抽出可能ハッシュ証明システムを用いたKEMの構成について

松田 隆宏* 花岡 悟一郎

産業技術総合研究所 情報セキュリティ研究センター
305-8568 茨城県つくば市梅園 1-1-1 つくば中央第 2 事業所つくば本部・情報技術共同研究棟
{t-matsuda,goichiro-hanaoka}@aist.go.jp

あらまし CRYPTO 2010 において、Wee は、“抽出可能ハッシュ証明システム”(XHPS) の概念を導入し、XHPS から選択暗号文攻撃に対して安全な (CCA 安全な)KEM が構成できることを示し、これによって、近年の “探索問題の困難性” に基づく方式の構成や安全性証明を抽象化・一般化した枠組みで説明できるとした。本稿では、この XHPS に基づく KEM について振り返る。まず、この KEM の CCA 安全性を証明するためには、XHPS に必要な要件を弱めることができることを示す。これによって、Wee の示した枠組みよりも多くの CCA 安全な KEM の安全性を説明できるようになり、新たな CCA 安全な方式も導出できる。また、XHPS に新たな性質を導入し、この性質を持つ XHPS から KEM を構成すると、CCA 安全なハイブリッド暗号を構成する際に有用な安全性である “Constrained” CCA 安全性を満たすことを示す。最後に、XHPS から構成される KEM は、効率的な複数受信者用 KEM へと拡張できることを示す。この手法によって、多くの新たな効率的複数受信者用 KEM が得られる。

More on KEMs Based on Extractable Hash Proof Systems

Takahiro Matsuda Goichiro Hanaoka

Research Center for Information Security (RCIS), AIST,
Tsukuba Central 2, 1-1-1, Umezono, Tsukuba, Ibaraki 305-8568.

Abstract In CRYPTO 2010, Wee proposed the notion of ”Extractable Hash Proof Systems” (XHPS), and showed that CCA secure KEMs can be constructed from it. This explains several recently proposed KEMs based on the hardness of search problems (rather than decisional problems) in a general framework. We revisit XHPS and the XHPS-based KEM, and show that to prove CCA security of the XHPS-based KEM, some requirements can be relaxed. This widens the applicability of the original framework, and explains why many known KEMs are CCA secure. Moreover, we introduce a new property for XHPS, and show how it leads to KEMs that achieve “constrained” CCA security, which is a useful security notion of KEMs for obtaining CCA secure PKE schemes. Finally, we show that the XHPS-based KEM can be extended to efficient multi-recipient KEMs, from which we can derive several new efficient schemes.

1 はじめに

実用的な効率性を持つ選択暗号文攻撃 (CCA) に対する安全性を持つ公開鍵暗号 (PKE) の構成は重要な研究課題である。その中でも、鍵カプセル化メカニズム (KEM) と共通鍵暗号 (DEM) を用いた “ハイブリッド暗号” の構成法が確立されており、CCA 安全性や、Constrained CCA (CCCA) 安全性と呼ばれる安全性を持つ KEM と、それらに対応した適切な安全性を持つ DEM を組み合わせることにより、CCA 安全な PKE を構成できることが知られている [3, 7]。従って、効率の良い (C)CCA 安全な KEM を構成することは、効率的な PKE のための主要な方法である。

CRYPTO’10 において、Wee [9] は、“抽出可能ハッシュ証明システム” (eXtractable Hash Proof System, XHPS)、及びその機能拡張版である All-But-One XHPS, (**ABO-XHPS**) という概念を導入し、ABO-XHPS に基づく CCA 安全な KEM の構成法を示した。そして、近年提案されてきた実用的効率性を持つ具体的な計算問題の困難性に基づく CCA 安全な KEM([1, 2, 8] など) の構成・証明方法は、(ABO-)XHPS という抽象化・一般化された枠組みで説明できることを示した。XHPS の枠組みの特徴として、“判定問題” の困難性のみではなく、近年増えてきている “探索問題” の困難性に基づく KEM ([2, 8] など) の構成や安全性を説明できるとい

*日本学術振興会特別研究員 (PD)。

う点が挙げられる。

しかし、ABO-XHPS を用いた枠組みで説明できる上記の具体的な KEM と一見似たような構成・証明手法であるが、[9] の枠組みには当てはまらない (C)CCA 安全な KEM も多数存在するため ([7, 4, 5] など)、XHPS から CCA 安全な KEM を構成する [9] の枠組みをさらに拡張し、より広いクラスの KEM の構成・安全性証明を捕らえることができるようにできれば、KEM の構成・安全性証明の手法に関するより深い理解に繋がり、今後の (C)CCA 安全な KEM 及び PKE の構成法、さらに、KEM や PKE を構成要素とする上位の暗号技術の研究にとって非常に有用であると考えられる。

本研究の貢献　本稿では、[9] での ABO-XHPS に基づく KEM について振り返る。第一に、この KEM の CCA 安全性を証明するためには、構成要素の ABO-XHPS に必要な機能的要件を弱め、代わりに我々が新たに提案する計算量的な性質 “計算量的健全性”(CS 安全性) を満たしていれば十分であることを示す。この機能的要件の弱化によって、[9] で示された枠組みでは捕らえきれない多くの CCA 安全な KEM の安全性を説明できるようになり、さらに、新たな CCA 安全な KEM も導出できる。第二に、上記とは別の新たな ABO-XHPS の性質 “抽出される値の擬似ランダム性”(PR-Ext 安全性) を提案し、この性質を持つ ABO-XHPS から KEM を構成すると、CCCA 安全性を満たすことを示す。また、PR-Ext 安全な ABO-XHPS から、CS 安全な方式への変換法も示す。最後に、XHPS から構成される KEM は、効率的な (C)CCA 安全性を持つ複数受信者用 KEM へと拡張できることを示す。

以上の成果により、ABO-XHPS の枠組みでその構成・安全性を説明できる既存の KEM の幅は広がり、さらに、多くの新しい (C)CCA 安全な (単一・複数受信者用の)KEM が構成できる。特に、複数受信者用の KEM では、現在知られる方式で最も暗号文サイズに関して効率の良い方式や、素因数分解に基づく効率的な方式が得られる。(なお、紙面の都合上、本稿では定義の一部、及び全ての定理の証明を省略する。)

