SCIS 2015 The 32nd Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 20 - 23, 2015
The Institute of Electronics,
Information and Communication Engineers

複数の鍵発行機関が存在可能な関数型暗号に対する失効機能の実現
Revocable-Storage Decentralized Multi-Authority Functional Encryption

土田 光 *† Hikaru Tsuchida
金山 直樹 ‡ Naoki Kanayama
西出 隆志 ‡ Takashi Nishide
岡本 栄司 ‡ Eiji Okamoto
Kwangjo Kim §

あらまし 近年，サーバへの不正アクセスが問題となっている．問題の解決にあたり属性ベース暗号が提案されている．しかし属性ベース暗号は動的な属性変化に対応できない．そこで，ユーザ属性鍵の失効機能を備えた方式が求められる．既存研究として，更新鍵が必要だが Encryptor に失効者情報を意識させずに済む Indirect な失効方式や，更新鍵は不要だが Encryptor が失効者情報を暗号文に規定しなくてはならない Direct な失効方式が提案されている．一方，関数型暗号をベースとした代理人再暗号化による失効方式も提案されている．この方式は条件式の自由度は高いが，鍵発行機関が単一の方式のみ提案されている．本研究では，Indirect/Direct の性質を同時に実現したパッチによる失効機能を有する，複数の鍵発行機関が存在可能な関数型暗号を提案する．また，Indirect の長所と引き換えに，失効者パッチに関する暗号文の蓄積を効率的に軽減できる拡張方式も提案する．

キーワード 関数型暗号, 失効機能, Multi-Authority

1 はじめに

1.1 背景

近年，サーバへの不正アクセスおよび情報漏えいが問題となっている．この問題に対し，有効であるのが属性ベース暗号 [1] である．この暗号方式によって，サーバへの信頼を仮定することなく，データを暗号文の状態でサーバにストアし，暗号方式単体でアクセス制御を実現できる．また，属性ベース暗号を包括する方式として，関数型暗号 [2, 3] が提案されている．

ここで，具体的なケースを考えてみる．たとえば A 社が利用するサーバ上に，「“A 社社員”∧“営業部”」という属性条件が規定された暗号文が存在したとする．通常，この暗号文にアクセスできるのは A 社の営業部に所属するユーザのみである．しかし，退職者や営業部から異動になった社員が，不正に当該属性に関連する鍵を保存していた場合，それらを用いた不正なアクセスを許すこととなる．つまり，前述の暗号方式では動的な属性変化に対応ができない．そこで，暗号方式に鍵失効機能を付与する必要がある．既存研究として，以下の失効方式が存在する．まず，正規ユーザへの更新鍵配布を用いた失効方式 [4, 5]（以下，Indirect な失効方式）が挙げられる．これは更新鍵を要する代わりに，Encryptor に失効者の情報を意識させることなく，失効を実現できる．次に更新鍵を用いない失効方式（以下，Direct な失効方式）が存在する [6]．これは，更新鍵が不要な一方で，Encryptor による暗号文に対する失効者の規定が必要となる．更に Direct かつ複数の鍵発行機関が存在可能な方式 [7] や，Indirect と Direct の 2 つの失効方式を備えた方式も存在する [8, 9]．また，関数型暗号に対し，第三者信頼機関を用いて失効機能を実現する方式も存在する．具体的には，代理人再暗号化サーバを設定することで失効機能を実現する方式や [10]，専用エンティティが秘密鍵の世代を管理することで失効を行う方式 [11] も提案されている．

暗号方式としては，属性管理の観点から，複数の鍵発行機関が存在可能である方が好ましい．失効方式に関しても Indirect/Direct はトレードオフの関係にあり，併用もしくは同時に両者の長所を兼ね備えている方式が望まれる．また，アクセス条件の表現の自由度から，属性ベース暗号よりも関数型暗号の方が優れている．以上より，1. 複数の鍵発行機関が存在可能，2.Indirect かつ Direct な失効方式を備えている，3. 関数型暗号である，といった 3 つの特徴を兼ね備えた方式が必要とされている．

