p\|+\|q\|$	$\|q\|$	$2\|q\|$	$2kn\|q\|$	$2k\|p\|$
DSA-OT 型	$3\|p\|+\|q\|$	$\|q\|$	$2\|q\|$	$2kn\|p\|$	$k\|p\|$

表 2 性能評価 (署名者の計算量)

Table 2 Comparison of OS_k^n schemes in computational cost for a signer

方式	計算量 (署名者)
Fiat-Shamir 型	$(3(3n+1)\|q\|/4+k\|q\|^2/\|p\|^2)M_p$
Schnorr 型	$((2kn+3)\|q\|/4+kn\|q\|^2/\|p\|^2+2kn+n-1)M_p+nI_p$
RSA 型	$(5kn\|N\|/16+2kn+n/2-1/2)M_N+2nI_p$
DSA 型	$(5kn\|q\|/4+2kn\|q\|^2/\|p\|^2+kn+n-1)M_p+nI_p+knI_q$
ECDSA 型	$(39kn\|q\|/8+2kn\|q\|^2/\|p\|^2+11(kn+n-1)/4)M_p+(3kn\|q\|/2+kn+n-1)I_p+knI_q$
DSA-OT 型	$((7kn+2k+3)\|q\|/4+2k\|q\|^2/\|p\|^2+2kn+n-1)M_p+nI_p+kI_q$

表 3 性能評価 (受取人の計算量)

Table 3 Comparison of OS_k^n schemes in computational cost for a recipient

方式	計算量 (受取人)
Fiat-Shamir 型	$(3(19k+2)\|q\|/8+k\|q\|^2/\|p\|^2+k)M_p$
Schnorr 型	$((2k+3)\|q\|/4+n+k-1)M_p$
RSA 型	$(5k\|e\|/8+n/2+3k-1/2)M_N+2nI_p$
DSA 型	$((2k+3)\|q\|/4+n+2k-1)M_p+kI_q$
ECDSA 型	$(39k\|q\|/8+k\|q\|^2/\|p\|^2+11(k+n-1)/4)M_p+(3k\|q\|/2+k+n-1)I_p+kI_q$
DSA-OT 型	$((7k+3)\|q\|/4+n+2k-1)M_p+kI_p$

算についてはバイナリ法 [12] を用いており，具体的な計算手法は [10], [19] に従う．RSA 型については，中国人の剰余定理を利用して演算の高速化を行う．検証にかかる計算量は通常の署名と比べて Fiat-Shamir 型では 2 倍，他の方式では通常の署名と同等なため，具体的な計算量の記述は省略する．表中で用いられる記号は各方式で使われている記号と同じ意味を持ち，同じ記号であっても他の方式とは異なることに注意しなくてはならない．例えば，DSA 型での p と ECDSA 型での p は異なる．また，M_p は法のサイズが $|p|$ ビットでの 1 回の乗算剰余を意味し，I_p, I_q はそれぞれ法のサイズが $|p|, |q|$ ビットでの 1 回の逆元計算を意味するものとする．

4.2 各種方式の解析

Fiat-Shamir 型 [5]：この方式は Fiat-Shamir 署名 [8] に基づいており，全ての 3 交信型の署名方式に適用可能である．他の方式とは異なり，オブリビアス性という性質を満たすためにハッシュ関数の一方向性を明示的に利用している．したがって，ハッシュ関数における逆計算が難しいという強い仮定を要する．また，その他の欠点として通信回数，通信量，計算量という点で非常に効率が悪いことが挙げられる．通信回数は他の方式が 2 回であるのに対し，3 回必要となる．さらに，1 回あたりに送るパラメータ数も多いことから全体の通信量も多く，これらのパラメータを用いて演算を行うため必要な計算量も多い．また，最終的に作成される署名は 2 つの Fiat-Shamir 署名の組であり，その 2 つを合わせることで初めて署名として機能する．そのため，署名サイズも大きく，署名構造も通常の Fiat-Shamir 署名と異なるという欠点も挙げられる．この方式の利点としては，witness-hiding 方式を用いることで，他の方式にはない唯一の特徴を実現できることが挙げられる．その特徴とは，$\mathcal{R}$ は n 個のメッセージのどの k 個の署名を得たかを秘密にしたまま，確かにどれか k 個の署名を持っていることを $\mathcal{V}$ に証明することができるというものである．これにより，他の方式よりも $\mathcal{R}$ のプライバシを保護することが可能になる．

Schnorr 型 [20]：この方式は Schnorr 署名 [17] に基づいており，最終的に得られる署名は通常の Schnorr 署名と同じになる．Fiat-Shamir 型と比べて鍵長は同じであるが，署名長，通信量，計算量の点で Fiat-Shamir 型よりはるかに効率が良い．例えば，最も基本的な OS_1^2 の場合，両方式における p, q を $|p|=1024, |q|=160$ とすると，Fiat-Shamir 型に比べて，署名長は約 95%，全体の通信量は約 75%，署名生成の計算量は約 64%の削減となる．

RSA 型 [20]：これは RSA 署名 [15] を利用した方式であり，最終的に得られる署名は通常の RSA 署名と同じになる．したがって，この方式の中で用いるハッシュ関数を $\mathcal{H}: \{0,1\}^* \rightarrow \mathbb{Z}_N$ とした場合，得られる署名は FDH 方式と同じ構成になり，高い安全性を満たすという利点がある [3]．また，署名文の構造を RSA-PSS にすることも可能であり，高い汎用性を有する．