2　諸定義

本節では、本稿で使用する基礎的な用語や要素技術の定義を行う。基本的な表記法/用語として本稿では以下を用いる: n が整数ならば $[n] = \{1, \ldots, n\}$ とする。“$x \leftarrow y$” は y が集合ならば x を一様ランダムに取り出す操作を、それ以外は単に y を x に代入する操作を表す。“PPTA” は確率多項式時間アルゴリズムを意味する。“k” は常にセキュリティパラメータを指すことにする。

複数受信用 KEM　複数受信者用 KEM Γ は、以下の様な入出力を持つ 5 つの PPTA (MSetup, MKG, MEnc, MExt, MDec) からなる: (ここでは n 人の受信者の場合を考える)

セットアップ:	pp	$\leftarrow \mathtt{MSetup}(1^k)$
鍵生成:	(pk, sk)	$\leftarrow \mathtt{MKG}(\mathsf{pp})$
カプセル化:	(c, K)	$\leftarrow \mathtt{MEnc}(\mathbf{pk})$
各受信者の暗号文抽出:	c_i	$\leftarrow \mathtt{MExt}(pk_i, c)$
復号:	$K \ / \ \perp$	$\leftarrow \mathtt{MDec}(sk_i, c_i)$

上記において、pp は公開パラメータであり、明示しないが全てのアルゴリズムに入力されるとする。(pk, sk) は公開鍵/秘密鍵対、$\mathbf{pk} = (pk_1, \ldots, pk_n)$ は受信者 1 から受信者 n までの公開鍵であり、c はセッション鍵 $K \in \mathcal{K}$ の受信者 1 から受信者 n までに向けた暗号文、c_i は c から抽出された受信者 i 用の暗号文である。$\mathcal{K}$ は Γ のセッション鍵空間である。

複数受信者用 KEM の正当性として、全ての $\mathsf{pp} \leftarrow \mathtt{MSetup}(1^k)$、全ての多項式 $n = n(k)$ について、以下の確率が無視できることを要求する。

$$\Pr[\ (pk_i, sk_i) \leftarrow \mathtt{MKG}(\mathsf{pp}) \text{ for } i \in [n];\ (c, K) \leftarrow \mathtt{MEnc}(\mathbf{pk} = (pk_1, \ldots, pk_n)) : \mathtt{MDec}(sk_i, \mathtt{MExt}(pk_i, c)) \neq K \text{ for some } i \in [n]\ ]$$

安全性の定義　本稿では、複数受信者用 KEM の安全性として選択暗号文攻撃に対する識別不可能性 (CCA 安全性) と、Constrained CCA 安全性 (CCCA 安全性) [7] を取り扱う。

$\mathtt{ATK} \in \{\mathtt{CCA}, \mathtt{CCCA}\}$、$n \in \mathbb{N}$ とする。複数受信者用 KEM Γ を ATK 攻撃する攻撃者 $\mathcal{A}$ のアドバンテージを以下で定義する:

$$\mathsf{Adv}^{\mathtt{ATK}}_{\Gamma,\mathcal{A},n}(k) = |\Pr[\mathsf{pp} \leftarrow \mathtt{MSetup}(1^k);\ (pk_i, sk_i) \leftarrow \mathtt{MKG}(\mathsf{pp}) \text{ for } i \in [n];\ K_0^* \leftarrow \mathcal{K};\ (c^*, K_1^*) \leftarrow \mathtt{MEnc}(\mathbf{pk} = (pk_1, \ldots, pk_n));\ b \leftarrow \{0,1\};\ b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pp}, \mathbf{pk}, c^*, K_b^*) : b' = b] - 1/2|$$

ただし、$\mathtt{ATK} = \mathtt{CCA}$ の場合、$\mathcal{O}$ は復号オラクルであり、受信者番号 $i \in [n]$ と暗号文 c を受け取り、$K = \mathtt{MDec}(sk_i, \mathtt{MExt}(pk_i, c))$ を返す。また、$\mathtt{ATK} = \mathtt{CCCA}$ の場合、$\mathcal{O}$ は Constrained 復号 (CDEC) オラクルであり、入力として受信者番号 $i \in [n]$、述語 $\mathsf{pred}(\cdot) : \mathcal{K} \to \{0,1\}$、及び暗号文 c を受け取り、以下の様に動作する:

$$\mathcal{O}_{cdec}(i, \mathsf{pred}(\cdot), c) = \begin{cases} K & \mathtt{MDec}(sk_i, \mathtt{MExt}(pk_i, c)) = K \neq \perp \\ & \wedge\ \mathsf{pred}(K) = 1 \text{ の場合} \\ \perp & \text{それ以外} \end{cases}$$

さらに、ATK に依らず、$\mathcal{A}$ は $\mathtt{MExt}(pk_i, c) = \mathtt{MExt}(pk_i, c^*)$ を満たすクエリをしてはならない。

CCCA 試行において、Q 回クエリを行う攻撃者 $\mathcal{A}$ を考える。$\mathcal{A}$ の j 回目の CDEC クエリを $(i_j, \mathsf{pred}_j(\cdot), c_j)$ と書くとする。攻撃者 $\mathcal{A}$ と全ての pred_j が PPTA であり、以下で定義される “試行 $\mathcal{E}$ についての $\mathcal{A}$ の Uncertainty” と呼ばれるパラメータ:

$$\mu_{\mathcal{A},\mathsf{Expt}} = \frac{1}{Q} \sum_{j \in [Q]} \Pr[\mathcal{E}; K \leftarrow \mathcal{K} : \mathsf{pred}_j(K) = 1]$$

が全ての “CCCA 試行と同等のステップ数で動作する試行 $\mathcal{E}$” について無視できる場合、$\mathcal{A}$ は “正当な CCCA 攻撃者” であると定義する。