1.2 本研究における貢献

本研究においては，Indirect および Direct の両失効方式の長所を同時に備えた，複数の鍵発行機関が存在可能な関数型暗号方式を提案する．つまり，更新鍵を用いることなく，かつ，Encryptor が失効者情報を意識する必要のない失効機能を，複数の鍵発行機関が存在可能な関数型暗号に付与した方式を提案する．先行研究との特徴比較を表 1 に示す．ここで，[8, 9] はある属性に対し，Indirect もしくは Direct のどちらか一方の失効を実現している (Indirect/Direct) が，提案方式は Indirect と Direct の長所を同時に有する Patch による失効（Indirect&Direct）であることに注意する．また，Encryptor に失効者情報を規定させる代わりに，暗号文に蓄積される失効者の

* 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. Graduate School of System and Information Engineering, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan.
† tsuchida@cipher.risk.tsukuba.ac.jp
‡ 筑波大学 システム情報系 〒 305-8573 茨城県つくば市天王台 1-1-1. Faculty of Engineering, Information and Systems, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan.
§ Computer Science Dep't, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 305-701, Korea.

表 1: 先行研究と提案手法との比較

	鍵発行機関	失効方式	暗号方式
M14[7]	複数 (CA 必要)	Direct	属性ベース暗号 (monotone)
NH09[8]	単一	Indirect/Direct	属性ベース暗号 (monotone)
TSTYK14[10]	単一	代理人再暗号化	関数型暗号 (non-monotone)
提案方式	複数 (CA 不要)	Patch(Indirect&Direct)[1]	関数型暗号 (non-monotone)

パッチを効率的に軽減できる失効方式も提案する．

2 準備

2.1 記法

A が分布であるとき，$y \xleftarrow{\mathsf{R}} A$ は y を A から分布に従い，ランダムに選ぶことを意味する．A が集合ならば，$y \xleftarrow{\mathsf{U}} A$ は y を A から一様に選ぶことを意味する．素位数 q の有限体を $\mathbb{F}_q$ とし，$\mathbb{F}_q \backslash \{0\}$ を $\mathbb{F}_q^\times$ とする．また，$\mathbb{F}_q$ 上のベクトル $(x_1, \ldots, x_n) \in \mathbb{F}_q$ を $\vec{x}$ と表記する．ここで，2 つのベクトル $\vec{x}, \vec{y}$ の内積 $\sum_{i=1}^n x_i v_i$ を $\vec{x} \cdot \vec{y}$ とし，$\mathbb{F}_q^n$ での零ベクトルを $\vec{0}$ と表記する．なお，X^{-1} は行列 X の逆行列を表し，X^T は行列 X の転置行列を意味する．ベクトル空間 $\mathbb{V}$ の要素は $\mathbf{x} \in \mathbb{V}$ と書き表す．また，$\mathbb{B} := (\mathbf{b}_1, \ldots, \mathbf{b}_N)$ および $\mathbb{B}^* := (\mathbf{b}_1^*, \ldots, \mathbf{b}_N^*)$ に対し，$(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \mathbf{b}_i$ と $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \mathbf{b}_i^*$ とそれぞれ書き表すこととする．なお，$\vec{e}_{t,j}$ は $(\overbrace{0 \ldots 0}^{j-1}, 1, \overbrace{0 \ldots 0}^{n_t - j}) \in \mathbb{F}_q^{n_t}$ $(j = 1, \ldots, n_t)$ を意味する．また，$GL(n, \mathbb{F}_q)$ は次元 n の $\mathbb{F}_q$ 上の一般線形群を指す．

