鍵更新機能付き検索可能暗号：鍵隔離モデルによる実現

渡邉 洋平[1]　穴田 啓晃[2]　松崎 なつめ[2]

概要：検索可能暗号は暗号化したままキーワードの検索が可能な高機能暗号技術であり，これまでに盛んに研究されてきた．本稿では，松崎ら (SCIS 2017, ISEC2017-5) によって整理された鍵更新可能な公開鍵検索可能暗号 (Key-Updatable Public-key Encryption with Keyword Search: KU-PEKS) の要件に基づき，ある種の KU-PEKS として鍵隔離型 PEKS (Key-Insulated PEKS: KI-PEKS) を定式化し，具体的構成法を提案する．

キーワード：検索可能暗号，鍵隔離暗号，鍵更新

Key-Updatable Public-key Encryption with Keyword Search: The Case of Key-insulated Model

Yohei Watanabe[1]　Hiroaki Anada[2]　Natsume Matsuzaki[2]

Abstract: Publi-key encryption with keyword search (PEKS) enables one to search keywords stored in a server while preserving the confidentiality of the keywords. Recently, Matsuzaki et al. (SCIS 2017, ISEC2017-5) clarified requirements for key-updatable PEKS (KU-PEKS), which is PEKS with key-updating functionality. In this paper, we propose key-insulated PEKS (KI-PEKS) as a kind of realizations of KU-PEKS. Specifically, we formalize a model and security notions of KI-PEKS and propose a concrete construction of KI-PEKS.

Keywords: Public-key encryption with keyword search, key-insulated encryption, key update

1. はじめに

境，大岸，笠原 [15] が 2000 年に，また Boneh と Franklin [5] が 2001 年に，楕円曲線上のペアリングの双線型性を本質的に用い，任意の個人識別情報（ID）を公開鍵として利用可能な暗号方式，ID ベース暗号 (Identity-Based Encryption: IBE) を理論的に実現した．2004 年には Boneh ら [4] が，暗号化したままキーワードの検索が可能な公開鍵暗号方式（検索可能公開鍵暗号，以下，検索可能暗号）を提案する等，ペアリングを数学的構造として利用したいわゆる高機能暗号が盛んに研究されてきた．一方，これらの高機能暗号の実用面では，アメリカ国立標準技術研究所（National Institute of Standards and Technology: NIST）による標準化の動き [11], [12] がある．しかしながら，高機能暗号が普及するためには安全性評価等の課題が未だ存在するとされている [11].

我々は，高機能暗号の上記の課題に関し，公開鍵暗号のユーザ個別に配付される秘密鍵の更新（以下，鍵更新）に着眼する．松崎ら（SCIS2017[16]，ISEC2017-5[17]）は，高機能暗号のプリミティブの中でも検索可能暗号を採り上げ，クラウドに預託した暗号化キーワードのデータベースに対し暗号化クエリで所望の情報を検索する前提で，鍵更新のモデルと要件を検討してきた．要件の詳細については 3 を参照されたい．

現代暗号理論分野において，これまでに鍵更新及び鍵漏洩耐性に関する研究は数多く存在する．代表的なものは，

[1] 電気通信大学 大学院情報理工学研究科
Graduate School of Informatics and Engineering, The University of Electro-Communications
日本学術振興会特別研究員 (PD)
[2] 長崎県立大学　情報システム学部　情報セキュリティ学科
Department of Information Security, University of Nagasaki

鍵を適宜更新することである世代の鍵が漏洩したとしても前の世代には影響を及ぼさないフォワード安全な暗号技術 [6]，秘密鍵が部分的に漏洩した場合にも安全性を保証可能な暗号技術 [8]，また秘密鍵を更新用のものと復号用するものの 2 種類に分け，更新用の鍵を隔離しておくことで復号用の鍵が漏れたとしても一定の安全性を保証する鍵隔離型の暗号技術 [7] などがある．

本稿では，[16], [17] でまとめられている要件に基づき，鍵更新型検索可能暗号の具体的構成を提案する．なお具体的構成については，前述したようなこれまでに研究されてきた鍵更新機能を基に，以下の 1), 2) の 2 つのアプローチで検討を進めており，本稿はそのうちの 2) となる．1) のアプローチについては，[18] を参照のこと．

1) 公開鍵更新モデル：ユーザの秘密鍵更新に伴い，対応する公開鍵も更新するモデルである．公開鍵の定期的な配布と管理が必要となるが，[16], [17] における要件を満たしている．
2) 鍵隔離モデル：ユーザの秘密鍵の更新に際して，対応する公開鍵の更新が不要なモデルである．公開鍵の定期的な配布と管理は不要となるが，暗号文の再暗号化に関する要件を満たしていない．

具体的には，4 節にて本稿で扱う鍵隔離型検索可能暗号 (Key-Insulated Public-key Encryption with Keyword Search: KI-PEKS) のモデル及び安全性を定義し，5 節にてその具体的構成法を提案する．提案方式は，階層型 ID ベース鍵隔離公開鍵暗号 (Hierarchical Key-Insulated IBE) [14] の構成法に基づく．より詳しい構成の方針は 5.1 節を参照されたい．提案する具体的構成法はシンプルかつ標準的な仮定である Symmetric eXternal Diffie-Hellman (SXDH) 仮定の下で安全である．また上記 2) でまとめた通り，提案するモデルは十分な要件を満たしていないが，要件を満たしている [18] に比べ，提案構成法はランダムオラクルを用いることなく安全性を証明可能である．より理想的な鍵隔離モデルを実現するための指針を 6 節にて議論し，7 節にてまとめと今後の課題を述べる．

2. 準備

記法．任意の $p \in \mathbb{N}$ に対し，$\mathbb{Z}_p := \{0, 1, \ldots, p-1\}$，また $\mathbb{Z}_p^\times := \mathbb{Z}_p \setminus \{0\}$ とする．$(y_1, y_2, \ldots, y_m) \leftarrow \mathcal{A}(x_1, x_2, \ldots, x_n)$ と書くとき，アルゴリズム $\mathcal{A}$ に $x_1, x_2, \ldots, x_n$ を入力し，$y_1, y_2, \ldots, y_m$ が出力されたことを表す．$(y_1, y_2, \ldots, y_m) \leftarrow \mathcal{A}^{\mathcal{O}}(x_1, x_2, \ldots, x_n)$ は $\mathcal{A}$ がオラクル $\mathcal{O}$ にアクセスできることを表す．集合 $\mathcal{X}$ から x を一様ランダムに取り出す動作を $x \xleftarrow{\$} \mathcal{X}$ と書く．本稿を通し，セキュリティパラメータとして λ を用いる．$\mathcal{W}$ はセキュリティパラメータ λ によって決まるキーワードの集合である．

