対話型署名機能付き暗号化方式

井田 潤一† 渡邉 洋平† 四方 順司†‡

† 横浜国立大学 大学院環境情報学府/研究院
‡ 横浜国立大学 先端科学高等研究院
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
{ida-junichi-hx, watanabe-yohei-xs}@ynu.jp, shikata@ynu.ac.jp

あらまし 近年, Dodis と Fiore によって対話型の公開鍵暗号方式と認証方式が提案された．対話型の方式の利点として, 非対話型のものと比べ, 弱い暗号プリミティブから強い安全性を満たす方式を構成することが可能である．しかし, 公開鍵暗号とディジタル署名の両機能を効率的に同時に達成する方式である署名機能付き暗号化方式 (Signcryption) に関しては, 対話型のものは未だ報告されていない．そこで, 本稿では対話型の Signcryption を新たに提案し, 弱い暗号プリミティブである IND-CPA 安全な公開鍵暗号を用いて強い安全性である IND-CCA 安全性を満たす対話型 Signcryption の一般的構成法を提案する．

Interactive Signcryption

Ida Junichi† Yohei Watanabe† Junji Shikata†‡

†Graduate School of Environment and Information Sciences, Yokohama National University
‡Institute of Advanced Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, JAPAN
{ida-junichi-hx, watanabe-yohei-xs}@ynu.jp, shikata@ynu.ac.jp

Abstract Recently, interactive public key encryption and authentication have been proposed by Dodis and Fiore. Interactive schemes can be constructed from weaker cryptographic primitives than non-interactive schemes. However, there is no report on signcryption, which realizes confidentiality and integrity simultaneously, in the interactive setting. In this paper, we first propose notions of interactive signcryption, and show a generic construction that meets strong confidentiality and strong integrity from weak cryptographic primitives such as IND-CPA secure public key encryption.

1 はじめに

公開鍵暗号 (Public-Key Encryption: PKE) とディジタル署名 (Digital Signature: DS) の両機能を効率的に同時に達成する方式として, Zheng[9] によって提案された署名機能付き暗号化方式 (Signcryption) が知られている．Signcryption は秘匿性と完全性を同時に保証しつつ, 単純に PKE と DS を組み合わせるよりも効率が良いという利点がある．この提案以降，Signcryption の構成に関する研究が多く行われてきた [1, 3, 5, 8]．特に近年，できるだけ弱い暗号プリミティブから強い安全性を満たす Signcryption の一般的構成について研究が行われてきたが [5, 8]，いずれも IND-CCA 安全な PKE（またはそれ相当の暗号プリミティブ）が構成部品として必要であり，それらよりも弱い暗号プリ

ミティブ（例えばIND-CPA安全なPKE）からの一般的構成は知られていない．

また, 2014年にDodisとFiore[7]によって対話型暗号技術が提案された．対話型暗号技術の利点として，従来の非対話型暗号技術に比べ，弱い暗号プリミティブから構成可能である点，またそれにより計算効率も良い点が挙げられる．特に，[7]では非対話型では達成できなかったIND-CPA安全の（非対話型）PKEから一般的に2-roundのIND-CCA安全の対話型PKEを構成することに成功している．しかし，[7]ではPKEとDSのみを扱っており，未だに対話型のSigncryptionは知られていない．特に，対話型PKE及びDSでは，対話の終了をもって暗号文または署名が受信者側に出力されるため，単純に組み合わせて同時に秘匿性と完全性を同時に保証できるかは自明ではない．また，[7]ではPKEとDS両方を一般的に捉えるモデルとしてMessage Transmission Protocol (MTP)を考えているが，MTPでは対話型のSigncryptionを捉えることが出来ない．

本稿の成果． 対話型のSigncryptionを新たに提案し, モデルと安全性を定義する．また一般的構成法として3-roundと2-roundの2つの構成法を提案する． これらの構成法は送信するメッセージ量とラウンド数のトレードオフの関係にある．本稿のメインの成果は次の2つである．(1)非対話型のSigncryptionでは達成できていなかった弱い暗号プリミティブであるIND-CPA安全な公開鍵暗号とディジタル署名とワンタイム署名を用いて強い安全性であるIND-CCA安全性かつsUF-CMA安全性を満たす対話型Signcryptionの構成法を提案する．(2)論文[7]の対話型の公開鍵暗号と同様の暗号プリミティブから2-roundのSigncryptionの構成法を提案する．