定義 1. 全ての *PPTA* $\mathcal{A}$ と全ての多項式 $n = n(k)$ について $\mathsf{Adv}^{\mathtt{CCA}}_{\Gamma,\mathcal{A},n}(k)$ が無視できる場合、複数受信者用 *KEM* Γ は CCA 安全であるという。また、全ての正当な CCCA 攻撃者 $\mathcal{A}$ と全ての多項式 $n = n(k)$ について $\mathsf{Adv}^{\mathtt{CCCA}}_{\Gamma,\mathcal{A},n}(k)$ が無視できる場合、Γ は CCCA 安全であるという。

単一受信者用の KEM 単一受信者用の KEM を考える場合はセットアップと鍵生成を分けて考える必要が無いため、区別のために、鍵生成、カプセル化、復号のアルゴリズムをそれぞれ KG、Enc、Dec と “M” をつけないで書くことにする。

3 抽出可能ハッシュ証明システム

本節では、ABO-XHPS 及びそれを説明する際に必要となる一方向関係族についての定義を、[9] での定義と対比しつつ振り返る。その後、4 節での ABO-XHPS に基づく KEM の (C)CCA 安全性に繋がる新たな性質を 2 種類提案し、さらに片方の性質を満たす ABO-XHPS からもう片方の性質を満たす方式への変換を提案する。

3.1 一方向関係族

二項関係 R には、“ある値 u を与えられ、$(u,s) \in R$ を満たす s を求めよ” という “探索問題” を自然に定義できる。一方向関係とは、u を与えられても $(u,s) \in R$ を満たす s を計算するのが困難な二項関係 R のことを指す。より一般的に、R がパラメータ pp に依存する場合を考え、それを “一方向関係族” 呼ぶ。[9] に習い、以下の様に関係族を定式化する。

(擬似乱数生成器 (PRG) を持つ様な) 関係族 $\mathcal{R}$ は以下の 3 つの PPTA $(\mathtt{SetupR}, \mathtt{SampR}, \mathsf{G})$ からなる: $\mathtt{SetupR}$ は 1^k を入力として受け取り、公開/秘密パラメータの対 $(\mathsf{pp}, \mathsf{sp})$ を出力する。表記の簡単化のため明示しないが、pp は他の二つのアルゴリズムにも入力される。pp は集合 $\mathcal{U}$、$\mathcal{S}$, $\mathcal{W}$、及び $\mathcal{K}$ を決定し、さらに $\mathcal{U} \times \mathcal{S}$ 上での関係 $\mathcal{R}_{\mathsf{pp}}$ を一つ決定する。$\mathtt{SampR}$ は一様乱数 $w \in \mathcal{W}$ を用いて $(u,s) \in \mathcal{R}_{\mathsf{pp}}$ を満たすペアを、$u \in \mathcal{U}$ が一様ランダムである様に選び出力する。G は pp によって決まる PRG であり、$s \in \mathcal{S}$ を受け取り、$K \in \mathcal{K}$ を出力する。

(PRG を持つ) 一方向関係族としての安全性を定義するために、関係族 $\mathcal{R}$ の持つ PRG G の擬似ランダム性に対する攻撃者 $\mathcal{A}$ のアドバンテージを以下で定義する:

$$\mathsf{Adv}^{\mathtt{PRG}}_{\mathcal{R},\mathcal{A}}(k) = |\Pr[(\mathsf{pp},\mathsf{sp}) \leftarrow \mathtt{SetupR}(1^k); w \leftarrow \mathcal{W}; (u,s) \leftarrow \mathtt{SampR}(w); b \leftarrow \{0,1\}; K_0^* \leftarrow \mathcal{K}; K_1^* \leftarrow \mathsf{G}(s); b' \leftarrow \mathcal{A}(\mathsf{pp}, u, K_b^*) : b' = b] - 1/2|$$

定義 2. $\mathcal{R}$ を関係族とする。全ての *PPTA* $\mathcal{A}$ について $\mathsf{Adv}^{\mathtt{PRG}}_{\mathcal{R},\mathcal{A}}(k)$ が無視できる場合、$\mathcal{R}$ を一方向関係族であるという。

具体的な一方向関係族 ここでは HDH 仮定 [4, 2] に基づく Diffie-Hellman 関係 $\mathcal{R}^{\mathsf{DH}}$ を一方向関係族の例として挙げる。$\mathbb{G}$ を素数位数 p の巡回群、$H : \mathbb{G} \to \{0,1\}^k$ をハッシュ関数とし、(G, H) で HDH 仮定が成り立つとする。$\mathcal{U} = \mathcal{S} = \mathbb{G}$、$\mathcal{W} = \mathbb{Z}_p$、$\mathcal{K} = \{0,1\}^k$ とする。$\mathcal{R}^{\mathsf{DH}} = (\mathtt{SetupR}, \mathtt{SampR}, \mathsf{G})$ は以下の通りである: $\mathtt{SetupR}$ は $\mathsf{sp} = \alpha \in \mathbb{Z}_p$ と $g \in \mathbb{G}$ を選び、$\mathsf{pp} = (g, h) = (g, g^\alpha)$ とする。pp は “$s = u^\alpha \Leftrightarrow (u,s) \in \mathcal{R}^{\mathsf{DH}}_{\mathsf{pp}}$” という関係を決定する。$\mathtt{SampR}$ は $w \in \mathbb{Z}_p$ をランダムに選び、$(u,s) = (g^w, h^w)$ を出力する。G は、$\mathsf{G}(s) = H(s)$ と定義する。HDH 仮定が成り立つならば、$\mathcal{R}^{\mathsf{DH}}$ は一方向関係族である。また、G の定義を変えることで、DDH や DBDH 仮定に基づく一方向関係族も考えることができる。

Wee [9] の一方向関係族の定義との違い [9] での定義では、一方向関係族 $\mathcal{R}$ の安全性をあらわす試行において、$(u,s) \in \mathcal{U} \times \mathcal{S}$ を受け取り、$(u,s) \in \mathcal{R}_{\mathsf{pp}}$ が成り立つかどうかを答える “関係オラクル” を攻撃者 $\mathcal{A}$ に与えた攻撃状況での G の擬似ランダム性を要求したが、このような一方向関係族の定義は、本稿での定義に比べ制限が大きく、例えば上記の HDH 仮定に基づく関係族 $\mathcal{R}^{\mathsf{DH}}$ は捕らえられない。[9] での定義を満たすためには、双線形写像を持つ群での計算困難性 (DBDH 仮定など) や、いわゆる Gap タイプのオラクルを考える仮定 (GHDH、SDH 仮定など) を要求する必要がある。