2.1 双線形写像

p を素数，$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_T$ を位数 p の巡回群，g_1 と g_2 をそれぞれ $\mathbb{G}_1$ と $\mathbb{G}_2$ の生成元とし，e は効率的に計算可能な双線形写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ とする．双線形写像生成器 $\mathcal{G}$ を，λ を入力し，$(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ を出力する多項式時間アルゴリズムとする．e は以下の性質を持つ: 任意の $u, u' \in \mathbb{G}_1$ 及び $v, v' \in \mathbb{G}_2$ に対し，$e(uu', v) = e(u, v)e(u', v)$ 及び $e(u, vv') = e(u, v)e(u, v')$ が成り立つ．本稿では，非対称ペアリング，すなわち $\mathbb{G}_1 \neq \mathbb{G}_2$ であるものを考え，また $\mathbb{G}_1$ から $\mathbb{G}_2$ への効率的に計算可能な同型写像が知られていないものとする．

2.2 計算量仮定

$\mathcal{A}$ を確率的多項式時間攻撃者とし，$\mathcal{A}$ の DDHi 問題 $(i = 1, 2)$ に対するアドバンテージを以下のように定義する．

$$\mathsf{Adv}^{\mathsf{DDH}i}_{\mathcal{G},\mathcal{A}}(\lambda) := \left| \Pr\left[b' = b \;\middle|\; \begin{array}{l} D := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \leftarrow \mathcal{G}(\lambda), \\ c_1, c_2 \xleftarrow{\$} \mathbb{Z}_p,\ b \xleftarrow{\$} \{0,1\}, \\ \text{if } b = 0 \text{ then } Z := g_i^{c_1 c_2},\ \text{else } Z \xleftarrow{\$} \mathbb{G}_i, \\ b' \leftarrow \mathcal{A}(\lambda, D, g_i^{c_1}, g_i^{c_2}, Z) \end{array} \right] - \frac{1}{2} \right|.$$

定義 1 (DDHi 仮定)．全ての確率的多項式時間攻撃者 $\mathcal{A}$ に対して $\mathsf{Adv}^{\mathsf{DDH}i}_{\mathcal{G},\mathcal{A}}(\lambda) < \epsilon(\lambda)$ ならば，($\mathcal{G}$ に関する) DDHi 仮定が成り立つという．

定義 2 (SXDH 仮定)．十分大きなセキュリティパラメータ λ に対し，双線形群生成器 $\mathcal{G}$ に関して DDH1 仮定及び DDH2 仮定が成り立つならば，$\mathcal{G}$ に関する SXDH 仮定が成り立つという．

3. 鍵更新機能付き検索可能暗号: KU-PEKS

3.1 概念モデルと要件

本節では，松崎ら (SCIS2017[16], ISEC2017-5[17]) により整理された鍵更新機能付き検索可能暗号 (Key-Updatable Public-key Encryption with Keyword Search: KU-PEKS) の概念モデルと要件を概説する．

図 1 に KU-PEKS の概念モデルを図示する．KU-PEKS は送信クライアント，受信クライアント，クラウドの 3 つのエンティティからなる．また，通常の検索可能暗号における (1) 預託フェーズと，(3) 検索フェーズに加え，受信クライアント側で秘密鍵を更新して，対応した変換鍵を生成する (2) 鍵更新フェーズからなる．

(1) 預託フェーズでは，送信クライアントは，受信クライアントの公開鍵を用いて，検索キーワードを含むインデックスを暗号化してクラウドに預託する．
(2) 鍵更新フェーズでは，受信クライアントは，新しい秘密鍵を生成し，生成した鍵と従来持っていた秘密鍵を用いて変換鍵を生成し，クラウドに送信する．受信クライアントは，従来持っていた秘密鍵を削除する．

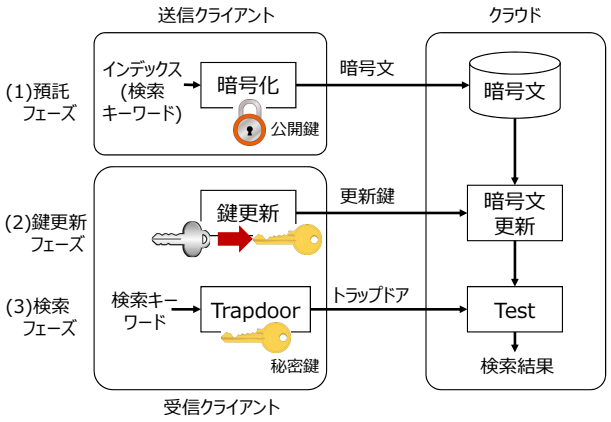

図 1　鍵更新可能な検索可能暗号（KU-PEKS）の概念モデル

一方，クラウドは変換鍵を用いて，預託フェーズで預かった暗号文を変換する．

(3) 検索フェーズでは，受信クライアントは，秘密鍵を用いて検索キーワードを暗号化したトラップドアを求め，クライドに送信する．クラウドは，暗号文とトラップドアを用いて検索してその結果を出力する．

KU-PEKS の要件は以下の 4 点である．

要件 1：受信クライアントの新しい秘密鍵は，古い鍵，および公開の情報から求められないこと．

要件 2：古い鍵は受信クライアントから削除すること．

要件 3：クラウドでは，更新前の古い公開鍵で暗号化された暗号文を対象に，更新後の新しい鍵で生成したトラップドアで検索できること．この要件は，システムの可用性を目的としたものであり，受信クライアントが，保持する新しい鍵だけで，古い暗号文をも対象として検索可能とする．この要件は，古い公開鍵で暗号化された暗号文を，復号することなく，新しい公開鍵で暗号化された暗号文に更新可能とすることで満たされる．

要件 4：クラウドでは，更新後の新しい公開鍵で暗号化された暗号文を対象に，更新前の古い鍵で生成したトラップドアで検索できないこと．この要件は，クラウドの攻撃に対する安全性を目的としたものである．本システムでは，クラウドは正しく検索するが，漏洩の可能性のある古い鍵を入手した悪意のクライアントと結託する場合を考慮する．この場合，更新前の古い公開鍵で暗号化された暗号文を対象とした攻撃は防ぐことは難しいが，本要件により，更新後の新しい公開鍵で暗号化された暗号文を対象とした攻撃を防ぐ．この要件は，新しい公開鍵で暗号化された暗号文は，クラウドにで古い暗号文には変換できないことで満たされる．

3.2　KU-PEKS と KI-PEKS

次節にて提案する鍵隔離型の KU-PEKS は，前節で述べた KU-PEKS の鍵更新フェーズにおいて，秘密鍵の更新に対応する公開鍵を一定とした方法である．これにより，公開鍵の配布とバージョン管理が不要となり，より実用的であるといえる．公開鍵を更新しない代わりに，暗号化時に入力として現在の期間情報も入力することで，その期間に依存した暗号文を生成する．ある期間に依存した暗号文は，同じ期間に依存した秘密鍵から生成されたトラップドアでのみ検索可能となる．ただし，ここで提案するモデル及び具体的方法は，前節で述べた要件 3「古い公開鍵で暗号化された暗号文を，復号することなく，新しい公開鍵で暗号化された暗号文に更新可能とする」については考慮しない方式となっている．すなわち，古い，すなわち前の期間に暗号化されたキーワードを新しい期間の秘密鍵を用いて検索できないということである．要件 3 を満たす方式については，6 節で議論する．