2 準備

本節では, 本稿で用いられる暗号プリミティブについて記述する．

2.1 公開鍵暗号

PKEは3つの多項式時間アルゴリズム（PKE.Kg, PKE.Enc, PKE.Dec）から構成される．

- $(pk, sk) \leftarrow \mathrm{PKE.Kg}(1^k)$：セキュリティパラメータ k を入力とし, 公開鍵と秘密鍵のペア (pk, sk) を出力する．
- $C \leftarrow \mathrm{PKE.Enc}(pk, m)$：公開鍵 pk と平文 m を入力とし暗号文 C を出力する．
- m or $\perp \leftarrow \mathrm{PKE.Dec}(sk, C)$：秘密鍵 sk と暗号文 C を入力とし, 平文 m あるいは復号不可を表す特別な記号 $\perp$ を出力する．

PKEは, 全ての $k \in \mathbb{N}$, $(pk, sk) \leftarrow \mathrm{PKE.Kg}(1^k)$, 平文 m において, $C \leftarrow \mathrm{PKE.Enc}(pk, m)$ に対し $M = \mathrm{PKE.Dec}(sk, C)$ をみたすものとする．

以下にIND-CPA安全性を定義する．

定義 1 (IND-CPA)．攻撃者 $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$ とチャレンジャーのゲームを次のように定義する．

$\mathrm{Exp}^{IND\text{-}CPA}_{\mathrm{PKE},\mathcal{A}}(k)$:

- $(pk, sk) \leftarrow \mathrm{PKE.Kg}(1^k)$.
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1(pk)$.
- $b \leftarrow \{0, 1\}$, $C^* \leftarrow \mathrm{PKE.Enc}(pk,\ m_b)$.
- $b' \leftarrow \mathcal{A}_2(st, C^*)$.
- $b = b'$ なら1を, それ以外なら0を出力する．

ただし $|m_0| = |m_1|$ である．攻撃者 $\mathcal{A}$ の優位性を $\mathrm{Adv}^{IND\text{-}CPA}_{\mathrm{PKE},\mathcal{A}}(k) = \left|\Pr[\mathrm{Exp}^{IND\text{-}CPA}_{\mathrm{PKE},\mathcal{A}}(k) = 1] - 1/2\right|$ と定義する．$\mathrm{Adv}^{IND\text{-}CPA}_{\mathrm{PKE},\mathcal{A}}(k) \leq \epsilon$ をいかなる多項式時間の攻撃者 $\mathcal{A}$ に対しても満たすとき, *PKE* が *IND-CPA* 安全であるという．

2.2 ディジタル署名

DSは以下の3つのアルゴリズム (DS.Kg, DS.Sign, DS.Ver) から構成される．

- $(vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$：セキュリティパラメータ k を入力とし, 検証鍵と署名鍵のペア (vk, sk) を出力する．
- $\sigma \leftarrow \mathrm{DS.Sign}(sk, m)$：署名鍵 sk とメッセージ m を入力とし署名 σ を出力する．

- 1 or 0 $\leftarrow \mathrm{DS.Ver}(vk, m, \sigma)$: 検証鍵 vk とメッセージ m と署名 σ を入力とし, メッセージを受理する場合は 1, そうでなければ 0 を出力する.

DS は, 全ての $k \in \mathbb{N}, (vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$, メッセージ m において, $\sigma \leftarrow \mathrm{DS.Sign}(sk, m)$ に対し $1 \leftarrow \mathrm{DS.Ver}(vk, m, \sigma)$ をみたすものとする.

以下に, UF-CMA 安全性と strongly UF-CMA (sUF-CMA) 安全性を定義する.

定義 2 (UF-CMA)**.** 攻撃者 $\mathcal{A}$ とチャレンジャーのゲームを次のように定義する.

$\mathrm{Exp}^{UF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k)$:

- $(vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$.
- $(m^*, \sigma^*) \leftarrow \mathcal{A}^{O(\cdot)}(vk)$.
- $m^* \notin \{m_i\}_{1 \le i \le t}$ かつ $\mathrm{DS.Ver}(vk, m^*, \sigma^*) = 1$ ならば 1 を出力し, それ以外なら 0 を出力する.