2.2 他の要素技術

失効者の規定には Subset Cover Framework における Complete Subset method（CS 法）を用いる [12]．ここで，Subset Cover Framework とは完全二分木を用いたもので，葉ノードに全ユーザを割り当てる．このとき，正規ユーザを Subset によって規定することで，間接的に失効ユーザを区別できる．これが CS 法である．本方式では **CS**.**Setup**, **CS**.**Cover** を用いている．詳細は [5, 12] を参照されたい．また，アクセス条件の規定には Span Program を用いる．ここで Span Program とはアクセス条件を行列に変換し扱うというものである．

今回，Subset Cover Framework は紙面の都合により省略する．なお，Span Program は [3] に準ずる．

2.3 Dual Pairing Vector Spaces(DPVS)

定義 1 (対称ペアリング群). 対称ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, \boldsymbol{e})$ はそれぞれ，素数 q（後述の $\mathbb{G}, \mathbb{G}_T$ の位数），加法的巡回群 $\mathbb{G}$，乗法的巡回群 $\mathbb{G}_T$，$G \neq 0 \in \mathbb{G}$，多項式時間で計算可能な非退化性を持つ双線形写像 $\boldsymbol{e}$: $\mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ から構成される．セキュリティパラメータ 1^λ を入力に取り上述の対称ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, \boldsymbol{e})$ を出力するアルゴリズムを $\mathcal{G}_{\mathsf{bpg}}(1^\lambda)$ と表記する．

[1] ただし，提案方式はユーザの新規追加や失効ユーザの復帰ができない．このため，セットアップ時にユーザ木を十分に大きくする必要がある．また，クラウドサーバや Encryptor は暗号文生成および失効者情報更新時，最新パッチを各鍵発行機関から取得する必要がある．更に暗号文の蓄積や復号時の処理の観点から高いコストを要する．

定義 2 (Dual Pairing Vector Spaces(DPVS)). *DPVS* は $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, \boldsymbol{e})$ はそれぞれ，素位数 q，N 次ベクトル空間 $\mathbb{V} := \overbrace{\mathbb{G} \times \ldots \times \mathbb{G}}^{N}$，巡回群 $\mathbb{G}_T$，$\mathbb{V}$ の標準基底 $\mathbb{A} := (\mathbf{a}_1, \ldots, \mathbf{a}_N), \mathbf{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$，ペアリング演算 $\boldsymbol{e}$: $\mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$ から成る．ここで，$\mathbf{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ と $\mathbf{y} := (H_1, \ldots, H_N) \in \mathbb{V}$ としたとき，$\boldsymbol{e}(\mathbf{x}, \mathbf{y}) := \prod_{i=1}^N \boldsymbol{e}(G_i, H_i) \in \mathbb{G}_T$ と定義される．更に $\phi_{i,j}(\mathbf{a}_j) = \mathbf{a}_i$ かつ $\phi_{i,j}(\mathbf{a}_k) = \mathbf{0} (k \neq j)$ となる写像 $\phi_{i,j}$ を用意する．このとき，$X := (\chi_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N \times N}$ およびベクトル $\mathbf{v} \in \mathbb{V}$ に対し，$X(\mathbf{v}) := \sum_{i=1,j=1}^{N,N} \chi_{i,j} \phi_{i,j}(\mathbf{v})$ と定義する．同様に $(\vartheta_{i,j}) := (X^{-1})^T$ に対し，$(X^{-1})^T(\mathbf{v})$ $:= \sum_{i=1,j=1}^{N,N} \vartheta_{i,j} \phi_{i,j}(\mathbf{v})$ と定義する．また，$\mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N)$ はセキュリティパラメータ λ と $\mathbb{V}$ の次数 N を引数に取り，$\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, \boldsymbol{e})$ を出力する．

2.4 安全性仮定

定義 3 (DLIN:Decisional Linear 仮定). *DLIN* 問題とは，$(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta \xi G, \sigma \kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$ が与えられた状態で，$\beta \in \{0, 1\}$ を推測することである．なお，各パラメータは以下にして与えられる．

$\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$:

$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, \boldsymbol{e}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$,

$\kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Y_0 := (\delta + \sigma) G, Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}$,

return $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta \xi G, \sigma \kappa G, Y_\beta)$,

ただし，$\beta \xleftarrow{\mathsf{U}} \{0, 1\}$ とする．確率的アルゴリズム $\mathcal{E}$ に対し，*DLIN* 問題を解くにあたっての $\mathcal{E}$ のアドバンテージを次のように定義する．: $\mathsf{Adv}_\varepsilon^{\mathsf{DLIN}}(\lambda) := |\Pr[\mathcal{E}(1^\lambda, \varrho) \to 1 \| \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)] - \Pr[\mathcal{E}(1^\lambda, \varrho) \to 1 \| \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)]|$.