4.　鍵隔離検索可能暗号：KI-PEKS

本節では，鍵隔離型の鍵更新機能を有する検索可能暗号である Key-Insulated Public-key Encryption with Keyword Search (KI-PEKS) を定式化する．

4.1　モデル

KI-PEKS は以下の流れで実行される．$\mathcal{T}$ を期間の集合とする．ユーザははじめに鍵生成を行い，補助鍵 hk，初期秘密鍵 sk_0，公開鍵 pk を得る．pk は公開され，sk_0 はユーザのローカルストレージ，hk は物理的に安全なデバイス (USB メモリ等) に保存され，デバイスはネットワークから隔離されているものとする．平文は別の暗号化方式で暗号化されているものとし，その平文に紐づくキーワードを以下のように暗号化する．キーワード ω は現在の期間 $t \in \mathcal{T}$ と公開鍵 pk でもって暗号化され，その暗号文を $c_{\omega,t}$ と書く．各暗号文は（平文自体の暗号文と共に）サーバに保存されているとする．ユーザは以下の手順で秘密鍵を更新する．各期間 $T \in \mathcal{T}$ のはじめに，hk を用いてその期間の更新情報 δ_T を生成する．ある期間 $T' \in \mathcal{T}$ の秘密鍵 $sk_{T'}$ は δ_T を用いて期間 T の秘密鍵 sk_T に更新される．ここで，更新は定期的に行われる必要はなく，任意の期間の秘密鍵から任意の期間の秘密鍵に更新可能であるものとする．ユーザは以下の流れでキーワード ω を検索する．まず sk_t を用いて ω のトラップドア $td_{\omega,t}$ を生成し，サーバに送信する．サーバは検索アルゴリズムを実行し，その暗号文が t に暗号化された ω の暗号文であれば 1 を，そうでなければ 0 を出力，1 を出力したキーワードの暗号文（とそれに紐づく平文の暗号文）を返す．

ここで，本方式は前節で述べた理想的な要件である「古い期間の暗号文を新しい期間の暗号文に更新可能であること」については考えないモデルとなっていることに留意されたい．より理想的なモデルの KI-PEKS については 6 節

で議論する．

KI-PEKS のモデルを以下のように定義する．KI-PEKS Π は次の 6 つのアルゴリズムからなる．

- $(pk, sk_0, hk) \leftarrow \mathsf{KeyGen}(\lambda)$: 確率的アルゴリズムであり，$\lambda$ を入力し，公開鍵 pk，初期秘密鍵 sk_0，補助鍵 hk を出力する．
- $\delta_T \leftarrow \Delta\text{-}\mathsf{Gen}(pk, hk, T)$: pk，hk，期間 $T \in \mathcal{T}$ を入力し，T における更新情報 δ_T を出力する．
- $sk_T \leftarrow \mathsf{Upd}(pk, sk_{T'}, \delta_T)$: pk，ある期間 $T' \in \mathcal{T}$ の秘密鍵 $sk_{T'}$，δ_T を入力し，期間 T の秘密鍵 sk_T を出力する．
- $td_{\omega,t} \leftarrow \mathsf{TdGen}(pk, sk_{\omega,t}, \omega)$: pk，sk_t，検索したい $omega \in \mathcal{W}$ を入力し，トラップドア $td_{\omega,t}$ を出力する．
- $c_{\omega,t} \leftarrow \mathsf{Enc}(pk, \omega, t)$: 確率的アルゴリズムであり，$pk$，キーワード $\omega \in \mathcal{W}$，$t \in \mathcal{T}$ を入力し，暗号文 $c_{\omega,t}$ を出力する．
- 1 or $0 \leftarrow \mathsf{Test}(pk, td_{\omega,t}, c_{\omega,t'})$: 確定的アルゴリズムであり，$pk$，$td_{\omega,t}$ と $c_{\omega,t'}$ を入力し，1 または 0 を出力する．

上記のモデルでは，以下の正当性を満たすものとする: 全ての $\lambda \in \mathbb{N}$，全ての $(pk, sk_0, hk) \leftarrow \mathsf{KeyGen}(\lambda)$，全ての $\omega \in \mathcal{W}$，全ての $t, t' \in \mathcal{T}$ に対して，$1 \leftarrow \mathsf{Test}(pk, \mathsf{TdGen}(\mathsf{Upd}(pk, sk_{t'}, \Delta\text{-}\mathsf{Gen}(pk, hk, t))\omega), \mathsf{Enc}(pk, \omega, t))$ が成り立つ．

4.2 安全性定義

KI-PEKS では，以下の選択キーワード攻撃と鍵漏洩に対する識別不可能性 (Indistinguishability against key exposure and chosen keyword attacks: IND-KE-CKA)，及び計算量的一貫性 (Computational Consistency) を定義する．

IND-KE-CKA. サーバは正しく検索は行うが，暗号文に内在するキーワードの情報を得ようとする状況を想定する．IND-KE-CKA では通常の PEKS 同様，攻撃者 $\mathcal{A}$ は任意のキーワードに対するトラップドアを得ることが可能であり，その中でトラップドアを得ていないキーワードに関して暗号文から情報が一切漏れないことを保証する．加えて，$\mathcal{A}$ は漏洩した鍵を得ることができる．具体的には，Key-insulated Encryption 同様，補助鍵は漏れていないが多数の秘密鍵が漏れている場合，または秘密鍵は一切漏れていないが補助鍵が漏れている場合に関して，上記の安全性を考える．$\mathcal{A}$ を確率的多項式時間攻撃者とし，IND-KE-CKA ゲームを以下のように定義する．

$\mathsf{Exp}^{\mathsf{CKA}}_{\Pi,\mathcal{A}}(\lambda)$:

$(pk, sk_0, hk) \leftarrow \mathsf{KeyGen}(\lambda)$,

$(\omega_0^*, \omega_1^*, t^*, \mathsf{state}) \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{find}, pk)$,

$b \xleftarrow{\$} \{0,1\}, c^*_{\omega_b^*, t^*} \leftarrow \mathsf{Enc}(pk, \omega_b^*, t^*)$,

$b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{guess}, c^*_{\omega_b^*, T^*}, \mathsf{state})$

If $b' = b$ then output 1,

Else output 0.

