4-3　紛失通信プロトコルの考察

4-3　A Survey on Oblivious Transfer Protocols

Le Trieu Phong
Le Trieu Phong

要旨

本論文では、公開鍵による暗号化スキームから紛失通信（OT）プロトコルを構築することに関する考察を行う。送信者と受信者の双方が誠実であることを想定した単純な 1-out-of-2 OT の構築をまず行う。その後、不誠実な送信者または受信者がいわゆる完全にシミュレーション可能なセキュリティを活用する状況を想定した、より複雑な構造について考察する。その後、DDH 仮定および DLIN 仮定によって構築されたセキュアなインスタンス化について説明する。

In this paper, we survey some constructions of oblivious transfer (OT) protocols from public key encryption schemes. We begin with a simple construction of 1-out-of-2 OT when both the sender and the receiver are assumed to be honest. We then move to a more complex construction assuming either dishonest sender or receiver, enjoying the so-called fully simulatable security. We then highlight some concrete instantiations secure under the decisional Diffie-Hellman (DDH) and the decision linear assumptions.

[キーワード]
紛失通信，公開鍵による暗号化スキーム
Oblivious transfer, Public key encryption schemes

1　はじめに

1.1　本論文の背景

紛失通信プロトコル [2] は論文において広く研究が行われている。単純な形態においては、送信者が2つのメッセージを保有し、受信者が2つのメッセージのうちの1つを受信したいと考え、どちらのメッセージを受信したかを送信者に開示しない形態が挙げられる。これは論文において 1-out-of-2 と呼ばれ、より複雑なプロトコル（[3] を参照のこと）を構築するための基本的なツールとなる。構造については、図1のとおりである。

送信者と受信者が存在する適応性のあるクエリーを含む紛失通信（適応性のある OT と呼ばれる）は、Naor と Pinkas が初めて研究を行った [12]。送信者は n 個のメッセージを保有し、受信者はそのうち k 個のメッセージを1つずつ受信したいと考える。それによって、(1) 送信者は受信者がどのメッセージを受信したかを確認することができず、(2) 受信者は k 個のメッセージ以外のメッセー

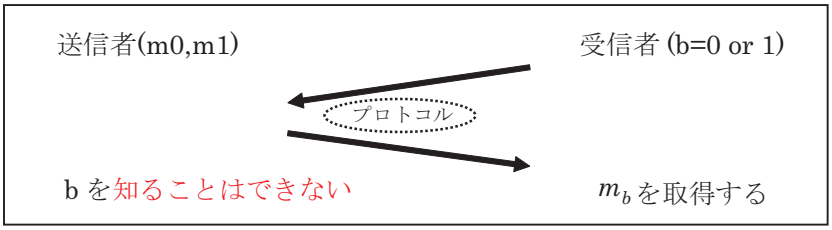

図1　1-out-of-2 紛失通信

ジを受信することができない。このような種類のOTは、主に特許検索、紛失検索、医学データベース等に活用されている。

上記の要件を満たすセキュリティのコンセプトは、研究に基づいて進化してきた。完全にシミュレーション可能なスキームは、現実世界と理想世界のパラダイムに基づいて、[1]に基づいてCamenischをはじめとする研究者によって紹介された。理想的なパラダイムにおいては、信頼できる第三者（TTP）が存在し、送信者はTTPに対して全てのメッセージを提供する。受信者がメッセージを受信したい場合は、受信者は該当するインデックスをTTPに送付するだけでよい。一方、現実のパラダイムにおいては、TTPは存在せず、適応性のあるOTのプロトコルは送信者と受信者によって運用される。完全にシミュレーション可能なスキームの考えとして、繰り返し発生する脅威に関しては、現実世界と理想世界とを区別することはできない。

さらに、Camenischをはじめとする研究者は、ランダム・オラクル・モデル（ROM）と標準モデルにおいて完全にシミュレーション可能な適応性の高いOTのモデルを初めて提供した。特に、OgataおよびKurosawa[15]によるROMのスキームが完全にシミュレーション可能なセキュリティを実現できることを示すことに成功した。さらに、組み合わせのグループにおいてqベースの仮定（qがnによって影響を受ける）を使用した標準モデルのシステムを構築した。