ここで，任意の確率的多項式時間での計算能力を持つ攻撃者 $\mathcal{E}$ に対し，$\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ がセキュリティパラメータ λ において無視できるほど小さい *(negligible)* とき，*DLIN* 仮定が成り立つ．

3 複数の鍵発行機関が存在可能かつ失効機能を備えた関数型暗号

本節では，複数の鍵発行機関が存在可能かつ失効機能を備えた関数型暗号 (Revocable-Storage Decentralized Multi-Authority Functional Encryption，RS-DMA-FE) のシステムモデルおよび安全性を定義する．

3.1 システムモデル

定義 4 (RS-DMA-FE). *RS-DMA-FE* は以下の *8* つのアルゴリズムで構成される．

1. $\mathsf{GSetup}(1^\lambda)$
   $\mathsf{GSetup}(1^\lambda)$ を実行し，gparam を出力・公開する．

2. ASetup(gparam, $t, n_t^{(F)}, N_{max,t}$)
属性管理局 t（以下，AA_t）が実行する．ただし，$1 \leqq t \leqq d$ である．また，$n_t^{(F)}$ は管理する属性ベクトルの次数，$N_{max,t}$ は AA_t が管理する属性を有するユーザの総数（今回，AA_t は単純化のために，一つの属性のみ を管理している．複数の属性を管理する場合は，その属性と対応するユーザ総数をそれぞれ入力する．つまり $\{N_{max,t}\}$ を入力）．実行後，AA_t の属性用公開鍵 apk_t，失効用公開鍵（失効者パッチ）$rpk_{t,r\ell_{t,k}}$ (k はバージョンを意味する．セットアップ時は $k=1$，以降，更新の度に $k+1$ となる)，AA_t の属性用秘密鍵 ask_t，失効用秘密鍵 rsk_t を出力する．出力後，$apk_t, rpk_{t,r\ell_{t,k}}$ は公開し，ask_t, rsk_t はストアする．

3. RLUpdate($t, rpk_{t,r\ell_{t,k}}, rsk_t, r\ell_{t,k+1}$)
AA_t が実行する．$r\ell_{t,k+1}$ は最新の失効者リストを意味する．実行後，AA_t の最新の失効用公開鍵 $rpk_{t,r\ell_{t,k+1}}$ を出力する．出力後，$rpk_{t,r\ell_{t,k+1}}$ は公開する．

4. KeyGen(gparam, $t, ask_t, rsk_t, gid, \vec{x}_t$)
AA_t が大域ユーザ識別子 gid に対し，属性ベクトル $\vec{x}_t$ に関連するユーザ属性鍵 $uak_{gid,(t,\vec{x}_t}$ および局所ユーザラベル L_t に関連するユーザ ID 鍵 uik_{gid,L_t} を発行する際に，実行する．実行後，ユーザ鍵 $usk_{gid,(t,\vec{x}_t),L_t} = (uak_{gid,(t,\vec{x}_t)}, uik_{gid,L_t})$ を出力し，AA_t はユーザ gid に $usk_{gid,(t,\vec{x}_t),L_t}$ を与える．