3.2 All-But-One XHPS

ABO-XHPS は (一方向) 関係族と関連付けられて定義される。以下では、ABO-XHPS $\mathcal{X}$ が関係族 $\mathcal{R}$ に関連付けられていることを明示する場合、“$\mathcal{X}^{\mathcal{R}}$” と記述する。概して言えば、ABO-XHPS は、計算困難な探索問題を持つ二項関係 $\mathcal{R}$ についてのいわゆる “検証者指定非対話型知識の証明プロトコル” のうち特殊な性質を持つものであり (証明システムとしての解釈については [9] を参照)、内部構造として、公開鍵 pk によって決定される (タグ付き) ハッシュ関数族 $\mathsf{H}_{pk} : \mathcal{T} \times \mathcal{U} \to \{0,1\}^*$ を持つ ($\mathcal{T}$ はタグ空間)。

ABO-XHPS $\mathcal{X}$ は以下の様な関係を全ての $(\mathsf{pp},\mathsf{sp}) \leftarrow \mathtt{SetupR}(1^k)$ で満たす 6 つの PPTA $(\mathtt{XKG}, \mathtt{Pub}, \mathtt{Ext}, \widehat{\mathtt{XKG}}, \widehat{\mathtt{Priv}}, \widehat{\mathtt{Ext}})$ からなる:

“証明” π の公開計算 全ての pk、全ての tag、及び全ての $(u,s) \leftarrow \mathtt{SampR}(w)$ で、$\pi = \mathtt{Pub}(pk, \mathsf{tag}, w) = \mathsf{H}_{pk}(\mathsf{tag}, u)$。

抽出モード. 全ての $(pk, sk) \leftarrow \mathtt{XKG}(\mathsf{pp}, \mathsf{sp})$ と全ての (tag, u, π) で、$\pi = \mathsf{H}_{pk}(\mathsf{tag}, u)$ なら

ば $s = \mathtt{Ext}(sk, \mathsf{tag}, u, \pi) \neq \perp$ かつ $(u, s) \in \mathcal{R}_{\mathsf{pp}}$、そうでなければ$\mathtt{Ext}(sk, \mathsf{tag}, u, \pi) = \perp$。

All-But-One (ABO) モード 全ての tag^* と全ての $(pk, \widehat{sk}) \leftarrow \widehat{\mathtt{XKG}}(\mathsf{pp}, \mathsf{tag}^*)$ について:
(1) **"証明"π の秘密計算**: 全ての $(u, s) \in \mathcal{R}_{\mathsf{pp}}$ で、$\pi = \widehat{\mathtt{Priv}}(\widehat{sk}, u) = \mathsf{H}_{pk}(\mathsf{tag}^*, u)$。
(2) 全ての $\mathsf{tag} \neq \mathsf{tag}^*$ 及び全ての (u, π) について、$\pi = \mathsf{H}_{pk}(\mathsf{tag}, u)$ ならば $s = \widehat{\mathtt{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi) \neq \perp$ かつ $(u, s) \in \mathcal{R}_{\mathsf{pp}}$。($\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ の場合の要件は無し。)

2 つのモードの識別不可能性 全ての tag^* について、2 つの分布 $\{(pk, sk) \leftarrow \mathtt{XKG}(\mathsf{pp}, \mathsf{sp}) : pk\}$ と $\{(pk, \widehat{sk}) \leftarrow \widehat{\mathtt{XKG}}(\mathsf{pp}, \mathsf{tag}^*) : pk\}$ は統計的に識別不可能。

Wee [9] の ABO-XHPS の定義との違い [9] の定義では、XKG には sp が入力されない。しかし、[9] の ABO-XHPS に基づく KEM の構成にはこの制限は不要であり、ABO-XHPS の構成の制限となるため、本稿では sp の入力を許す。

また、[9] の Ext 及び $\widehat{\mathtt{Ext}}$ は、機能的な要件 (正当性) として、(i) $\mathsf{H}_{pk}(\mathsf{tag}, u) = \pi \Leftrightarrow (u, \mathtt{Ext}(sk, \mathsf{tag}, u, \pi)) \in \mathcal{R}_{\mathsf{pp}}$、及び (ii) $\mathsf{H}_{pk}(\mathsf{tag}, u) = \pi \Leftrightarrow (u, \widehat{\mathtt{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)) \in \mathcal{R}_{\mathsf{pp}}$ が要求されるが、このうち (i) は、$\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$ の場合 Ext が何を出力するかが明確でないため、我々は $\perp$ が出力される様に明示的に要求する。知られている全ての ABO-XHPS はこの性質を満足する。(ii) については、本稿での要求の方が弱いことに気付かれたい。4 節で示す様に、[9] の ABO-XHPS に基づく KEM の CCA 安全性の証明のためには、本稿での弱い機能的要件と、3.3 節で導入する "計算量的な性質" のみ満たせば十分であるため、ABO-XHPS の構成の幅を広げるために、弱い定義を採用する。

3.3 計算量的健全性

ここでは、[9] で提案された ABO-XHPS に基づく KEM を CCA 安全であると示すために十分な、ABO-XHPS についての "計算量的な" 性質、**計算量的健全性**(Computational Soundness, 以下 CS 安全性) を提案する。概して言えば、CS 安全性は、ABO モードの証明システムとしての健全性であり、$\mathsf{tag} \neq \mathsf{tag}^*$、$\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$、かつ $\widehat{\mathtt{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi) \neq \perp$ となる (tag, u, π) を見つけることが困難であるという性質である。

CS 安全性は、攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ が ABO-XHPS $\mathcal{X}$ の CS 安全性を破ることを試される CS 試行 $\mathsf{Expt}^{\mathsf{CS}}_{\mathcal{X},\mathcal{A}}(k)$ (図 1 左) を用いて定義される。

定義 3. 全ての *PPTA* $\mathcal{A}$ について $\Pr[\mathsf{Expt}^{\mathsf{CS}}_{\mathcal{X},\mathcal{A}}(k) = 1]$ が無視できる場合、*ABO-XHPS* $\mathcal{X}$ は CS 安全であるという。