Camenischをはじめとする研究者の研究成果を受けて、この点についてさらに研究が行われた。[5]においては、GreenとHohenbergerがいわゆるq-hidden LRSW仮定に基づいて汎用的結合可能性（UC）を提供しかつ完全にシミュレーション可能なスキームを構築した。JareckiおよびLiu[8]は、RSAグループに含まれるq-DHI（Diffie-Hellman Inversion）仮定に基づくスキームに関する研究を行った。

qベースではない仮定に関しては、KurosawaおよびNojima[9]がDDH仮定に基づく完全にシミュレーション可能な単純なスキームを示した。しかしながら、本スキームではGreenとHohenbergerが[6]で示すとおり、各通信において$O(n)$の大きな通信コストが必要となった。その後、GreenとHohenbergerは、組み合わせのグループにおいてdecision 3-party DDH（3DDH）仮定に基づくシステムを構築した。その結果、Kurosawa、Nojima、およびPhong[10]は検証可能なシャッフル・プロトコルを使用して、DDH仮定に基づいてセキュリティを確保したうえで、コストを$O(1)$に削減することで[9]のデメリットを克服した。さらに、[11]において、上記の研究者は適応性のあるOTの標準システムについて提案し、当該OTシステムは標準の良く知られた仮定に基づいてセキュアなインスタンス化を実現する。

1.2 本論文の目的

本論文の主な目的は、公開鍵の暗号化スキームに基づいて構築したOTのいくつかのシステムについて考察することにある。まず、PKEスキームに基づいて構築した、よく知られた単純な1-out-of-2 OTのシステムについて考える（[3]を参照）。

その後、Kurosawa、Nojima、およびPhong[11]が提案する標準モデルに基づく完全にシミュレーション可能な適応性の高いOT（主な構成要素として特別なプロパティを持つPKEを使用する）の標準の構築方法について説明する。本主要によって、DDH仮定とDLIN（$d \geq 2$）仮定によってプロトコルが生成される。簡単な比較は表1のとおりである。

紛失通信に関するこれらの手法は、two-party computation（2PC）プロトコルのような複雑かつ高機能なプロトコルを構築するために必須である。理論的には、紛失通信において暗号文を構築することが可能であるため、紛失通信はSecurity Fundamentals Groupの研究課題としては適切なものであった。

2 注記

本論文において、$\mathrm{OT}^{n}_{k\times 1}$は、送信者の$n$個のメッセージと受信者の$k$個の選択肢を含む適応性のあるOTを指す。ZKPKはzero-knowledge proof of knowledge（知識のゼロ知識証明）を指し、ZKPMはzero-knowledge proof of membership（メンバーシップのゼロ知識証明）を指す。WIPKはwitness-indistinguishable proof of knowledge（証拠識別不能知識証明）を指す。

表1 完全にシミュレーション可能な適応性の高いOTスキーム

スキーム	仮定	通信コスト（1回あたり）	初期化コスト
CNS [1]	q-strong DH および q-PDDH	$O(1)$	$O(n)$
GH [5]	q-hidden LRSW（UC secure）	$O(1)$	$O(n)$
JL [8]	q-DHI（RSA グループ）	$O(1)$	$O(n)$
KN [9]	DDH	$O(n)$	$O(n)$
GH [6]	decision 3-party DH（3DDH）	$O(1)$	$O(n)$
KNP [10]	DDH	$O(1)$	$O(n)$（変動が多い）
KNP [11]	DDH	$O(1)$	$O(n)$（変動が少ない）
	DLIN		$O(n)$

（ランダム・オラクルを含まない）

$a[i]$ は、a の i-番目の要素を指す。例えば、a がビットスリングであるとき、$a[i]$ は i 番目のビットを指す。a が複数の要素を含むタプルであるとき、$a[i]$ は i 番目の要素となる。

3 単純な 1-out-of-2 OT の構築

(KGen, Enc, Dec) のアルゴリズムで構成される PKE が存在するとする。アルゴリズム KGen は公開鍵 pk と秘密鍵 sk を戻す。pk を使用して、Enc はメッセージ m を入力し、暗号文 c を戻し、暗号文 c は sk を使用して Dec によって解読される。