ここで，$\mathcal{O}$ は以下の 3 つのオラクル $\{Td, SK, HK\}$ を指す．

Td: $(\omega, t) \in \mathcal{W} \times \mathcal{T}$ を入力に取り，$\mathsf{TdGen}(pk, sk_t, \omega)$ を返す．ここで，sk_t は既に保存されていたものを用いるか，そうでなければ $sk_t \leftarrow \mathsf{Upd}(pk, sk_0, \Delta\text{-}\mathsf{Gen}(pk, hk, t))$ を実行して返し，また保存しておく．

SK: $t \in \mathcal{T}$ を入力に取り，保存されている sk_t を返す．保存されていなければ，Td と同様に新たに sk_t を生成して返し，また保存しておく．

HK: クエリに応じて hk を返す．

$\mathcal{A}$ は上記オラクルに以下の制限の下でアクセス可能である．

(1) Td オラクルに (ω_0^*, t^*) 及び (ω_1^*, t^*) はクエリできない．

(2) SK オラクルに t^* はクエリできない．

(3) HK オラクルにクエリしていない場合のみ，SK オラクルにクエリできる．

(4) SK オラクルに一度もクエリしていない場合のみ HK オラクルにクエリできる．

定義 3 (IND-KE-CKA)**.** 全ての確率的多項式時間攻撃者 $\mathcal{A}$ に対して，$\mathsf{Adv}^{\mathsf{CKA}}_{\Pi,\mathcal{A}}(\lambda) := |\Pr[\mathsf{Exp}^{\mathsf{CKA}}_{\Pi,\mathcal{A}} = 1] - 1/2| < \epsilon(\lambda)$ ならば，*KI-PEKS* Π は IND-KE-CKA 安全であるという．

計算量的一貫性 (Computational Consistency). 正当性が真陰性が起こらないことを保証するのに対し，計算量的一貫性は偽陽性が起こらないことを保証する．より正確には，確率的多項式時間アルゴリズムが偽陽性が起こすようなキーワードと期間を見つける確率が十分小さいことを保証する．具体的には以下のように定義される．$\mathcal{A}$ を確率的多項式時間攻撃者とし，Consistency ゲームを以下のように定義する．

$\mathsf{Exp}^{\mathsf{Cons}}_{\Pi,\mathcal{A}}(\lambda)$:

$(pk, sk_0, hk) \leftarrow \mathsf{KeyGen}(\lambda)$,

$((\omega, t), (\omega', t')) \leftarrow \mathcal{A}(pk)$,

$td_{\omega',t'} \leftarrow \mathsf{TdGen}(pk, \mathsf{Upd}(pk, sk_0, \Delta\text{-}\mathsf{Gen}(pk, hk, t')), \omega')$,

$c_{\omega,t} \leftarrow \mathsf{Enc}(pk, \omega, t)$

If $\mathsf{Test}(pk, td_{\omega',t'}, c_{\omega,t}) \rightarrow 1$ then output 1,

Else output 0.

定義 4 (Computational Consistency)**.** 全ての確率的多項式時間攻撃者 $\mathcal{A}$ に対して，$\mathsf{Adv}^{\mathsf{Cons}}_{\Pi,\mathcal{A}}(\lambda) := \Pr[\mathsf{Exp}^{\mathsf{Cons}}_{\Pi,\mathcal{A}} = 1] < \epsilon(\lambda)$ ならば，*KI-PEKS* Π は Computational Consistency を満たすという．

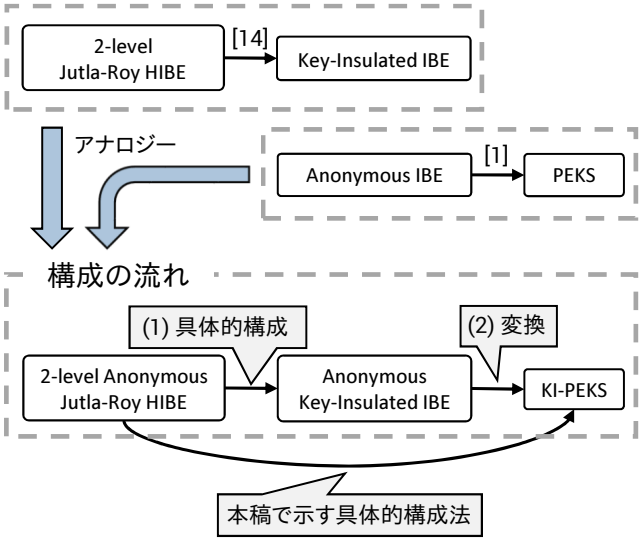

図 2 構成方針の概要

5. 具体的構成法

本節では，SXDH 仮定に基づく KI-PEKS の具体的構成法を提案する．

5.1 構成の方針

構成の方針として，Abdalla ら [1] の Anonymous IBE から PEKS への変換をベースとし，所望の鍵隔離機能を持つ Anonymous IBE から KI-PEKS への変換を考える．Anonymous IBE から PEKS への変換は非常にシンプルであり，うまく Anonymous Key-Insulated IBE を構成できれば，KI-PEKS への変換も成功すると考えられる．従って，変換した結果 KI-PEKS となるような Anonymous Key-insulated IBE の構成を目指す．

[2], [9] の結果から，2-level Hierarchical IBE (HIBE) から弱い安全性を満たす Key-insulated IBE に変換できることは自明であるが，(満たすべき) 強い安全性を満たす Key-Insulated IBE を構成するのは難しい．従って，同様に 2-level Anonymous HIBE を Anonymous Key-insulated IBE へブラックボックス的に変換することは難しいと考えられる．[14] では，Jutla と Roy によって提案された HIBE [10], [13] に代数的な工夫を加えることによって，2-level Jutla-Roy HIBE を基にした (十分な安全性を満たす) Key-insulated IBE の構成に成功している．従って，同様に 2-level Anonymous Jutla-Roy HIBE に代数的な工夫を加え十分な安全性を持つよう調整しながら Anonymous Key-Insulated IBE を実現することを目指す．しかしながら，今回考える (Anonymous) Key-insulated IBE と従来の Key-insulated IBE [9], [14] のモデルは少々異なる点に留意する必要がある．具体的には，今回の方式はマスター鍵の漏洩まで考える必要がある一方で，従来の方式はマスター鍵の漏洩は考慮せず，各 ID に依存した秘密鍵の漏洩のみを考えている点である．今回，KI-PEKS において，hk の漏洩を考慮しているが，これは Abdalla らの変換における Anonymous IBE のマスター鍵に相当する．従って，hk の漏洩を考慮する KI-PEKS に変換するためには，マスター鍵の漏洩をも考慮した Anonymous Key-insulated IBE を考える必要がある．