5. Enc($\{apk_t, rpk_{t,r\ell_{t,k_i}}\}, m, \mathbb{S}$)
平文 $m \in \mathbb{G}_T$ をアクセス構造 $\mathbb{S}$ を伴って，関連する AA_t の公開鍵 $\{apk_t, rpk_{t,r\ell_{t,k_i}}\}$ によって暗号化する際に，実行する．実行後，暗号文 $ct_{\mathbb{S},\{r\ell_{t,k_i}\}}$ が出力される．(k_i は属性カテゴリ i に関する失効者パッチの最新バージョン番号である．新規に暗号文を生成した場合，失効者パッチに関する暗号文は最新バージョンに関するもののみが生成されることに注意する．)

6. Delegate($ct_{\mathbb{S},\{rl_{t,k}\}}, \{rpk_{t,rl_{t,k+1}}\}$)
暗号文を更新する際に実行．実行後，$ct_{\mathbb{S},\{r\ell'_{t,k+1}\}}$ を出力する．

7. Rand($ct_{\mathbb{S},\{r\ell_{t,k}\}}$)
暗号文を再ランダム化する際に実行．実行後，$ct'_{\mathbb{S},\{r\ell_{t,k}\}}$ を出力する．

8. Dec(gparam, $\{apk_t, rpk_{t,r\ell_{t,k}}\}, usk_{gid,(t,\vec{x}_t),L_t}, ct_{\mathbb{S},\{r\ell_{t,k}\}}$)
暗号文 $ct_{\mathbb{S},\{r\ell_{t,k}\}}$ をユーザ gid が復号する際に実行する．実行後，m もしくは空シンボル $\perp$ を出力する．

RS-DMA-FE は，全てのセキュリティパラメータ λ，属性集合 $\Gamma := \{(t,\vec{x})\}$，大域ユーザ識別子 gid，平文 m，アクセス構造 $\mathbb{S}$ に対し，もしも以下が成り立つなら，$m =$ Dec(gparam,$\{apk_t, rpk_{t,r\ell_{t,k}}\}, usk_{gid,(t,\vec{x}_t),L_t}, ct_{\mathbb{S},\{r\ell_t,k\}}$) が圧倒的確率で成立する．もしも以下が成り立たないなら，無視できる確率でしか上式は成立しない．

$$\begin{aligned}
&\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda),\\
&(apk_t, rpk_{t,r\ell_{t,k}}, ask_t, rsk_t)\\
&\quad \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t, n_t^{(F)}, N_{max,t}),\\
&(usk_{gid,(t,\vec{x}_t),L_t})\\
&\quad \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{gparam}, t, ask_t, rsk_t, gid, \vec{x}_t),\\
&(ct_{\mathbb{S},\{r\ell_{t,k_i}\}}) \xleftarrow{\mathsf{R}} \mathsf{Enc}(\{apk_t, rpk_{t,r\ell_{t,k_i}}\}, m, \mathbb{S}),\\
&(ct_{\mathbb{S},\{r\ell'_{t,k+1}\}}) \xleftarrow{\mathsf{R}} \mathsf{Delegate}(ct_{\mathbb{S},\{r\ell_t\}}, \{rpk_{t,r\ell_{t,k}}\}),\\
&(ct'_{\mathbb{S},\{r\ell_t,k\}}) \xleftarrow{\mathsf{R}} \mathsf{Rand}(ct_{\mathbb{S},\{r\ell_{t,k}\}})\ where\ \Gamma \in \mathbb{S}
\end{aligned}$$

なお，S を鍵発行局の集合としたとき，各属性は必ず一つの発行局に割り当てられる．あるいは属性は $(t,\vec{x})$ の形を取る．

3.2 安全性要件

本小節では，RS-DMA-FE 方式の暗号文に対し，適応的平文秘匿性 (Adaptively Payload Hiding aginst Chosen Plaintext Attack, PH) を定義する．

定義 5 (適応的平文秘匿性)．*RS-DMA-FE* 方式が選択平文攻撃対し，暗号文の適応的平文秘匿性（PH）を持つとは，任意の多項式時間攻撃者 $\mathcal{A}$ に対し，任意のセキュリティパラメータ λ において下記のゲームに関して，$\mathsf{Adv}_{\mathcal{A}}^{RS-DMA-FE,PH}(\lambda) := |\Pr[b' = b] - 1/2|$ が $negligible$ な値であることを言う．