送信者が2つのメッセージ m_0, m_1 を保有し、受信者がビット b を保有するとする。受信者は送信者に b を開示することなく、m_b を取得したいとする。その際、以下が実行される。

1. 受信者は送信者に対して $(pk_b, sk_b) \leftarrow \mathrm{KGen}$ と完全にランダム化した pk_{1-b} を送信する。
2. 送信者は受信者に対して $c_0 = \mathrm{Enc}(pk_0, m_0)$ と $c_1 = \mathrm{Enc}(pk_1, m_1)$ を送信する。
3. 受信者は sk_b を使用して c_b を解読し、m_b を取得する。

送信者がビット b について認識することができないように、pk_b は乱数と区別できない必要がある。つまり、KGen が乱数に見える公開鍵を発行する必要がある。本条件は、実際に使用されている多くの PKE スキームで実現している。

受信者が m_{1-b} を取得することができないように、$\mathrm{Enc}(pk_{1-b}, m_{1-b})$ がゼロの $\mathrm{Enc}(pk_{1-b}, 0)$ の暗号化と区別できない必要がある。ゼロの $\mathrm{Enc}(pk_{1-b}, 0)$ は PKE の標準の強秘匿性 [4] のことを指す。本条件も、論文における多くのスキームで実現している。

4 検証可能シャッフルに基づいて構築した一般的な適応性のある OT

ここで、完全にシミュレーション可能なセキュリティを有する適応性のある OT の一般的な構築について説明する。まず、構成要素がいくつか必要となる。

4.1 主要な要素

4.1.1 閾値公開鍵暗号

2-out-of-2 閾値公開鍵暗号（TPKE）スキームは、以下のアルゴリズムによって構成される。

- TGen：S と R の2者がプロトコルを運用し、それぞれ (pk, sk_S) と (pk, sk_R) を取得する。pk は合意された公開鍵を指し、sk_S, sk_R は共有された秘密鍵を指す。（公開鍵は以下の全てのアルゴリズムで必要である、明確に説明するために公開鍵については記載しない。）
- $\mathrm{TEnc}(M; r)$：プレーンテキスト M とランダム・コイン r に対して暗号文 C を出力する。

- TDec(sk_P, C)：P∈{S, R}の場合、μ_P（秘密鍵key sk_Pに基づいて暗号文Cを解読したもの）を出力する。
- TComb(C, μ_S, μ_R)：入力C, μ_S, μ_Rを組み合わせることによって、プレーンテキストMを出力する。

TPKEスキームには、以下のプロパティが必要である。

準同型：

$$\mathrm{TEnc}(M;r) \otimes \mathrm{TEnc}(M';r') = \mathrm{TEnc}(M \oplus M'; r \odot r')$$

上記において、$\otimes, \oplus, \odot$は対応するスペースにおける演算子を指す。

強秘匿性：全てのMについて、乱数rに対応する暗号文Enc$(M;r)$は暗号文スペースを通じてほぼ常に配布される。

4.1.2 検証可能なシャッフル

TPKEの$1 \le i \le n$に対して、一連の暗号文$C_i = \mathrm{TEnc}(M_i; r_i)$がSによって作成されたとする。$I$はメッセージ・スペースの単位元であるとする。Rが$\{1, \ldots, n\}$上の順列$\pi$を選択し、$s_i$をランダム化して$1 \le i \le n$に対して一連の$C_i' = C_{\pi(i)} \otimes \mathrm{TEnc}(I; s_i)$を構築することで、両方の暗号文に同じプレーンテキストが含まれるようにすることは容易なことである。$C_i'(1 \le i \le n)$のセットは、オリジナルのシャッフルと呼ばれる。スキームTPKEが強秘匿性である場合、シャッフル$C_i'(1 \le i \le n)$を公開することでは順列πのどの情報もSには開示されない。シャッフルの正確性は以下のプロトコルで検証される。

$$\mathrm{ZKPK}\ \{(\pi, s_i): C_i' = C_{\pi(i)} \otimes \mathrm{TEnc}(I; s_i)\ \forall 1 \le i \le n\},$$