構成における最も大きな障壁は秘密鍵が漏洩しうる状況で匿名性を保つことである．Anonymous (H)IBE では，匿名性を担保するための必要条件のひとつとして「公開情報による任意の暗号文の ID チェックが不可能である」というものがある．暗号文の ID チェックとは，その暗号文がどの ID で暗号化されたものかをチェックすることを意味する．例えば (匿名性を持たない) 2-level Boneh-Boyen HIBE [3] では，公開パラメータ $mpk := (g, g_1 := g^{\alpha}, g_2, h_1, h_2)$，マスター鍵 $\alpha \in \mathbb{Z}_p$，ID $\mathtt{I}$ $(\in \mathbb{Z}_p)$ の秘密鍵 $sk_{\mathtt{I}} = (d_1, d_2) := (g_2^{\alpha}(g_1^{\mathtt{I}}h_1)^r, g^r)$，$\mathtt{I}$ への暗号文 $c = (c_0, c_1, c_2) := (M \cdot e(g_1, g_2)^s, g^s, (g_1^{\mathtt{I}}h_1)^s)$ であるが，ID $\mathtt{I}'$ に対して $e(g, c_2) = e(c_1, g_1^{\mathtt{I}'}h_1)$ かどうかをチェックすることで ID チェックが可能である．さて，HIBE において子ユーザの秘密鍵を生成する際の親の鍵の再ランダム化は (匿名性を有するかどうかに関わらず) 必須である．匿名性を持たない HIBE では公開パラメータを用いて再ランダム化を行っているが，再ランダム化に用いるパラメータは得てして暗号文の ID チェックも可能なパラメータであるため，Anonymous HIBE を構成したければ再ランダム化用パラメータは公開できない．例えば 2-level Boneh-Boyen HIBE では，$sk_{\mathtt{I}}$ から $\hat{\mathtt{I}}$ の秘密鍵を構成する場合は $sk_{(\mathtt{I},\hat{\mathtt{I}})} := (d_1(g_1^{\mathtt{I}}h_1)^{r_1}(g_1^{\hat{\mathtt{I}}}h_2)^{r_2}, d_2 g^{r_1}, g^{r_2})$ であり，上で示した (ID チェックが可能な) 公開パラメータを用いて再ランダム化していることがわかる．そこで Anonymous HIBE では，通常，秘密鍵を復号パートと再ランダム化パートに分け生成することによってこの条件をクリアしている．すなわち，再ランダム化用パラメータを任意の ID にも適用できるよう公開する (これにより暗号文の ID チェックが可能になっている) のが問題であるため，ある ID にだけ依存させた形で再ランダム化パラメータを用意し，それをその ID の秘密鍵の一部とすることで，匿名性を有しつつ再ランダム化も可能にしている．従って，ターゲット ID の秘密鍵が漏れ得る Anonymous Key-insulated IBE を構成する際には，漏洩情報から匿名性が崩れないよう工夫しなければならない．加えて上で述べた通り，従来の Key-insulated IBE とは異なり，マスター鍵の漏洩にも耐性のある Anonymous Key-insulated IBE でなくてはならない．

上記の議論より，適当な Anonymous Key-Insulated IBE を定式化し，(1) 2-level Anonymous Jutla-Roy HIBE を基にした具体的構成法を提案した上で，(2) Anonymous Key-Insulated IBE から KI-PEKS への一般的変換法の提

案を行うのが実際の構成の流れである．しかしながら，紙面の都合上 Anonymous Key-Insulated IBE の定式化等を記述できないため，次節では，(2) における Anonymous Key-Insulated IBE の各アルゴリズムを (1) を用いてインスタンス化したもの，すなわち 2-level Anonymous Jutla-Roy HIBE を基にした KI-PEKS の具体的構成法を示す (図 2 参照)．

5.2 提案構成法

KI-PEKS II =(KeyGen, Δ-Gen, Upd, Enc, Test) は以下のように構成される．

– KeyGen(λ): $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_1, g_2, e) \leftarrow \mathcal{G}$ を実行する．$\{x_j, y_j, \beta_j, \beta'_j\}_{j=0}^{4} \xleftarrow{\$} \mathbb{Z}_p$，及び $\alpha \xleftarrow{\$} \mathbb{Z}_p^{\times}$ を選び，以下を計算する．

$$z = e(g_1, g_2)^{x_0\alpha - y_0},\quad u_1 := g_1^{x_1\alpha - y_1},\quad w_1 := g_1^{x_2\alpha - y_2},$$
$$h_1 := g_1^{x_3\alpha - y_3},\quad v_1 := g_1^{x_4\alpha - y_4}.$$

また，各 $i \in \{0,1,2,3,4\}$ に対して，$D_{x,i} := g_2^{x_i + \beta_i}$ 及び $D_{y,i} := g_2^{-y_i - \beta'_i}$ を計算し，以下を出力する．

$$pk := (g_1, \hat{g}_1 := g_1^{\alpha}, u_1, w_1, h_1, v_1, z)$$
$$sk_0 := (g_2, \{\beta_i, \beta'_i\}_{i=0}^{4}),$$
$$hk := (g_2, \{D_{x,i}, D_{y,i}\}_{i=0}^{4}).$$

– Δ-Gen(pk, hk, t): $\tilde{r}_1, \tilde{r}_2 \xleftarrow{\$} \mathbb{Z}_p$ を選び，以下を計算する．

$$d_1 := g_2^{\tilde{r}_1}, \qquad d_2 := g_2^{\tilde{r}_2},$$
$$d_{x,1} := (D_{x,2})^{\tilde{r}_1}, \qquad d_{x,2} := (D_{x,2})^{\tilde{r}_2},$$
$$d'_{x,1} := D_{x,0}\left((D_{x,1})^t D_{x,3}\right)^{\tilde{r}_1}, \quad d'_{x,2} := \left((D_{x,1})^t D_{x,3}\right)^{\tilde{r}_2},$$
$$d''_{x,1} := (D_{x,4})^{\tilde{r}_1}, \qquad d''_{x,2} := (D_{x,4})^{\tilde{r}_2},$$
$$d_{y,1} := (D_{y,2})^{\tilde{r}_1}, \qquad d_{y,2} := (D_{y,2})^{\tilde{r}_2},$$
$$d'_{y,1} := D_{y,0}\left((D_{y,1})^t D_{y,3}\right)^{\tilde{r}_1}, \quad d'_{y,2} := \left((D_{y,1})^t D_{y,3}\right)^{\tilde{r}_2},$$
$$d''_{y,1} := (D_{y,4})^{\tilde{r}_1}, \qquad d''_{y,2} := (D_{y,4})^{\tilde{r}_2}.$$