DSA 型：これは電子署名標準である DSA を利用した方式であり，署名生成，検証時において DSA に変更を一切加えることなくそのまま利用できるという利点がある．オンラインショッピングやオンラインバンキングの運用を想定して暗号プロトコルを実装する場合，国際的に標準化されている規格に基づいて構築するのが一般的であるため，DSA をそのまま利用できるという性質は実用性という点で優れていると言える．また，Schnorr 型と同程度の署名長，通信量，計算量となるため，効率も良い．

ECDSA 型：これは電子署名標準である ECDSA を利用した方式であり，上記 DSA 型と同様，署名生成，検証時において ECDSA を容易に適用できるという利点がある．また，ECDSA を用いることにより，鍵長が短くて済むことや通信量が抑えられるという利点も挙げられる．計算量についても同様のことが言える．バイナリ法 [12] や [10], [19] の計算手法を適用すると，rP の計算は $39|r|M_p/8 + 3|r|I_p/2$ と予測され，署名者の計算量は表 2 のように表せ，受取人の計算量は表 3 のように表せる．例えば，最も基本的な OS_1^2 の場合，DSA 型の p, q を $|p| = 1024, |q| = 160$ とし，ECDSA 型の p, q を $|p| = 160, |q| = 160$ とすると，DSA 型に比べて，全体の通信量は約 42%，署名生成の計算量は約 63%の削減となり，最も効率が良い．

DSA-OT 型：これは通常の手段で別途作成した署名をオブリビアス通信を用いて送るという最も単純にオブリビアス署名を実現する方式である．この方式では，どんな署名方式にも適用できるという利点がある一方，署名とオブリビアス通信という 2 つの操作をそれぞれ独自に行わなくてはならないため，計算コストが増大し，効率が悪いという問題が生じる．また，オブリビアス通信自体の計算コストも大きいため，なおさら効率が悪い．例えば，最も基本的な OS_1^2 の場合，DSA 型に比べて，署名生成の計算量は約 47%増大し，受取人の計算量は約 50%増大してしまう．

5. むすび

本稿ではオブリビアス署名の明確な定義を示し，さらに，DLP 及び ECDLP の困難性を利用したオブリビアス署名方式を提案した．提案方式は 2 種類あり，それぞれ電子署名標準である DSA 及び ECDSA に基づく．また，従来方式，提案方式，オブリビアス通信を利用した方式について，計算量，署名長，通信量等，種々の観点から評価を行い，各方式の特徴を示した．

文　献

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

[2] M. Abe and T. Okamoto, "Provably Secure Partially Blind Signautres", CRYPTO 2000, LNCS 1880, pp.271-286, 2000.

[3] M. Bellare and P. Rogaway, "The exact security of digital signatures - How to sign with RSA and Rabin", Eurocrypt '96, pp.399-416, Springer-Verlag, 1996.

[4] D. Chaum, "Blind signatures for untraceable payments", CRYPTO '82, pp.199-203, 1982.

[5] L. Chen, "Oblivious Signatures", European Symposium on Research in Computer Security (ESORICS94), LNCS 875, pp.161-172, Springer-Verlag, 1996.

[6] C.K. Chu and W.G. Tzeng, "Efficient k-out-of-n Oblivious Transfer Schemes with Adaptive and Non-adaptive Queries", PKC '05, LNCS 3386, pp.172-183, 2005.

[7] S. Even, O. Goldreich and A. Lempel, "A randomized protocol for signing contracts", Communications of the ACM, vol.28, no.6, pp.637-647, 1985.

[8] A. Fiat and A. Shamir, "How to prove yourself : Practical solutions to identification and signature problems", CRYPTO '86, LNCS 263, pp.186-194, Springer-Verlag, 1987.

[9] A. Juels, M. Luby and R. Ostrovsky, "Security of Blind Digital Signatures", CRYPTO '97, pp.150-164, Springer-Verlag, 1997.

[10] B.S. Kaliski Jr., "Comments to NIST", 1991.

[11] Y.T. Kalai, "Smooth Projective Hashing and Two-Message Oblivious Transfer", EUROCRYPT '05, LNCS 3494, pp.78-95, 2005.

[12] D. Knuth, "The Art of Computer Programming Volume 2 Seminumerical Algorithms", Addison-Wesley, vol.2, 1998.

[13] M. Naor and B. Pinkas, "Efficient Oblivious Transfer Protocols", SODA '01, pp.448-457, 2001.

[14] M. Naor and B. Pinkas, "Computationally Secure Oblivious Transfer", Journal of Cryptology, 18, 1, pp.1-35, 2005.

[15] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.

[16] M.O. Rabin, "How to exchange secrets by oblivious transfer", Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[17] C.P. Schnorr, "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 4, 3, pp.161-174, 1991.

[18] W.G. Tzeng, "Efficient 1-out-of-n Oblivious Transfer Schemes with Universal Usable Parameters", IEEE Transactions on Computers, vol.53, no.2, pp.232-240, 2004.

[19] 岡本 栄司,「NIST のディジタル署名案について」, 電子情報通信学会, ISEC1991-64, pp.71-75, 1991.

[20] 岡本 健, 椎名 信行, 岡本 栄司,「オブリビアス署名の設計と解析」, SCIS 2005, pp.1447-1452, 2005.