Setup
チャレンジャー $\mathcal{C}$ は $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$ を $\mathcal{A}$ に与える．各鍵発行局 $AA_t \in S$ に対し，$\mathcal{C}$ は $(ask_t, rsk_t, apk_t, rpk_{t,r\ell_{t,k}}) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t, n_t^{(F)}, N_{max,t})$ を実行する．そして，$\{apk_t, rpk_{t,r\ell_{t,k}}\}_{t\in S}$ を $\mathcal{A}$ に与える．

Phase1
$\mathcal{A}$ は *Adaptively* に，多項式に比例する個数のユーザ鍵を要求する．$\mathcal{A}$ は $\mathcal{C}$ もしくはオラクル $\mathsf{KeyGen}(\mathsf{gparam}, t, ask_t, rsk_t, gid, \vec{x}_t)$ に $(gid, t, \vec{x}_t)$ を渡し，$usk_{gid,(t,\vec{x}_t),L_t} = (uak_{gid,(t,\vec{x}_t)}, uik_{gid,L_t})$ を得る．

Challenge
ここで $\Gamma_i := \{(t,\vec{x})\}(i = 1,\ldots,\nu)$ が gid_i に関して KeyGen オラクルに要求されたとする．$\mathcal{A}$ はアクセス構造 $\mathbb{S}^*$ と失効者リスト $\{RL_{t,k}\}_{t\in S}$ を出力する．更にメッセージ $M_0^*, M_1^* \in \mathcal{M}$(メッセージ長は等しい) と共に，$(\mathbb{S}^*, \{RL_{t,k}\}_{t\in S}, M_0^*, M_1^*)$ を $\mathcal{C}$ に渡す．ただし，以下の条件が成り立つこと．

$$(\Gamma_i \notin \mathbb{S}^*) \vee (gid_i \in \{RL_{t,k}\})$$

$\mathcal{C}$ はランダムなビット $b \xleftarrow{\mathsf{U}} \{0,1\}$ を選び，$ct_{\mathbb{S},\{RL_t,k\}}^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\{apk_t, rpk_{t,RL_{t,k}}\}, M_b^*, \mathbb{S}^*)$ を $\mathcal{A}$ に与える．

Phase2
$\mathcal{A}$ は続けてユーザ鍵を $\mathcal{C}$ に要求する．ただし，前述の条件を満たした鍵のみ $\mathcal{C}$ より与えられる．