を計算する．すなわち，

$$d_1 := g_2^{\tilde{r}_1}, \qquad d_2 := g_2^{\tilde{r}_2},$$
$$d_{x,1} := g_2^{\tilde{r}_1 x_2 + \tilde{r}_1 \beta_2}, \qquad d_{x,2} := g_2^{\tilde{r}_2 x_2 + \tilde{r}_2 \beta_2},$$
$$d'_{x,1} := g_2^{x_0 + \tilde{r}_1(x_1 t + x_3) + \tilde{r}_1(\beta_1 t + \beta_3)},$$
$$d'_{x,2} := g_2^{\tilde{r}_2(x_1 t + x_3) + \tilde{r}_2(\beta_1 t + \beta_3)},$$
$$d''_{x,1} := g_2^{\tilde{r}_1 x_4 + \tilde{r}_1 \beta_4}, \qquad d''_{x,2} := g_2^{\tilde{r}_2 x_4 + \tilde{r}_2 \beta_4},$$
$$d_{y,1} := g_2^{-\tilde{r}_1 y_2 - \tilde{r}_1 \beta'_2}, \qquad d_{y,2} := g_2^{-\tilde{r}_2 y_2 - \tilde{r}_2 \beta'_2},$$
$$d'_{y,1} := g_2^{-y_0 - \tilde{r}_1(y_1 t + y_3) - \tilde{r}_1(\beta'_1 t + \beta'_3)},$$
$$d'_{y,2} := g_2^{-\tilde{r}_2(y_1 t + y_3) - \tilde{r}_2(\beta'_1 t + \beta'_3)},$$
$$d''_{y,1} := g_2^{-\tilde{r}_1 y_4 - \tilde{r}_1 \beta'_4}, \qquad d''_{y,2} := g_2^{-\tilde{r}_2 y_4 - \tilde{r}_2 \beta'_4}.$$

以下を出力する．

$$\delta_t := (\{d_i, d_{x,i}, d'_{x,i}, d''_{x,i}, d_{y,i}, d'_{y,i}, d''_{y,i}\}_{i=1}^{2}).$$

– Upd($pk, sk_{t'}, \delta_t$): $sk_{t'} = (g_2, \{\beta_j, \beta'_j\}_{j=0}^{4}, \{\tilde{k}_i, \tilde{k}_{x,i}, \tilde{k}'_{x,i}, \tilde{k}''_{x,i}, \tilde{k}_{y,i}, \tilde{k}'_{y,i}, \tilde{k}''_{y,i}\}_{i=1}^{2})$，$\delta_t := (\{d_i, d_{x,i}, d'_{x,i}, d''_{x,i}, d_{y,i}, d'_{y,i}, d''_{y,i}\}_{i=1}^{2})$ とする．$r'_1, r'_2 \xleftarrow{\$} \mathbb{Z}_p$ を選び，以下を計算する．

$$k_1 := d_1 d_2^{r'_1} = g_2^{r_1},$$
$$k_2 := d_2^{r'_2} = g_2^{r_2},$$
$$k_{x,1} := d_{x,1} d_1^{-\beta_2} (d_{x,2} d_2^{-\beta_2})^{r'_1} = g_2^{r_1 x_2},$$
$$k_{x,2} := (d_{x,2} d_2^{-\beta_2})^{r'_2} = g_2^{r_2 x_2},$$
$$k'_{x,1} := d'_{x,1} g_2^{-\beta_0} (d_1)^{-\beta_1 t - \beta_3} (d'_{x,2} (d_2)^{-\beta_1 t - \beta_3})^{r'_1} = g_2^{x_0 + r_1(x_1 t + x_3)},$$
$$k'_{x,2} := (d'_{x,2} (d_2)^{-\beta_1 t - \beta_3})^{r'_2} = g_2^{r_2(x_1 t + x_3)}$$
$$k''_{x,1} := d''_{x,1} d_1^{-\beta_4} (d''_{x,2} d_2^{-\beta_4})^{r'_1} = g_2^{r_1 x_4},$$
$$k''_{x,2} := (d''_{x,2} d_2^{-\beta_4})^{r'_2} = g_2^{r_2 x_4},$$
$$k_{y,1} := d_{y,1} d_1^{\beta'_2} (d_{y,2} d_2^{\beta'_2})^{r'_1} = g_2^{-r_1 y_2},$$
$$k_{y,2} := (d_{y,2} d_2^{\beta'_2})^{r'_2} = g_2^{-r_2 y_2},$$
$$k'_{y,1} := d'_{y,1} g_2^{\beta'_0} (d_1)^{\beta'_1 t + \beta'_3} (d'_{y,2} (d_2)^{\beta'_1 t + \beta'_3})^{r'_1} = g_2^{-y_0 - r_1(y_1 t + y_3)},$$
$$k'_{y,2} := (d'_{y,2} (d_2)^{\beta'_1 t + \beta'_3})^{r'_2} = g_2^{-r_2(y_1 t + y_3)}$$
$$k''_{y,1} := d''_{y,1} d_1^{\beta'_4} (d''_{y,2} d_2^{\beta'_4})^{r'_1} = g_2^{-r_1 y_4},$$
$$k''_{y,2} := (d''_{y,2} d_2^{\beta'_4})^{r'_2} = g_2^{-r_2 y_4}.$$

ここで，$r_1 := \tilde{r}_1 + r'_1 \tilde{r}_2$，$r_2 := r'_2 \tilde{r}_2$ である．以下を出力する．

$$sk_t = (g_2, \{\beta_j, \beta'_j\}_{j=0}^{4}, \{k_i, k_{x,i}, k'_{x,i}, k''_{x,i}, k_{y,i}, k'_{y,i}, k''_{y,i}\}_{i=1}^{2}).$$

– TdGen(pk, sk_t, ω): $sk_t = (g_2, \{\beta_j, \beta'_j\}_{j=0}^{4}, \{k_i, k_{x,i}, k'_{x,i}, k''_{x,i}, k_{y,i}, k'_{y,i}, k''_{y,i}\}_{i=1}^{2})$ とする．$\gamma \xleftarrow{\$} \mathbb{Z}_p$ を選び，以下を計算する．

$$td := k_1 k_2^{\gamma} = g_2^{r},$$
$$td_x := k_{x,1} (k_{x_2})^{\gamma} = g_2^{r x_2},$$
$$td'_x := k'_{x,1} (k''_{x,1})^{\omega} (k'_{x_2} (k''_{x,2})^{\omega})^{\gamma} = g_2^{x_0 + r(x_1 t + x_3 + x_4 \omega)},$$
$$td_y := k_{y,1} (k_{y_2})^{\gamma} = g_2^{-r y_2},$$
$$td'_y := k'_{y,1} (k''_{y,1})^{\omega} (k'_{y_2} (k''_{y,2})^{\omega})^{\gamma} = g_2^{-y_0 - r(y_1 t + y_3 + y_4 \omega)}.$$