ここでは O は署名オラクルであり, m を入力とし, σ を出力する. $\mathcal{A}$ は高々 $t = poly(k)$ 回, 署名オラクルを利用することができる. また $(m_1, m_2, \ldots m_t)$ を署名オラクル O へのメッセージとし, $(\sigma_1, \sigma_2, \ldots \sigma_t)$ を署名オラクル O へのクエリに対する答えとする. この時, $\mathcal{A}$ の優位性を $\mathrm{Adv}^{UF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) = \Pr[\mathrm{Exp}^{UF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) = 1]$ と定義する. いかなる多項式時間の攻撃者 $\mathcal{A}$ に対しても $\mathrm{Adv}^{UF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) \le \epsilon$ を満たすとき, ディジタル署名が UF-CMA 安全であるという.

定義 3 (sUF-CMA)**.** 定義 2 において $\mathrm{Exp}^{UF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) = 1$ となる条件を $m^* \notin \{m_i\}_{1 \le i \le t}$ から $(m^*, \sigma^*) \notin \{(m_i, \sigma_i)\}_{1 \le i \le t}$ に変更し, このゲームを新たに $\mathrm{Exp}^{sUF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k)$ とおく. この時, $\mathcal{A}$ の優位性を $\mathrm{Adv}^{sUF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) = \Pr[\mathrm{Exp}^{sUF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) = 1]$ と定義し, $\mathrm{Adv}^{sUF\text{-}CMA}_{\mathrm{DS},\mathcal{A}}(k) \le \epsilon$ をいかなる多項式時間の攻撃者 $\mathcal{A}$ に対しても満たすとき, ディジタル署名が sUF-CMA 安全であるという.

また, 署名オラクルにアクセスする回数を高々 1 回に制限した sUF-CMA 安全な署名はワンタイム署名 (One-Time Signature: OTS) と呼ばれ, 特に OT-sUF-CMA 安全と呼ぶ.

2.3 汎用一方向性ハッシュ関数

汎用一方向性ハッシュ関数 (Universal One-Way Hash Function: UOWHF) を以下のように定義される.

定義 4 (UOWHF)**.** ハッシュ関数族 $\{\mathcal{H}_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in I}$ において, $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$ とチャレンジャーのゲームを以下のように定義する.

$\mathrm{Exp}^{\mathrm{UOWHF}}_{\mathcal{A}}(k)$:

- $(x, st) \leftarrow \mathcal{A}_1(1^k)$.
- $i \leftarrow \mathrm{Gen}(1^k)$.
- $x^* \leftarrow \mathcal{A}_2(i, x, st)$.
- $(x, x^*) \in \mathcal{D}_i^2 \wedge x \neq x^* \wedge H_i(x) = H_i(x^*)$ なら 1 を, それ以外なら 0 を出力する.

ここで Gen はセキュリティパラメータ k を入力とし, k ビットで表せる自然数 $i \in I$ を出力するアルゴリズムである. 攻撃者 $\mathcal{A}$ の優位性を $\mathrm{Adv}^{\mathrm{UOWHF}}_{\mathcal{A}}(k) = \Pr[\mathrm{Exp}^{\mathrm{UOWHF}}_{\mathcal{A}}(k) = 1]$ と定義する. いかなる多項式時間の攻撃者 $\mathcal{A}$ に対しても $\mathrm{Adv}^{\mathrm{UOWHF}}_{\mathcal{A}}(k) \le \epsilon$ を満たすとき, ハッシュ関数族 $\{H_i\}_{i \in I}$ は汎用一方向性ハッシュ関数族であるという.

3 Interactive Signcryption

本節では, 対話型の署名機能付き暗号化方式 (Interactive Signcryption Scheme: ISCS) を提案する. Dodis と Fiore [7] は, 対話型暗号化方式, 認証方式を考えるうえでの共通のモデルを Message Transmission Protocol (MTP) として定式化した. しかしながら, MTP では ISCS を捉えることが出来ない. そのため, 本稿では ISCS のモデルから考える.

3.1 モデル

MTP を基に, 以下の ISCS のモデルを考える. MTP では送信者の鍵を $sendk$, 受信者の鍵を $recvk$ としていたところを, それぞれ公開鍵と秘密鍵に分けた点が主な変更点であり, 不自然な変更は行っていない.