CS 安全性を持つ具体的な ABO-XHPS [9] において、Wee は DBDH 仮定を用いる [1] の KEM を基にした ABO-XHPS、CDH 仮定を用いる [2] の KEM を基にした ABO-XHPS、及び素因数分解の困難性に基づく [8] の KEM を基にした ABO-XHPS を示した。これらは全て CS 安全である。また、上記以外にも、近年提案された CCA 安全な KEM で、Selective 安全な ID ベース暗号でのような証明技法を用いる様な方式 ([4, 5, 10] など) はほぼ全て本稿での機能的要件を満たし、かつ CS 安全な ABO-XHPS として理解できる。

3.4 抽出された値の擬似ランダム性

ここでは、"**抽出された値の擬似ランダム性**" (Pseudorandom Extraction Property、以下 PR-Ext 安全性) という新たな ABO-XHPS の安全性を提案する。概して言えば、この安全性は、ABO モードの $\widehat{\mathtt{Ext}}$ を使って、$\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$ を満たす (tag, u, π) から s を抽出した場合、s が $\mathcal{S}$ の一様乱数と識別不可能できないことをを捕らえている。この安全性は、4 節において示す ABO-XHPS に基づく KEM の CCCA 安全性に繋がる。

PR-Ext 安全性は、攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ が ABO-XHPS $\mathcal{X}$ の PR-Ext 安全性を破ることを試される PR-Ext 試行 $\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k)$ (図 1 右) を用いて定義される。ただし、試行において、$\mathcal{A}_2$ の出力の中の $(\mathsf{tag}', u', \pi')$ は、$\mathsf{tag}' \neq \mathsf{tag}^*$ かつ $\mathsf{H}_{pk}(\mathsf{tag}', u') \neq \pi'$ を満たさねばならない。

定義 4. 全ての *PPTA* $\mathcal{A}$ について $|\Pr[\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k) = 1] - 1/2|$ が無視できる場合、*ABO-XHPS* $\mathcal{X}$ は PR-Ext 安全であるという。

PR-Ext 安全性を持つ具体的な ABO-XHPS ここでは、[7, Sect. 3.2] の KEM を基にした方式と、[4, Sect. 5] の KEM を基にした方式を図 2 に示す。両方式とも、3.1 節の Diffie-Hellman 関係族 $\mathcal{R}^{\mathsf{DH}}$ に関連付けられた ABO-XHPS であり、タグ空間 $\mathcal{T} = \mathbb{Z}_p$ である。なお、$\mathcal{X}_{\mathtt{HaKu}}$ の $\widehat{\mathtt{XKG}}$ における A_1 と A_2、及び、$\widehat{\mathtt{Ext}}$ における s はラグランジュ補完により計算できる。また、$\mathcal{X}_{\mathtt{HaKu}}$ の $\widehat{\mathtt{Ext}}$ において、$\mathsf{tag} = \mathsf{dummy}$ のときは s を計算できないが、dummy の情報は pk から情報理論的に隠されており、計算能力に依らず、dummy を発見することは困難である。

3.5 PR-Ext 安全性から CS 安全性への変換

PR-Ext 安全性を持つ ABO-XHPS $\mathcal{X}$ から、CS 安全性を持つ方式 $\mathcal{X}'$ を得る方法を提案する。

$\mathcal{R}$ を任意の関係族とする。ABO-XHPS $\mathcal{X}^{\mathcal{R}}$ から、別の ABO-XHPS $\mathcal{X}'^{\mathcal{R}}$ を図 3 の様に構成する (なお、同じ関係族 $\mathcal{R}$ に関連付けられている限り、構成要素として 2 つの別々の ABO-XHPS$\mathcal{X}_1^{\mathcal{R}}$、$\mathcal{X}_2^{\mathcal{R}}$ を用いても良い)。構成要素 $\mathcal{X}^{\mathcal{R}}$ の内部構造のハッシュ関数族を H とすると、$\mathcal{X}'^{\mathcal{R}}$ の内部構造のハッシュ関数族 H′ は、構成から自

然に $\mathsf{H}'_{PK}(\mathsf{tag}, u) = (\mathsf{H}_{pk_1}(\mathsf{tag}, u), \mathsf{H}_{pk_2}(\mathsf{tag}, u))$ と定義する。以下が示せる。

定理 1. $\mathcal{R}$ を任意の *(*必ずしも一方向でない*)* 関係族とする。$\mathcal{X}^{\mathcal{R}}$ が PR-Ext 安全な *ABO-XHPS* ならば、$\mathcal{X}'^{\mathcal{R}}$ は CS 安全な *ABO-XHPS* である。

4 ABO-XHPS を用いた KEM

本節では、本稿のまとめとして、ABO-XHPS を用いた KEM についての成果を示す。

$\mathcal{R}$ を関係族として、ABO-XHPS $\mathcal{X}^{\mathcal{R}}$ と、ターゲット衝突困難ハッシュ関数 (TCRHF) $\mathsf{TCR} : \mathcal{U} \to \mathcal{T}$ から、単一受信者用の KEM Γ_1 を図 4 左、複数受信者用の KEM Γ_M を図 4 右の様に構成する。以下の 2 つの定理が示せる。

定理 2. $\mathcal{R}$ が一方向関係族、$\mathcal{X}^{\mathcal{R}}$ が CS 安全 *(*同様に、PR-Ext 安全*)* な *ABO-XHPS*、TCR が *TCRHF* ならば、単一受信者用 *KEM* Γ_1 は CCA 安全 *(*同様に、CCCA 安全*)* である。

定理 3. $\mathcal{R}$ が一方向関係族、$\mathcal{X}^{\mathcal{R}}$ が CS 安全 *(*同様に、PR-Ext 安全*)* な *ABO-XHPS*、TCR が *TCRHF* ならば、複数受信者用 *KEM* Γ_M は CCA 安全 *(*同様に、CCCA 安全*)* である。