ここで，$r := r_1 + \gamma r_2$ である．以下を出力する．

$$td_{\omega,t} := (td, td_x, td'_x, td_y, td'_y).$$

– Enc(pk, ω, t): $s, \mathsf{tag} \xleftarrow{\$} \mathbb{Z}_p$，$R \xleftarrow{\$} \mathbb{G}_T$ に対して以下を計算する．

$$\frac{C_0 e(C,td)}{e(C_x, td_x^{\mathsf{tag}} td'_x) e(C_y, td_y^{\mathsf{tag}} td'_y)}$$
$$= R \cdot e(g_1,g_2)^{(x_0\alpha - y_0)s} \cdot \frac{e(g_1^{s(t(x_1\alpha-y_1)+\mathsf{tag}(x_2\alpha-y_2)+x_3\alpha-y_3+\omega(x_4\alpha-y_4))}, g_2^r)}{e(g_1^{s\alpha}, g_2^{x_2 r\mathsf{tag}+x_0+r(tx_1+x_3+\omega x_4)}) e(g_1^s, g_2^{-y_2 r\mathsf{tag}-y_0-r(ty_1+y_3+\omega y_4)})}$$
$$= R \cdot e(g_1,g_2)^{(x_0\alpha-y_0)s} \frac{1}{e(g_1^{s\alpha}, g_2^{x_0}) e(g_1^s, g_2^{-y_0})} = R.$$

図 3 提案構成法の正当性.

$$C_0 := R \cdot z^s,\ C_x := \hat{g}_1^s,\ C_y := g_1^s,$$
$$C := \left(u_1^t w_1^{\mathsf{tag}} h_1 v_1^{\omega}\right)^s.$$

$c_{\omega,t} := (R, C_0, C_x, C_y, C, \mathsf{tag})$ を出力する.

- $\mathsf{Test}(pk, td_{\omega,t}, c_{\omega,t})$: $td_{\omega,t} := (td, td_x, td'_x, td_y, td'_y)$, $c_{\omega,t} := (R, C_0, C_x, C_y, C, \mathsf{tag})$ とする. 以下が成り立つならば 1 を，そうでなければ 0 を出力する.

$$R = \frac{C_0 e(C,td)}{e(C_x, td_x^{\mathsf{tag}} td'_x) e(C_y, td_y^{\mathsf{tag}} td'_y)}.$$

上記構成法の正当性は図 3 の通り.

定理 1. 上記構成法による *KI-PEKS* II は SXDH 仮定の下で IND-KE-CKA 安全である.

定理 2. 上記構成法による *KI-PEKS* II は SXDH 仮定の下で Computational Consistency を満たす.

紙面の都合上，上記定理の証明は省略する.

6. より理想的な KI-PEKS の実現に向けて

前述したとおり，本稿における KI-PEKS は理想としている KU-PEKS に比べ，「古い暗号文を検索可能である」という要件 3 を満たしていない. 本節では，その要件の実現に向けた方針を議論する. 以下では，古い暗号文の検索ができるよう，再暗号化アルゴリズム ReEnc を考える. 具体的には，Setup において再暗号化鍵 rk も生成されるものとし，サーバが秘密裏に保持しているものとする. サーバは以前の期間に暗号化された暗号文を再暗号化し，任意の期間 T の暗号文を生成する. 具体的には、以下のように Setup を修正，ReEnc を定義する.

– $(pk, sk_0, hk, rk) \leftarrow \mathsf{Setup}(\lambda)$: 確率的アルゴリズムであり，公開鍵 pk，初期秘密鍵 sk_0，補助鍵 hk，再暗号化鍵 rk を出力する.

– $c_{\omega,T} \leftarrow \mathsf{ReEnc}(pk, rk, c_{\omega,T'}, T)$: pk，rk，$c_{\omega,T'}$，T を入力し，期間 T の暗号文 $c_{\omega,T}$ を出力する.

なおその他にも [18] のモデルにより近い修正が考えられるが，本稿では上の修正について議論する. 別修正に関しては付録 8 を参照されたい.

次に，提案した構成法が上記モデルを満たすように修正できるかについて議論する. 暗号文において，t に依存するのは $C = (u_1^t w_1^{\mathsf{tag}} h_1 v_1^{\omega})^s$ である. $(u_1^{t'} w_1^{\mathsf{tag}} h_1 v_1^{\omega})^s = C(u_1^{t'-t})^s$ であるから，期間 t' の暗号文に更新したい場合は rk を用いて $(u_1^{t'-t})^s = g_1^{s(t'-t)(x_1\alpha-y_1)}$ を計算できれば良い. s は暗号文ごとに異なり，そのものを暗号文に含ませることはできない (安全性が崩れてしまう) ため，C_x や C_y のような形でしか暗号文には含むことができない. 従って，rk は $x_1\alpha - y_1$ を $g_1^{x_1\alpha-y_1}$ のような指数部としてではなく，そのものを含んでいる必要がある. しかし，x_1 と y_1 を rk として考えると，証明上うまくいかない. 具体的には，DDH2 問題をシミュレートする際に，そのインスタンスを埋め込む関係上，シミュレータが x_1 及び y_1 そのものの値を知らないまま証明することになる. 提案構成法ではそれらの値を知らなくてもシミュレートが可能であったが，今回のような修正を加えてしまうと証明が通らなくなってしまう.

しかしながら，再暗号化のためには x_1 と y_1 を別々に保持する必要はなく，$x_1\alpha - y_1$ の形で保持しておけば十分である. そこで，$rk := x_1\alpha - y_1$ の場合証明がどうなるかを考えてみる. 単純に攻撃者 (すなわちサーバ) が $x_1\alpha - y_1$ を入手できるとすると，上記のような問題は回避できるが，それとは別にシミュレートが難しい箇所が出てくる. 具体的には，証明中に DDH1 問題のインスタンスのひとつ $g_1^{c_1}$ を g_1^{α} として使用する箇所があり，すなわち α そのものの値をシミュレータが知らないような状況が出てくる. そこで，2 つの乱数 $rk, x_1 \xleftarrow{\$} \mathbb{Z}_p$ をランダムに選び，$y_1 := x_1 c_1 - rk$ としてみると，この場合シミュレータは y_1 がわからないものの，無事 rk を攻撃者に渡すことが可能となる. 問題は hk が $D_{y,1} := -y_1 - \beta'_1$ を，sk_0 (及び全ての $t \in \mathcal{T}$ に対する sk_t) が β'_1 を含む点である. y_1 がわからない以上，$D_{y,1} \xleftarrow{\$} \mathbb{Z}_p$ をランダムに選べば β'_1 がわからず，逆も然りである. つまり $D_{y,1}$ と β'_1 の両方を同時に作ることはできないということだが，攻撃者のタイプを推測することによってうまくこの問題を回避できると考えている. すなわち，HK オラクルにクエリする攻撃者かそうでない攻撃者かをシミュレーションの冒頭で推測し，前者であれば β'_1 を攻撃者に渡す必要がないため $D_{y,i} \xleftarrow{\$} \mathbb{Z}_p$ をランダムに選べばよく，後者であれば β'_1 をランダムに選び，sk_0 (またはすべての sk_t) の要素とすればよい.

従って，次の解決すべき課題はこの修正アプローチが正しいか精査することである.