GrothおよびLu[7]による研究のとおり、上記のプロトコルは、ElGamalやPaillier等の準同型の暗号化スキームでは効果的に機能する。より広い意味で、Groth and Luによる研究成果は、以下のプロパティを有する準同型の暗号化スキームに適用することができる。

適切なメッセージ・スペース：メッセージ・スペースに小さな素因数（例：2^{80}より小さい素因数）が存在しないこと

ルートの抽出：$C^e = \mathrm{TEnc}(M; R)$から効率的にそれぞれの$e$とメッセージスペースの次数とが互いに素となる組み合わせについて$C = \mathrm{TEnc}(m; r)$となるような$(m; r)$を抽出することができる。

文献[7]で説明される検証可能なシャッフルのプロトコルは、統計情報に基づいた3ラウンドのhonest verifier zero-knowledge（HVZK）に基づく引数であり、標準の手法に基づいて完全なゼロ知識に変更することができる。

4.2 一般的なOTプロトコル

初期化

1. 送信者Sと受信者Rがプロトコル TGenを運用し、両者が共通の公開鍵pkを取得し、Sが秘密鍵sk_Sを取得し、Rが秘密鍵sk_Rを取得する。受信者RはZKPKによってpkに対応するsk_Rを認識していることを証明する。
2. $1 \le i \le n$について、Sは以下を計算し、Rに送信する。

$$C_i = \mathrm{TEnc}(M_i; r_i)$$

r_iはTEncが使用する乱数列を指す。

3. その後、送信者SはZKPKによってRに対して全てのiについてM_iを認識していることを証明する。（上記は、以下のインスタンス化においてr_iを認識していることを証明することと等しい。）
4. （**シャッフリング**）受信者Rは$\{1, \ldots, n\}$上の順列πと$1 \le i \le n$に対する乱数列数s_iを選択し、全てのiに関して以下を計算しSに対して送信する。

$$C_i' = C_{\pi(i)} \otimes \mathrm{TEnc}(I; s_i),$$

Iはメッセージ・スペースの単位元である。

5. 受信者Rは、ZKPKによってSに対してステップ**4.2**で説明される式を満足するπと$s_i(1 \le i \le n)$について認識していることを証明する。

j番目の送信

1. 受信者Rは入力項目としてインデックスσを取得し、Sに送信する。
2. 送信者Sは以下を確認し、

$$C' \in \{C_1', \ldots, C_n'\}$$

その後、以下を計算しRに送信する。

$\mu_S = \mathrm{TDec}(sk_S, C)$

3. その後、送信者SはZKPMによって上位のステップにおいて適切な暗号解読を行ったことを証明する。
4. 受信者Rも以下の通り暗号解読を行い、

$\mu_R = \mathrm{TDec}(sk_R, C)$

その後、$\mathrm{TComb}(pk, C, \mu_S, \mu_R)$によって$M_\sigma$を取得する。

以下の結果は、[11]においてKurosawa、Nojima、およびPhongによって構築されたものである。証明については[11]を参照すること。

命題：TPKEが強秘匿性を有する場合、上記の検証可能なシャッフルに基づいて構築した一般的な$\mathrm{OT}^n_{k\times 1}$は完全にシミュレーション可能である。

4.3 DDH仮定およびDLIN仮定によるインスタンス化

4.3.1 DDH仮定に基づいて構築した$\mathrm{OT}^n_{k\times 1}$

閾値ElGamalによる暗号化スキームを使用する。本スキームは巡回群$G=(G,g,q)$において機能し、本巡回群においてgは一次配列qを生成し、GにおけるDDH仮定に基づいて強秘匿性を有する。

- TGen：Sは$sk_S = x_0 \leftarrow Z_q$を選択し、$h_0 \leftarrow g^{x_0}$を計算しRに送信する。同様に、Rは$sk_R = x_1 \leftarrow Z_q$を選択し、Sに$h_1 \leftarrow g^{x_1}$を送信する。同意された公開鍵は$h = h_0 h_1$である。
- $\mathrm{TEnc}(M; r)$：$r \leftarrow Z_q$および$M \in G$の場合に、以下を出力する。

$$C = (C[1], C[2]) = (g^r, M \cdot h^r)$$

- $\mathrm{TDec}(sk_P, C)$：PがSまたはRの場合に、$\mu_P = C[1]^{sk}$Pを出力する。
- $\mathrm{TComb}(C, \mu_S, \mu_R)$：$C[2]/(\mu_S \mu_R)$を出力する。