複数受信者用 KEM Γ_M は、ABO-XHPS の ABO モードで構成されていることに注意されたい。ABO モードでは、鍵生成の際に使用したタグ dummy を使った復号は不可能であるため、Γ_M では MEnc から出力された正しく作られた暗号文でも復号できない場合があるが、 ABO-XHPS の二つのモードの識別不能性により、dummy の情報は dummy を持つ受信者以外に対して情報理論的に隠されるため、MEnc を用いるかどうかに依らず $\mathsf{TCR}(u) = \mathsf{dummy}$ を満たす暗号文を作成することは実質不可能である。

Hiwatari ら [6] は、複数受信者用 KEM を 2 方式示したが、彼らの方式は Γ_M の構成要素として [2] と [4] の KEM に基づく ABO-XHPS を用いた形になっている。従って、Γ_M は、Hiwatari らの手法の ABO-XHPS を用いた一般化と考えることができる。

既存の (C)CCA 安全な KEM の安全性の説明 定理 2 によって、既存の CCA 安全な KEM [1, 2, 4, 5, 10]、あるいは CCCA 安全な KEM [7, 4] は、実は CS(あるいは PR-Ext) 安全な ABO-XHPS に、上記の変換を適用している構成になっていると見通しよく理解・説明できる。著者らは、本成果が今後 (C)CCA 安全な KEM を構成する際に良い知見を与えるものと信じている。

新たな (C)CCA 安全性を持つ KEM の導出 本節の成果により、多くの新たな KEM が得られる。例として、図 2 の二つの PR-Ext 安全な ABO-XHPS を定理 1 により組み合わせて CS 安全な ABO-XHPS を得て、それに定理 2 を適用して得られる単一受信者用 KEM を図 5 に示す。この方式は HDH 仮定に基づき安全性を証明でき、Cramer-Shoup [3] と同等の効率を持つ。

また、複数受信者用 KEM については、定理 3 を通して、3.3 節と 3.4 節で挙げた ABO-XHPS から新たな (C)CCA 安全な方式が数多く得られる。このうち前述の通り、[2] の KEM を基にした CS 安全な ABO-XHPS と [7] の KEM を基にした ABO-XHPS $\mathcal{X}_{\mathtt{HoKi}}$ からは Hiwatari ら [6] の提案した 2 つの方式そのものが得られる。また、それ以外では例えば、[1] の KEM に基づく CS 安全な ABO-XHPS からは、暗号文サイズが最も小さく (n 人に平文 m を送る際は $1+n$ 個の群の元 $+ |m|$ ビット)、各受信者の鍵サイズが定数の非常に効率的な方式が得られるほか、[8] の KEM を基にした CS 安全な ABO-XHPS からは、単純に n 個の暗号文を並べただけの方式と比較して真に効率が良い初の素因数分解の困難性に基づく複数受信者用 KEM が得られる。

このように新たな効率的な KEM が複数得られるということは、本稿の成果が有用であることの証であると考えられる。

参考文献

[1] X. Boyen, Q. Mei, and B. Waters. Direct chosen ciphertext security from identity-based techniques, 2005. Updated version of the paper published in ACMCCS 2005. Cryptology ePrint Archive: Report 2005/288.

[2] D. Cash, E. Kiltz, and V. Shoup. The twin Diffie-Hellman problem and applications. *EUROCRYPT 2008*, LNCS 4965, pp. 127–145, 2008.

[3] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Computing* 33(1):167-226, 2003.

[4] G. Hanaoka and K. Kurosawa. Efficient chosen ciphertext secure public key encryption under the computational Diffie-Hellman assumption. *ASIACRYPT 2008*, LNCS 5350, pp. 308–325, 2008.

[5] K. Haralambiev, T. Jager, E. Kiltz, and V. Shoup. Simple and efficient public-key encryption from computational Diffie-Hellman in the standard model. *PKC 2010*, LNCS 6056, pp. 279–295, 2010.

[6] H. Hiwatari, K. Tanaka, T. Asano, and K. Sakumoto. Multi-recipient public-key encryption from simulators in security proofs. *ACISP 2009*, LNCS 5594, pp. 293–308, 2009.

[7] D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. *CRYPTO 2007*, LNCS 4622, pp. 553–571, 2007.

[8] D. Hofheinz and E. Kiltz. Practical chosen ciphertext secure encryption from factoring. *EUROCRYPT 2009*, LNCS 5479, pp. 313–332, 2009.

[9] H. Wee. Efficient chosen-ciphertext security via extractable hash proofs. *CRYPTO 2010*, LNCS 6223, pp. 314–332, 2010.

[10] S. Yamada, Y. Kawai, G. Hanaoka, and N. Kunihiro. Public key encryption schemes from the (B)CDH assumption with better efficiency. *IEICE Transactions*, 93-A(11):1984–1993, 2010.

$\mathsf{Expt}^{\mathsf{CS}}_{\mathcal{X},\mathcal{A}}(k)$:
$(\mathsf{pp},\mathsf{sp}) \leftarrow \mathtt{SetupR}(1^k)$; $(\mathsf{tag}^*,\mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{pp})$;
$(pk,\widehat{sk}) \leftarrow \widehat{\mathtt{XKG}}(\mathsf{pp},\mathsf{tag}^*)$; $\mathcal{A}_2^{\mathcal{O}_{\mathsf{CS}}}(pk,\mathsf{st})$;
If $\mathcal{A}_2$ submits to $\mathcal{O}_{\mathsf{CS}}$ at least
one query (tag',u',π') s.t. $\mathsf{tag}' \neq \mathsf{tag}^* \wedge \mathsf{H}_{pk}(\mathsf{tag}',u') \neq \pi' \wedge \widehat{\mathtt{Ext}}(\widehat{sk},\mathsf{tag}',u',\pi') \neq \bot$
then return 1 else return 0

$\mathcal{O}_{\mathsf{CS}}(\mathsf{tag},u,\pi) = \begin{cases} \widehat{\mathtt{Ext}}(\widehat{sk},\mathsf{tag},u,\pi) & \text{If } \mathsf{tag} \neq \mathsf{tag}^* \\ \bot & \text{Otherwise} \end{cases}$