7. まとめと今後の課題

本稿では，鍵更新機能付き検索可能暗号 (Key-updatable Public-key Encryption with Keyword Search: KU-PEKS) のひとつの実現として鍵隔離型検索可能暗号 (Key-insulated Public-key Encryption with Keyword Search: KI-PEKS) を提案し，標準的な過程である SXDH 仮定の下で安全な構成法を提案した．今後の課題としては，6 節において議論したように，「古い暗号文も検索可能な」KU-PEKS を実現することである．

謝辞 本研究は JSPS 科研費（第一著者においては JP16J10532 及び JP17K12697，第二，第三著者においては JP17K00189）の助成によるものである．

参考文献

[1] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P. and Shi, H.: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions, *Advances in Cryptology – CRYPTO 2005* (Shoup, V., ed.), Lecture Notes in Computer Science, Vol. 3621, Springer Berlin Heidelberg, pp. 205–222 (2005).

[2] Bellare, M. and Palacio, A.: Protecting against key-exposure: strongly key-insulated encryption with optimal threshold, *AAECC*, Vol. 16, No. 6, pp. 379–396 (2006).

[3] Boneh, D. and Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles, *Advances in Cryptology – EUROCRYPT 2004* (Cachin, C. and Camenisch, J., eds.), Vol. 3027, Springer Berlin Heidelberg, pp. 223–238 (2004).

[4] Boneh, D., Di Crescenzo, G., Ostrovsky, R. and Persiano, G.: Public Key Encryption with Keyword Search, *Advances in Cryptology – EUROCRYPT 2004* (Cachin, C. and Camenisch, J., eds.), Lecture Notes in Computer Science, Vol. 3027, Springer Berlin Heidelberg, pp. 506–522 (2004).

[5] Boneh, D. and Franklin, M.: Identity-Based Encryption from the Weil Pairing, *Advances in Cryptology – CRYPTO 2001* (Kilian, J., ed.), Vol. 2139, Springer Berlin Heidelberg, pp. 213–229 (2001).

[6] Canetti, R., Halevi, S. and Katz, J.: Chosen-Ciphertext Security from Identity-Based Encryption, *Advances in Cryptology – EUROCRYPT 2004* (Cachin, C. and Camenisch, J., eds.), Vol. 3027, Springer Berlin Heidelberg, pp. 207–222 (2004).

[7] Dodis, Y., Katz, J., Xu, S. and Yung, M.: Key-Insulated Public Key Cryptosystems, *Advances in Cryptology – EUROCRYPT 2002* (Knudsen, L., ed.), Vol. 2332, Springer Berlin Heidelberg, pp. 65–82 (2002).

[8] Dziembowski, S. and Pietrzak, K.: Leakage-Resilient Cryptography, *FOCS '08*, pp. 293–302 (2008).

[9] Hanaoka, Y., Hanaoka, G., Shikata, J. and Imai, H.: Identity-based hierarchical strongly key-insulated encryption and its application, *Advances in Cryptology – ASIACRYPT 2005* (Roy, B., ed.), LNCS, Vol. 3788, Springer Berlin Heidelberg, pp. 495–514 (2005).

[10] Jutla, C. S. and Roy, A.: Shorter Quasi-Adaptive NIZK Proofs for Linear Subspaces, *Advances in Cryptology – ASIACRYPT 2013* (Sako, K. and Sarkar, P., eds.), Lecture Notes in Computer Science, Vol. 8269, Springer Berlin Heidelberg, pp. 1–20 (2013).

[11] Moody, D., Peralta, R., Perlner, R., Regenscheid, A., Roginsky, A. and Chen, L.: Report on pairing-based cryptography, *Journal of research of the National Institute of Standards and Technology*, Vol. 120, p. 11 (2015).

[12] National Institute of Standards and Technology: Pairing-Based Cryptography (Created January 17, 2017, Updated March 01, 2017). https://beta.csrc.nist.gov/Projects/Pairing-Based-Cryptography.

[13] Ramanna, S. C. and Sarkar, P.: Efficient (Anonymous) Compact HIBE from Standard Assumptions, *Provable Security, ProvSec 2014* (Chow, S., Liu, J., Hui, L. and Yiu, S., eds.), LNCS, Vol. 8782, Springer International Publishing, pp. 243–258 (2014).

[14] Watanabe, Y. and Shikata, J.: Identity-Based Hierarchical Key-Insulated Encryption Without Random Oracles, *Public-Key Cryptography – PKC 2016, Part I* (Cheng, C.-M., Chung, K.-M., Persiano, G. and Yang, B.-Y., eds.), LNCS, Vol. 9614, Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 255–279 (2016).

[15] 境隆一, 大岸聖史 and 笠原正雄: Cryptosystems based on pairing, *Symposium on Cryptography and Information Security (SCIS2000)* (2000).

[16] 松崎なつめ and 穴田啓晃: 検索可能暗号の鍵更新についての調査, *Symposium on Cryptography and Information Security 2017 (SCIS2017)* (2017).

[17] 松崎なつめ, 穴田啓晃 and 渡邉洋平: 鍵更新可能な検索可能暗号の一提案：検索可能代理人再暗号化の適用について, *IEICE Technical Report ISEC2017-5* (2017).

[18] 松崎なつめ, 穴田啓晃 and 渡邉洋平: 鍵更新機能付き検索可能暗号：公開鍵更新モデルによる実現, *Computer Security Symposium 2017* (2017).

8. より理想的な KI-PEKS の別モデル

6 節で述べたモデルに比べ，より [18] のモデルに近いものとして以下が考えられる．Δ-Gen が更新情報 δ_T だけでなく期間 T の暗号文への再暗号化鍵 rk_T も出力し，サーバは rk_T を用いて暗号文を再暗号化し，期間 T の暗号文を生成する．すなわち，再暗号化鍵が期間 T に依存する．

- $(\delta_T, rk_T) \leftarrow \Delta\text{-Gen}(pk, hk, T)$: pk，hk，$T \in \mathcal{T}$ を入力し，δ_T 及び rk_T を出力する．
- $c_{\omega,T} \leftarrow \mathsf{ReEnc}(pk, rk_T, c_{\omega,T'})$: pk，rk_T，$c_{\omega,T'}$ を入力し，$c_{\omega,T}$ を出力する．

5 節の提案構成法がこのモデルの下で安全になるよう修正可能か簡単に議論する．6 節で述べたように，期間 T' の暗号文の再暗号化は $C \cdot (u_1)^{s(T-T')}$ で可能なため，再暗号化鍵として $x_1\alpha - y_1$ が必要となる．再暗号化鍵が期間 T に依存するため，$x_1\alpha - y_1$ が T に依存した形である必要がある．また，T に依存させるからには rk_T を用いて別の期間 t の暗号文に変換できないようにさせたい．しかしながら，紙面の都合上詳細は割愛するが，これらの要求を満たすような rk_T を構成するのは難しい．従って，上記モデルを満たすためには少なくとも異なる構成アプローチが必要だと考えられる．