TPKEスキームは、**4.1**で説明した全ての条件を満たす。したがって、閾値ElGamalの暗号化スキームに基づいて$\mathrm{OT}^n_{k\times 1}$プロトコルを実現することができる。閾値ElGamalの暗号化スキームは上記命題のとおりDDH仮定に基づいて強秘匿性を有するため、$\mathrm{OT}^n_{k\times 1}$は本仮定に基づいて完全にシミュレーション可能である。

4.3.2 DLIN仮定に基づいて構築した$\mathrm{OT}^n_{k\times 1}$

$G=(G,g,q)$についても研究を行う。注記を追加する。以下のベクトルについて、

$$v = (v[1], \ldots, v[l]) \in G^{1\times l}$$
$$u = (u[1], \ldots, u[l]) \in Z_q^{1\times l}$$

以下を定義する。

$$v \cdot u^{\mathrm{T}} = u \cdot v^{\mathrm{T}} = \prod_{i=1}^{l} v[i]^{u[i]} \in G.$$

マトリックス−マトリックス乗数およびマトリックス−ベクトル乗数は同様に規定できる。場合によっては、演算子は暗黙的に理解される。また、$u, u' \in Z_q^{1\times l}$の場合、通常$u+u' = (u[1]+u'[1], \ldots, u[l]+u'[l])$となる。$(u+u')\cdot v^{\mathrm{T}} = (u\cdot v^{\mathrm{T}})(u'\cdot v^{\mathrm{T}}) \in G$および$v\cdot(u+u')^{\mathrm{T}} = (v\cdot u^{\mathrm{T}})(v\cdot u'^{\mathrm{T}}) \in G.$であることは容易に検証できる。

$d \geq 2,$の場合は、NaorおよびSegev[13]が紹介した以下のPKEスキームは、DLIN仮定に基づいて強秘匿性を有する。

- Gen：$sk \leftarrow Z_q^{(d+1)\times 1}, \varphi \leftarrow G^{d\times(d+1)}.$
  $\psi = \varphi \cdot sk \in G^{d\times 1}$の場合、秘密鍵は$sk$であり、公開鍵は$pk = (\varphi, \psi)$である。
- $\mathrm{Enc}(M; R)$：$M \in G$のメッセージとランダム化した$R \in Z_q^{1\times d}$を入力し、以下の暗号文を出力する。

$$C = (R\varphi, (R\psi)M) \in G^{1\times(d+1)} \times G.$$

- $\mathrm{Dec}(sk, C)$：Cおよびskの入力に対して、$C[2]/(C[1]\cdot sk)$を出力する。
  PKEスキームの確度は、式$(R\cdot\varphi)\cdot sk = R\cdot(\varphi\cdot sk)$によって得られる。PKEスキームの強秘匿性によって、φ, ψの場合、ペア$\mathrm{Enc}(1; R) = (R\varphi, R\psi)$は$G^{1\times(d+1)} \times G$上の乱数と区別できない。
  ここで、上記のPKEに関連して2-out-of-2閾値変化について説明する。これは、DLIN仮定に基づく適応性のあるOTによって実現するものである。
- TGen：SとRはGを使用してマトリックス$\varphi \in G^{d\times(d+1)}$について同意する。その後、両者はそれぞれ$Z_q^{(d+1)\times 1}$において秘密鍵$sk_S$および$sk_R$を選択する。Sは$\psi_S = \varphi \cdot sk_S \in G^{d\times 1}$を公開し、Rは$\psi_R = \varphi \cdot sk_R \in G^{d\times 1}$を公開する。同意

された共通の公開鍵は φ, ψ_S, ψ_R である。本公開鍵において、

$$\psi=\psi_S\psi_R=(\psi_S[1]\psi_R[1], \ldots, \psi_S[d]\psi_R[d])^T \in G^{d\times 1}$$