ISCSは$(\mathrm{KeyGen}_S(1^k), \mathrm{KeyGen}_R(1^k), \mathrm{S}(pk_R, sk_S, m, k), \mathrm{R}(pk_S, sk_R, k))$の4つのアルゴリズムから構成される．

- $(pk_S, sk_S) \leftarrow \mathrm{KeyGen}_S(1^k)$: セキュリティパラメータ$k$を入力し，受信者鍵ペアー$(pk_S, sk_S)$を出力する．
- $(pk_R, sk_R) \leftarrow \mathrm{KeyGen}_R(1^k)$: セキュリティパラメータ$k$を入力し，受信者鍵ペアー$(pk_R, sk_R)$を出力する．
- $\mathrm{S}(pk_R, sk_S, m)$: 確率的対話型アルゴリズムであり，セキュリティパラメータkと平文mをプライベートな入力として動く．
- $m \text{ or } \perp \leftarrow \mathrm{R}(pk_S, sk_R)$: 確率的対話型アルゴリズムであり，セキュリティパラメータkを入力とし，平文mかエラーを表す記号$\perp$を出力する．

SとRは対話を行いながら実行される．例えばSから対話が始まる場合は，SがメッセージM_1を送り，次にRがメッセージM_2を送り，というように対話が行われる．また送信者は出力を得ないため，一般性を失わずに，送信者が最後にメッセージを送信することとする．この対話型プロトコルの一連の動作を，

$$\langle \mathrm{S}(pk_R, sk_S, m), \mathrm{R}(pk_S, sk_R) \rangle = m'$$

と書き，高々n回の対話を必要とするものをn-roundプロトコルと呼ぶ．

ISCSは，全ての$k \in \mathbb{N}$, 平文mにおいて，$\langle \mathrm{S}(pk_R, sk_S, m), \mathrm{R}(pk_S, sk_R) \rangle = m$をみたすものとする．

3.2 安全性定義

ISCSでは，識別不可能性と偽造不可能性の2つの安全性定義を考える必要があるが，[7]と同様，対話型暗号技術特有の安全性，主には以下の中間者攻撃に対する安全性を考えなければならない．例えば，非対話型の識別不可能性の定義では，オラクルアクセスは**チャレンジ暗号文をもらう前後**に行うことができる．しかしながら，対話型の識別不可能性の定義を考える際には，**チャレンジ暗号文をもらっている最中**にオラクルアクセスが可能であることに留意しなければならない．これを$\langle \mathrm{S}(pk_R, sk_S, m_b), \mathcal{A}^{\mathrm{R}(pk_S, sk_R)} \rangle$（偽造不可能性の場合は$\langle \mathcal{A}^{\mathrm{S}(pk_R, sk_S, \cdot)}, \mathrm{R}(pk_S, sk_R) \rangle$）と書く．$\mathcal{A}^{\mathrm{R}(pk_S, sk_R)}$は$\mathcal{A}$が正当な受信者をオラクルとして用いることを表しており，すなわち，$\mathcal{A}$は送信者になりすまして正当な受信者と通信しながら，チャレンジ暗号文をもらう際には受信者として振る舞う．ここで，チャレンジャーとの一連の対話をチャレンジセッション，オラクルとの一連の対話をオラクルセッションと呼び，対話を終えるごとに1セッションと数える．特に選択暗号文攻撃を考える場合は，$\mathcal{A}$は各オラクルセッションの終わりに受信者の出力（すなわちmか$\perp$）を得ることが出来るものとする[1]．上記の安全性を定式化するために，いくつか定義を行う必要がある．

まず，Protocol Transcriptを定義する．簡単には，対話中のメッセージとそれに対するタイムスタンプの組をProtocol Transcriptと呼ぶ．本稿では，tを時刻として，またその時刻に押されたタイムスタンプとして用いる．

定義 5 (Protocol Transcript [7])**.** ISCSにおいて交換されたメッセージとそのタイムスタンプの組を *Protocol Transcript* とする．もし *ISCS* がn-roundであれば，*Protocol Transcript* Tは

$$T = \langle (M_1, t_1), \ldots, (M_n, t_n) \rangle$$

と表記される．ここで，$M_1, \ldots, M_n$は対話中の各メッセージ，$t_1, \ldots, t_n$はそれぞれに対応するタイムスタンプである．

さて，中間者攻撃において“ただ受け流すだけの攻撃（ピンポン攻撃という）”は必ず成功する．具体的には，チャレンジセッション中に受け取ったTranscriptをそのままオラクルに受け流す攻撃であり，当然最終的に復号結果をもらうことができる．これはすなわち非対話型の定義で復号オラクルにチャレンジ暗号文をクエリするのと同じことであり，従って，そのような攻撃を排除したうえで安全なISCSを定式化