$\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k)$:
$(\mathsf{pp},\mathsf{sp}) \leftarrow \mathtt{SetupR}(1^k)$; $(\mathsf{tag}^*,\mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{pp})$;
$(pk,\widehat{sk}) \leftarrow \widehat{\mathtt{XKG}}(\mathsf{pp},\mathsf{tag}^*)$;
$(\mathsf{tag}',u',\pi',\mathsf{st}') \leftarrow \mathcal{A}_2^{\mathcal{O}_{\mathtt{PR}}}(pk,\mathsf{st})$; $b \leftarrow \{0,1\}$;
$s'_0 \leftarrow \mathcal{S}$; $s'_1 \leftarrow \widehat{\mathtt{Ext}}(\widehat{sk},\mathsf{tag}',u',\pi')$; $b' \leftarrow \mathcal{A}_3(s'_b,\mathsf{st}')$;
If $b'=b$ then return 1 else return 0

$\mathcal{O}_{\mathtt{PR}}(\mathsf{tag},u,\pi) =$
$\begin{cases} \widehat{\mathtt{Ext}}(\widehat{sk},\mathsf{tag},u,\pi) & \text{If } \mathsf{tag} \neq \mathsf{tag}^* \wedge \mathsf{H}_{pk}(\mathsf{tag},u) = \pi \\ \bot & \text{Otherwise} \end{cases}$

図 1: ABO-XHPS の安全性を定義するための試行とオラクルの定義。CS 試行 (左) と PR-Ext 試行 (右)。

$\mathtt{XKG}(\mathsf{pp},\mathsf{sp})$: $x_1,x_2 \leftarrow \mathbb{Z}_p$; $X_i \leftarrow g^{x_i}$ for $i \in [2]$ $pk \leftarrow (g,h,X_1,X_2)$; $sk \leftarrow (\alpha,x_1,x_2)$	$\mathtt{XKG}(\mathsf{pp},\mathsf{sp})$: $a_0 \leftarrow \alpha$; $A_0 \leftarrow h$; $a_1,a_2 \leftarrow \mathbb{Z}_p$ $A_1 \leftarrow g^{a_1}$; $A_2 \leftarrow g^{a_2}$; Let $f(x) := \sum_{i=0}^2 a_i x^i$ $pk \leftarrow (g,A_0,A_1,A_2)$; $sk \leftarrow f(\cdot)$
$\mathtt{Pub}(pk,\mathsf{tag},w)$: $\pi \leftarrow (X_1^{\mathsf{tag}}X_2)^w$	$\mathtt{Pub}(pk,\mathsf{tag},w)$: $\pi \leftarrow (A_0A_1^{\mathsf{tag}}A_2^{\mathsf{tag}^2})^w$
$\mathtt{Ext}(sk,\mathsf{tag},u,\pi)$: If $u^{x_1\cdot\mathsf{tag}+x_2} = \pi$ then $s \leftarrow u^\alpha$ else $s \leftarrow \bot$.	$\mathtt{Ext}(sk,\mathsf{tag},u,\pi)$: If $u^{f(\mathsf{tag})} = \pi$ then $s \leftarrow u^\alpha$ else $s \leftarrow \bot$.
$\widehat{\mathtt{XKG}}(\mathsf{pp},\mathsf{tag}^*)$: $z_1,z_2,z_3 \leftarrow \mathbb{Z}_p^*$ $X_1 \leftarrow g^{z_1}h^{z_2}$; $X_2 \leftarrow g^{z_3}h^{-\mathsf{tag}^*\cdot z_2}$ $pk \leftarrow (g,h,X_1,X_2)$; $\widehat{sk} \leftarrow (z_1,z_2,z_3,\mathsf{tag}^*)$	$\widehat{\mathtt{XKG}}(\mathsf{pp},\mathsf{tag}^*)$: $\mathsf{dummy},z_1,z_2 \leftarrow \mathbb{Z}_p^*$; $A_0 \leftarrow h$ Compute $A_1 = g^{a_1}$ and $A_2 = g^{a_2}$ s.t. $(f(0),f(\mathsf{dummy}),f(\mathsf{tag}^*)) = (\alpha,z_1,z_2)$. $pk \leftarrow (g,A_0,A_1,A_2)$; $\widehat{sk} \leftarrow (\mathsf{dummy},z_1,z_2,\mathsf{tag}^*)$
$\widehat{\mathtt{Priv}}(\widehat{sk},u)$: $\pi \leftarrow u^{z_1\cdot\mathsf{tag}^*+z_2}$	$\widehat{\mathtt{Priv}}(\widehat{sk},u)$: $\pi \leftarrow u^{z_2}$
$\widehat{\mathtt{Ext}}(\widehat{sk},\mathsf{tag},u,\pi)$: $s \leftarrow (\pi \cdot u^{-(z_1\cdot\mathsf{tag}+z_3)})^{1/(z_2\cdot(\mathsf{tag}-\mathsf{tag}^*))}$	$\widehat{\mathtt{Ext}}(\widehat{sk},\mathsf{tag},u,\pi)$: Compute $s \leftarrow u^{f(0)}$ using $\widehat{sk}$.

図 2: PR-Ext 安全性を持つ具体的な ABO-XHPS。[7] に基づく $\mathcal{X}_{\mathtt{HoKi}}$ (左) と [4] に基づく $\mathcal{X}_{\mathtt{HaKu}}$ (右)。