が暗号化のために使用される。$\psi=\varphi\cdot(sk_S+sk_R)$ の条件が存在する。

- TEnc $(M;R)$：以下を出力する。

$$C=\mathrm{Enc}(M;R)=(R\varphi, (R\psi)M) \in G^{1\times(d+1)}\times G$$

- TDec (sk_P, C)：$P\in\{S,R\}$ の場合、以下を出力する。

$$\mu_P=C[1]\cdot sk_P \in G$$

- TComb (C, μ_S, μ_R)：$C[2]/(\mu_S\mu_R)$ を出力する。

OT の一般的な構築の際に上記のスキームを使用することで、DLIN 仮定に基づいて完全にシミュレーション可能なインスタンス化を実現することができる。

5 結論

本稿においては、暗号の基本的な要素と考えられる OT を構築するためのいくつかの手法について考察した。

現実的なメリットとして、クラウド・ストレージやクラウド・コンピューティングにおいてプライバシーを保護するシステムを開発するために役立つ手法が可能になるものと考えられる。本手法には改善の余地があり、将来的にはより優れた OT スキームが提供されるようになるものと考えられる。

参考文献

1 J. Camenisch, G. Neven, and A. Shelat, "Simulatable adaptive oblivious transfer," In M. Naor, editor, EUROCRYPT, Vol. 4515 of Lecture Notes in Computer Science, pp. 573–590, Springer, 2007.

2 S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," In CRYPTO, pp. 205–210, 1982.

3 Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan, "The relationship between public key encryption and oblivious transfer," In FOCS, pp. 325–335, 2000.

4 S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., 28(2): 270–299, 1984.

5 M. Green and S. Hohenberger, "Universally composable adaptive oblivious transfer," In J. Pieprzyk, editor, ASIACRYPT, volume 5350 of Lecture Notes in Computer Science, pp. 179–197, Springer, 2008.

6 M. Green and S. Hohenberger, "Practical adaptive oblivious transfer from a simple assumption," Cryptology ePrint Archive, Report 2010/109, 2010. http://eprint.iacr.org/

7 J. Groth and S. Lu, "Verifiable shuffle of large size ciphertexts," In T. Okamoto and X. Wang, editors, Public Key Cryptography, Vol. 4450 of Lecture Notes in Computer Science, pp. 377–392, Springer, 2007.

8 S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection," In O. Reingold, editor, TCC, Vol. 5444 of Lecture Notes in Computer Science, pp. 577–594, Springer, 2009.

9 K. Kurosawa and R. Nojima, "Simple adaptive oblivious transfer without random oracle," In M. Matsui, editor, ASIACRYPT, Vol. 5912 of Lecture Notes in Computer Science, pp. 334–346, Springer, 2009.

10 K. Kurosawa, R. Nojima, and L. T. Phong "Efficiency-improved fully simulatable adaptive ot under the DDH assumption," In J. A. Garay and R. D. Prisco, editors, SCN, Vol. 6280 of Lecture Notes in Computer Science, pp. 172–181, Springer, 2010.

11 K. Kurosawa, R. Nojima, and L. T. Phong, "Generic fully simulatable adaptive oblivious transfer," In 9th International Conference on Applied Cryptography and Network Security (ACNS ' 11), 2011. To appear.

12 M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," In M. J. Wiener, editor, CRYPTO, Vol. 1666 of Lecture Notes in Computer Science, pp. 573–590, Springer, 1999.

13 M. Naor and G. Segev, "Public-key cryptosystems resilient to key leakage," In S. Halevi, editor, CRYPTO, Vol. 5677 of Lecture Notes in Computer Science, pp. 18–35, Springer, 2009. Full version available at http://eprint.iacr.org/2009/105.pdf

14 C. A. Neff, "A verifiable secret shuffle and its application to e-voting," In ACM Conference on Computer and Communications Security, pp. 116–125, 2001.

15 W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity, 20(2-3): 356–371, 2004. Also available at http://eprint.iacr.org/2002/182

（平成23年6月15日 採録）

Le Trieu Phong
ネットワークセキュリティ研究所
セキュリティ基盤研究室専攻研究員
博士（学術）
暗号プロトコル