[1] $n = 1$の場合（非対話の場合）は，非対話型の識別不可能性における復号オラクルと同様の定義となる．

する必要がある．そこで，ピンポン攻撃を定式化するため，Matching Transcript という概念を定義する．そのためにまず “alternating” という概念を定義する．

定義 6 (Alternating [7])**.** $T = \langle (M_1, t_1), \ldots, (M_n, t_n) \rangle$ と $T^* = \langle (M_1^*, t_1^*), \ldots, (M_n^*, t_n^*) \rangle$ を *2*つの Protocol Transcript とする．このとき，以下の条件を満たすならば，T は T^* と "*alternating*" であるという*:* それぞれのタイムスタンプ列が

- 受信者から通信が開始したとき*:* $t_1 < t_1^* < t_2^* < t_2 < t_3 < \cdots < t_{n-1}^* < t_n^* < t_n$.
- 送信者から通信が開始したとき*:* $t_1^* < t_1 < t_2 < t_2^* < t_3^* < \cdots < t_{n-1}^* < t_n^* < t_n$.

定義 7 (Matching Transcript [7])**.** $T = \langle (M_1, t_1), \ldots, (M_n, t_n) \rangle$ と $T^* = \langle (M_1^*, t_1^*), \ldots, (M_n^*, t_n^*) \rangle$ を *2*つの Protocol Transcript とする．もし $\forall_i = 1, \ldots, n$ において $M_i = M_i^*$ かつ T は T^* と *"alternating"* であったとき*,* *2*つの Protcol Transcript は一致していると言い，$T \equiv T^*$ と書く．

定義 8 (ピンポン攻撃者 [7])**.** ISCS において，攻撃者 $\mathcal{A}$ が存在するとする[2]*.* T^* をチャレンジセッションにおける Transcript とし, $T_1, \ldots, T_Q$ をオラクルセッションにおいて攻撃者 $\mathcal{A}$ によって作られた Transcript とする．そのとき $T \equiv T^*$ となるような $T \in \{T_1, \ldots, T_Q\}$ が存在する場合，$\mathcal{A}$ をピンポン攻撃者と呼ぶ.

続いて，選択暗号文攻撃に対する対話型識別不可能性 (IND-iCCA) と, 選択文書攻撃に対する対話型強偽造不可能性 (sUF-iCMA) を定義する．

定義 9 (IND-iCCA)**.** 攻撃者 $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$ に対して次のゲームを考える．

$\mathrm{Exp}^{\mathrm{iCCA}}_{\mathrm{ISCS},\mathcal{A}}(k)$:

- $(pk_R, sk_R) \leftarrow \mathrm{KeyGen}_R(1^k), (pk_S, sk_S) \leftarrow \mathrm{KeyGen}_S(1^k)$.
- $b \leftarrow \{0, 1\}$.
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\mathrm{R}(pk_S, sk_R, \cdot)}(pk_S, pk_R, sk_S)$.
- $b' \leftarrow \langle \mathrm{S}(pk_R, sk_S, m_b), \mathcal{A}_2^{\mathrm{R}(pk_S, sk_R)}(pk_S, pk_R, sk_S, st) \rangle$.
- もし $b' = b$ かつ $\mathcal{A}$ がピンポン攻撃者でなければ 1 を出力し*,* そうでなければ 0 を出力する*.*

$\mathcal{A}$ の優位性を $\mathrm{Adv}^{\mathrm{iCCA}}_{\mathrm{ISCS},\mathcal{A}}(k) = |\Pr[\mathrm{Exp}^{\mathrm{iCCA}}_{\mathrm{ISCS},\mathcal{A}}(k) = 1] - 1/2|$ と定義する．$\mathrm{Adv}^{\mathrm{iCCA}}_{\mathrm{ISCS},\mathcal{A}}(k) < \epsilon$ がいかなる多項式時間の攻撃者 $\mathcal{A}$ に対しても成り立つとき，ISCS は IND-iCCA 安全であるという.