$\mathtt{XKG}'(\mathsf{pp},\mathsf{sp})$: $(pk_i,sk_i) \leftarrow \mathtt{XKG}(\mathsf{pp},\mathsf{sp})$ for $i \in [2]$ $PK \leftarrow (pk_1,pk_2)$; $SK \leftarrow (sk_1,sk_2)$ Return (PK,SK).	$\mathtt{Pub}'(PK,\mathsf{tag},w)$: $\pi_i \leftarrow \mathtt{Pub}(pk_i,\mathsf{tag},w)$ for $i \in [2]$ Return $\pi \leftarrow (\pi_1,\pi_2)$.	$\mathtt{Ext}'(SK,\mathsf{tag},u,\pi=(\pi_1,\pi_2))$: $s_i \leftarrow \mathtt{Ext}(sk_i,\mathsf{tag},u,\pi_i)$ for $i \in [2]$ If $s_1 = s_2 \neq \bot$ then return s_1 else return $\bot$.
$\widehat{\mathtt{XKG}}'(\mathsf{pp},\mathsf{tag}^*)$: $(pk_i,\widehat{sk}_i) \leftarrow \widehat{\mathtt{XKG}}(\mathsf{pp},\mathsf{tag}^*)$ for $i \in [2]$ $PK \leftarrow (pk_1,pk_2)$; $\widehat{SK} \leftarrow (\widehat{sk}_1,\widehat{sk}_2)$ Return $(PK,\widehat{SK})$.	$\widehat{\mathtt{Priv}}'(\widehat{SK},u)$: $\pi_i \leftarrow \widehat{\mathtt{Priv}}(\widehat{sk}_i,u)$ for $i \in [2]$ Return $\pi \leftarrow (\pi_1,\pi_2)$.	$\widehat{\mathtt{Ext}}'(\widehat{SK},\mathsf{tag},u,\pi=(\pi_1,\pi_2))$: $s_i \leftarrow \widehat{\mathtt{Ext}}(\widehat{sk}_i,\mathsf{tag},u,\pi_i)$ for $i \in [2]$ If $s_1 = s_2 \neq \bot$ then return s_1 else return $\bot$.

図 3: PR-Ext 安全な ABO-XHPS $\mathcal{X}$ からの CS 安全な ABO-XHPS $\mathcal{X}'$ の構成。

$\mathtt{KG}(1^k)$: $(\mathsf{pp},\mathsf{sp}) \leftarrow \mathtt{SetupR}(1^k)$ $(pk,sk) \leftarrow \mathtt{XKG}(\mathsf{pp},\mathsf{sp})$ $PK \leftarrow (\mathsf{pp},pk)$; $SK \leftarrow (\mathsf{sp},sk)$ Return (PK,SK).	$\mathtt{MSetup}(1^k)$: Return $(\mathsf{pp},\mathsf{sp}) \leftarrow \mathtt{SetupR}(1^k)$.	$\mathtt{MKG}(\mathsf{pp})$: $\mathsf{dummy} \leftarrow \mathcal{T}$ $(pk,\widehat{sk}) \leftarrow \widehat{\mathtt{XKG}}(\mathsf{pp},\mathsf{dummy})$ $SK \leftarrow (\widehat{sk},\mathsf{dummy})$ Return (pk,SK).
$\mathtt{Enc}(PK)$: $w \leftarrow \mathcal{W}$; $(u,s) \leftarrow \mathtt{SampR}(w)$ $K \leftarrow \mathsf{G}(s)$; $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$ $\pi \leftarrow \mathtt{Pub}(pk,\mathsf{tag},w)$; $c \leftarrow (u,\pi)$ Return (c,K).	$\mathtt{MEnc}(\mathbf{pk})$: Parse $\mathbf{pk}$ as $(pk_1,\ldots,pk_n)$. $w \leftarrow \mathcal{W}$; $(u,s) \leftarrow \mathtt{SampR}(w)$ $K \leftarrow \mathsf{G}(s)$; $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$ $\pi_i \leftarrow \mathtt{Pub}(pk_i,\mathsf{tag},w)$ for $i \in [n]$ $\boldsymbol{\pi} \leftarrow (\pi_1,\ldots,\pi_n)$; $c \leftarrow (u,\boldsymbol{\pi})$ Return (c,K).	$\mathtt{MExt}(pk_i,c)$: Parse c as $(u,\boldsymbol{\pi})$. Parse $\boldsymbol{\pi}$ as $(\pi_1,\ldots,\pi_n)$. Return $c_i \leftarrow (u,\pi_i)$.
$\mathtt{Dec}(SK,c)$: Parse c as (u,π).; $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$ If $s = \mathtt{Ext}(sk,\mathsf{tag},u,\pi) \neq \bot$ then return $K \leftarrow \mathsf{G}(s)$ else return $\bot$.	$\mathtt{MDec}(sk_i,c_i)$: Parse c_i as (u,π_i).; $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$ If $\mathsf{tag} \neq \mathsf{dummy}$ and $s = \widehat{\mathtt{Ext}}(\widehat{sk}_i,\mathsf{tag},u,\pi_i) \neq \bot$ then return $K \leftarrow \mathsf{G}(s)$ else return $\bot$.	

図 4: ABO-XHPS に基づく単一受信者用 KEM Γ_1 (左) と複数受信者用 KEM Γ_M (右) (図は n 人の場合)。

$\mathtt{KG}(1^k)$: $g \leftarrow \mathbb{G}$; $a_0,a_1,a_2,x_1,x_2 \leftarrow \mathbb{Z}_p$ $A_i \leftarrow g^{a_i}$ for $i \in \{0,1.2\}$ $X_i \leftarrow g^{x_i}$ for $i \in [2]$ $pk \leftarrow (g,A_0,A_1,A_2,X_1,X_2)$ $sk \leftarrow (a_0,a_1,a_2,x_1,x_2)$ Return (pk,sk).	$\mathtt{Enc}(pk)$: $w \leftarrow \mathbb{Z}_p$; $u \leftarrow g^w$ $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$ $\pi_1 \leftarrow (A_0A_1^{\mathsf{tag}}A_2^{\mathsf{tag}^2})^w$ $\pi_2 \leftarrow (X_1^{\mathsf{tag}}X_2)^w$ $c \leftarrow (u,\pi_1,\pi_2)$; $K \leftarrow H(A_0^w)$ Return (c,K).	$\mathtt{Dec}(sk,c)$: Parse c as (u,π_1,π_2). $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$ Let $f(x) := \sum_{i=0}^2 a_i x^i$ If $u^{f(\mathsf{tag})} = \pi_1$ and $u^{x_1\cdot\mathsf{tag}+x_2} = \pi_2$ then return $K \leftarrow H(u^{a_0})$ else return $\bot$.

図 5: $\mathcal{X}_{\mathtt{HoKi}}$ と $\mathcal{X}_{\mathtt{HaKu}}$ に基づき定理 1 と定理 2 によって得られる新たな CCA 安全性を持つ KEM の例。