定義 10 (sUF-iCMA)**.** 攻撃者 $\mathcal{A}$ に対して次のゲームを考える．

$\mathrm{Exp}^{\mathrm{iCMA}}_{\mathrm{ISCS},\mathcal{A}}(k)$:

- $(pk_R, sk_R) \leftarrow \mathrm{KeyGen}_R(1^k), (pk_S, sk_S) \leftarrow \mathrm{KeyGen}_S(1^k)$.
- $m^* \leftarrow \langle \mathcal{A}^{\mathrm{S}(pk_R, sk_S, \cdot)}(pk_S, pk_R, sk_R), \mathrm{R}(pk_S, sk_R) \rangle$.
- もし $m^* \neq \perp$ かつ $\mathcal{A}$ がピンポン攻撃者でなければ 1 を出力し*,* そうでなければ 0 を出力する*.*

$\mathcal{A}$ の優位性を $\mathrm{Adv}^{\mathrm{iCMA}}_{\mathrm{ISCS},\mathcal{A}}(k) = \Pr[\mathrm{Exp}^{\mathrm{iCMA}}_{\mathrm{ISCS},\mathcal{A}}(k) = 1]$ と定義する．$\mathrm{Adv}^{\mathrm{iCMA}}_{\mathrm{ISCS},\mathcal{A}}(k) < \epsilon$ がいかなる多項式時間の攻撃者 $\mathcal{A}$ に対しても成り立つとき，ISCS は sUF-iCMA 安全であるという.

4 提案構成法

本稿では 3-round プロトコルと 2-round プロトコル，それぞれの構成法を提案する．前者 (3-round プロトコル) は Dolev ら [6] の IND-iCCA 安全な 3-round PKE と Bellare ら [2] による sUF-CMA 安全な DS の構成法に基づいており，単純に組み合わせると OTS が 2 つ必要になるところを OTS を 1 つに削減している．後者 (2-round プロトコル) は前者で用いた 3-round PKE の代わりに，Dodis と Fiore[7] の 2-round PKE に基づいて構成している．Dodis と Fiore[7] の 2-round PKE は，1-bounded IND-CCA 安全な PKE[4] と DS から構成可能だが，この構成を単純に適用しても安全な 2-round プロトコルは得られないため，1-bounded IND-CCA 安全な PKE の構成部品である，IND-CPA

[2] すなわち $\langle \mathrm{S}(pk_R, sk_S, m_b), \mathcal{A}^{\mathrm{R}(pk_S, sk_R)} \rangle$ または $\langle \mathcal{A}^{\mathrm{S}(pk_R, sk_S, \cdot)}, \mathrm{R}(pk_S, sk_R) \rangle$ となる状況である.

安全な PKE, DS, OTS を用いて構成していく．以降，わかりやすいように DS と OTS のアルゴリズムを明示的に分けて書き，OTS=(OTS.Kg, OTS.Sign, OTS.Ver) とかく．

4.1 3-round の構成法

3-round プロトコルの構成法を以下に示す．PKE = (PKE.Kg, PKE.Enc, PKE.Dec) と DS = (DS.Kg, DS.Sign, DS.Ver) と OTS = (OTS.Kg, OTS.Sign, OTS.Ver) から ISCS = (KeyGen_S, KeyGen_R, S, R) を構成する．

- $\mathrm{KeyGen}_S(1^k)$: $(vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$ を生成し，$pk_S = vk, sk_S = sk$ として出力する．
- $\mathrm{KeyGen}_R(1^k)$: $(vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$ を生成し，$pk_R = vk, sk_R = sk$ として出力する．
- $\mathrm{S}(pk_R, sk_S, m)$:
  - OTS の鍵 $(sk_{\mathrm{OT}}, vk_{\mathrm{OT}}) \leftarrow \mathrm{OTS.Kg}(1^k)$ を生成し，受信者に $M_1 = vk_{\mathrm{OT}}$ を送信する．
  - 受信者から $M_2 = (ek, \sigma_R)$ を受信した後，$\mathrm{DS.Ver}(pk_R, ek \| vk_{OT}, \sigma_R) \rightarrow 1$ ならば, 以下の手順で署名付き暗号文 $M_3 = \sigma_S$ を生成する．
    1. $c \leftarrow \mathrm{PKE.Enc}(ek, m)$.
    2. $S \leftarrow \mathrm{DS.Sign}(sk_S, c)$.
    3. $s \leftarrow \mathrm{OTS.Sign}(sk_{OT}, c \| S)$.
    4. $\sigma_S \leftarrow (c, S, s)$.
- $\mathrm{R}(pk_S, sk_S)$:
  - 送信者から $M_1 = vk_{\mathrm{OT}}$ が届いた後，$(ek, dk) \leftarrow \mathrm{PKE.Kg}(1^k)$ を生成する．また $\sigma_R \leftarrow \mathrm{DS.Sign}(sk_R, vk_{OT} \| ek)$ を生成し，送信者に $M_2 = (ek, \sigma_R)$ を送信する．
  - 送信者から $M_3 = \sigma_S = (c, S, s)$ が届いた後，まず $\mathrm{OTS.Ver}(vk_{\mathrm{OT}}, c \| S, s)$ と $\mathrm{DS.Ver}(pk_S, c, S)$ を検証する．どちらも 1 を出力すれば，$m \leftarrow \mathrm{PKE.Dec}(dk, c)$ を出力する．そうでなければ $\perp$ を出力する．

以下に，上記の構成法の安全性を示す．証明は紙面の都合上省略し，本稿のフルバージョンにて示す．

定理 1. PKE が *IND-CPA* 安全かつ，DS が *UF-CMA* 安全かつ OTS が *OT-sUF-CMA* 安全ならば，上記構成法による 3-*round ISCS* は *IND-iCCA* 安全である．

定理 2. DS が *UF-CMA* 安全かつ OTS が *OT-sUF-CMA* 安全ならば，上記構成法による 3-*round ISCS* は *sUF-iCMA* 安全である．

4.2 2-round の構成法

前節の構成法と同様の暗号プリミティブに加えて UOWHF = $(\mathrm{Gen}, \{H_i\}_{i \in I})$ を用いた，2-round プロトコルの構成法を示す．ここで，各 H_i の値域を $\mathcal{R}_i = \{0,1\}^n$ とする $(n = poly(k))$．また，H_i の出力 v の i ビット目を v_i と書く．

- $\mathrm{KeyGen}_S(1^k)$: $(vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$ を生成し，$pk_S = vk, sk_S = sk$ として出力する．
- $\mathrm{KeyGen}_R(1^k)$: $(vk, sk) \leftarrow \mathrm{DS.Kg}(1^k)$ を生成し，$pk_R = vk, sk_R = sk$ として出力する．
- $\mathrm{S}(pk_R, sk_S, m)$:
  - 受信者から $M_1 = (ek, \sigma_R)$ が届いた後，$\mathrm{DS.Ver}(pk_R, ek, \sigma_R) \rightarrow 1$ ならば, 以下の手順で署名付き暗号文を生成する．
    1. $(sk_{OT}, vk_{OT}) \leftarrow OTS.Kg(1^k)$.
    2. $v = H_i(vk_{OT})$.
    3. $\bigoplus_{i=1}^{n} m_i = m$ となるような m_i を選ぶ．
    4. $c \leftarrow \mathrm{PKE.Enc}(ek_i^{(v_i)}, m_i)$ $(1 \leq i \leq n)$.
    5. $c \leftarrow (c_1, \ldots, c_n)$

6. $S \leftarrow \mathrm{DS.Sign}(sk_S, c)$.
7. $s \leftarrow \mathrm{OTS.Sign}(sk_{OT}, c\|S)$.
8. $\sigma_S \leftarrow (c, S, s)$.

最後に，$M_2 = (vk_{OT}, \sigma_S)$ を受信者に送信する．

- $\mathrm{R}(pk_S, sk_R)$:
  - $(ek_i^{(b)}, dk_i^{(b)}) \leftarrow \mathrm{PKE.Kg}(1^k)$ $(\forall i \in \{1, \ldots, n\}, \forall b \in \{0, 1\})$ を生成する．また $i \leftarrow \mathrm{Gen}(1^k)$ を実行する．$ek = (H_i, ek_1^{(0)}, ek_1^{(1)}, \ldots, ek_n^{(0)}, ek_n^{(1)}), dk = (dk_1^{(0)}, dk_1^{(1)}, \ldots, dk_n^{(0)}, dk_n^{(1)})$ とする．$\sigma_R \leftarrow \mathrm{DS.Sign}(sk_R, ek)$ を生成し，送信者に $M_1 = (ek, \sigma_R)$ を送信する．
  - $M_2 = (vk_{OT}, \sigma_S)$ を受信した後，まず $\mathrm{OTS.Ver}(vk_{\mathrm{OT}}, c\|S, s)$ と $\mathrm{DS.Ver}(pk_S, c, S)$ を実行する．どちらかが 0 を出力した場合，$\perp$ を出力する．そうでなければ $v = h(vk_{OT})$ を計算し，$m_i \leftarrow \mathrm{PKE.Dec}(dk_i^{(v_i)}, c)$ を得る．最後に $m = \bigoplus_{i=1}^{n} m_i$ を出力する．

以下に，上記の構成法の安全性を示す．証明は紙面の都合上省略し，本稿のフルバージョンにて示す．

定理 3. PKE が *IND-CPA* 安全かつ，DS が *UF-CMA* 安全かつ OTS が *OT-sUF-CMA* 安全かつハッシュ関数が *UOWHF* ならば，提案する上記構成法による 2-*round ISCS* は *IND-iCCA* 安全である．

定理 4. DS が *UF-CMA* 安全かつ OTS が *OT-sUF-CMA* 安全ならば，提案する上記構成法による 2-*round ISCS* は *sUF-iCMA* 安全である．

4.3 構成法の比較

本節では 2 つの構成法の総通信量の比較を行う．

簡単のため，それぞれの構成法における各署名 S, s, σ_R と暗号文 c は同程度の長さと考える．すると 2 つの構成法の総通信量の差は，2-round の構成法が 3-round のものより $(2n-1)|ek| + (n-1)|c| + |h|$ 大きく，差が n に比例している．また n は UOWHF のハッシュ長であり，比較的大きくなることがわかる．また 2-round の構成法は 3-round の構成法よりも若干帰着効率が悪く，特に UOWHF にルーズに帰着していることから，各パラメータ長が 3-round のものより大きくなることがわかる．これにより総通信量の差はさらに大きくなる．よって 2-round の構成法は考え得る最小のラウンド数を達成し，特に Dodis と Fiore が提案した iCCA PKE で用いられた暗号プリミティブのみを用いて構成できているものの，効率面では 3-round プロトコルの方が優れている．

構成法	ラウンド	メッセージ長
構成法 1	1-round	$\|vk_{OT}\|$
	2-round	$\|ek\| + \|\sigma_R\|$
	3-round	$\|c\| + \|S\| + \|s\|$
構成法 2	1-round	$2n\|ek\| + \|\sigma_R\| + \|h\|$
	2-round	$\|vk_{OT}\| + n\|c\| + \|S\| + \|s\|$

($|x|$ は x のビット長とする．)

4.4 謝辞

本研究は文部科学省国立大学改革強化推進事業の支援を受けたものです．第二著者は，JSPS 科研費 25·3998 の助成を受けています．

参考文献

[1] J. An, Y. Dodis, and T. Rabin. “On the Security of Joint Signature and Encryption ”, EUROCRYPT 2002, LNCS vol. 2332, pp. 83–107. Springer, 2002.

[2] M. Bellare, and S. Shoup. “Two-tier Signatures, Strongly Unforgeable Signatures, and Fiat-shamir without Random Oracles”, PKC 2007, LNCS vol. 4450, pp. 201–216. Springer, 2007.

[3] J. Baek, R. Steinfeld, and Y. Zheng. “Formal Proofs for the Security of Signcryp-

tion ", PKC 2002, LNCS vol. 2274, pp. 88–98. Springer, 2002.

[4] R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat, and V. Vaikuntanathan. "Bounded CCA2-Secure Encryption", ASIACRYPT 2007, LNCS vol. 4833, pp. 502–518. Springer, 2007.

[5] D. Chiba, T. Matsuda, J. Schuldt, and K. Matsuura, "Efficient Generic Constructions of Signcryption with Insider Security in the Multi-user Setting", ACNS 2011, LNCS vol. 6715, pp. 220–237. Springer, 2011.

[6] D. Dolev, C. Dwork, and M. Naor. "Non-malleable Cryptography", SIAM Journal on Computing, vol. 30(2): 391–437, ACM, 2000.

[7] Y. Dodis, and D. Fiore. "Interactive Encryption and Message Authentication", SCN 2014, LNCS vol. 8642, pp. 494–513. Springer, 2014.

[8] R. Nakano, and J. Shikata. "Constructions of Signcryption in the Multi-user Setting from Identity-based Encryption", IMACC 2013, LNCS vol. 8308, pp. 324–343. Springer, 2013.

[9] Y. Zheng. "Digital Signcryption or How to Achieve Cost(Signature & Encryption) $\ll$ Cost(Signature) + Cost(Encryption)", CRYPTO 1997, LNCS vol. 1294, pp. 165–179. Springer, 1997.