Guess
$\mathcal{A}$ は b を推測し，b' を出力する．

4 提案方式

4.1 RS-DMA-FE

本方式の構成の概要について述べる．まず，GSetup により各エンティティに大域公開パラメータを渡す．以下，

ベースとなる暗号 DMA-FE に関連する操作時は $mode = F$，失効機能 Patch に関連する操作時は $mode = P$ とする．添え字 F, P もこのように対応があると考える．次に ASetup により，各 AA_t が鍵生成に必要なパラメータ（双対基底含む），ユーザを管理する完全二分木および失効者パッチ $rpk_{t,r\ell_{t,k}}$ を生成する（$\mathsf{CP}_{t,r\ell_{t,1}}$ の作り方は RLUpdate を参照されたい．セットアップ時なので，失効者は存在しない）．このとき，ψ_t は gid を引数に取り，対象ユーザが割り当てられた葉ノードのラベル $L_{gid,t}$ を出力する関数である．また，$\varsigma_{L_{gid,t}}$ はユーザ gid が割り当てられた葉ノードに対して選んだ，葉ノードごとに異なる値である．ここで Encryptor は暗号文を生成する際，$rpk_{t,r\ell_{t,k}}$ からは対応する属性カテゴリやバージョン情報 k さえ知ることができれば十分であり，失効者情報を意識する必要はない (*1)．そして KeyGen により，各ユーザに鍵を生成・配布する．このとき，$\Phi_t : \{(*,0),(0,1),(1,1),\ldots,(0,h_t),(1,h_t)\} \to \{3,\ldots,n_t^{(P)}-1\}$ である．たとえば $(*,0)$ は根ノードを意味し，(h,c) は深さ h，$c \in \{0,1\}$ となり，0 は左の枝，1 は右の枝を意味する．ただし，鍵にユーザの完全二分木における割り当てに関する情報は含まれない (*2)．一方，Encryptor は各種公開パラメータを用いて Enc によって，平文 m を暗号化する．このとき，平文に関する暗号文およびアクセス条件に関する暗号文 $\mathbf{ct}_{\mathbb{S}}$ だけでなく，失効者パッチ $rpk_{t,r\ell_{t,k_i}}$ から最新の失効者パッチに関する暗号文 $\{\mathbf{c}_{P,i,k_i,z}\}$ も生成する．生成された暗号文 $ct_{\mathbb{S},\{rl_{t,k_i}\}}$ はクラウドサーバ (以下，CS) にストアされる．その後，属性条件を満たし，かつ該当する属性鍵が失効されていない Decryptor は，暗号文を CS から取得し，Dec によって復号する．なお，失効者パッチの更新には RLUpdate が用いられる．これによって生成・公開された最新の失効者パッチを，ストア済みの暗号文に対し CS が Delegate(i_D は失効者情報を更新する対象カテゴリーを意味する),Rand によって適用する．これより，既存の暗号文に対しても失効者情報が更新され，失効されたユーザは以前にアクセスできたデータであってもアクセス不可となる．したがって，動的な属性変化に対してもアクセス制御が実現できたことになる．

ここで本方式では，(*1)(*2) より Indirect の長所が実現でき，失効にあたってもユーザへの更新鍵発行が無いため，Direct の長所も兼ね備えている．また，[3] をベースの暗号方式として用いているため，複数の鍵発行機関が存在可能な関数型暗号でもある．

詳細を図 1 に示す．

4.2 提案方式の拡張

前述の提案方式では，失効者パッチ $rpk_{r\ell_{t,k}}$ とそれによって生成された失効者パッチに関する暗号文 $\{\mathbf{c}_{P,i,j,z}\}$ が蓄積していき，効率の面で問題がある．そこで，失効者パッチに関する暗号文の構造をそれぞれ以下にする．(ただし，失効者ゼロのときであっても $\vec{x}_{P,i} \cdot \vec{v}_{P,i,j,z} \neq 0$ が成り立つように注意する．そのため，$v^{(P)}_{i,j,z,\Phi_t(*,0)} = 0$ とする．)

$$\mathbf{c}_{P,i,j,z}$$
$$= (\overbrace{s_{P,i,j}\vec{v}_{P,i,j,z}}^{n_t^{(P)}}, \overbrace{s'_{P,i,j}\vec{v}_{P,i,j,z}}^{n_t^{(P)}}, \overbrace{0^{2n_t^{(P)}}}^{2n_t^{(P)}}, \overbrace{0^{n_t^{(P)}}}^{n_t^{(P)}}, \overbrace{-w_{i,j}\vec{v}_{P,i,j,z}}^{n_t^{(P)}},$$
$$\overbrace{s_{P,i,j}\eta^{[1]}_{t,j,z} + s'_{P,i,j}\eta^{[2]}_{t,j,z} + (-w_{i,j})\eta^{[3]}_{t,j,z} + \eta_{P,i,j,z}}^{1})_{\mathbb{B}_{P,t}}$$

これにより，Subset によって正規のユーザを規定することで間接的に失効ユーザを規定するのではなく，失効ユーザを Subset により直接規定する．これにより，前述の提案方式よりも，メモリ容量と復号時の効率の良い失効が実現できる．以降，この失効方式を Negative-CS 法と呼称する．

ただし，Negative-CS 法を用いた場合，Indirect の利点が失われる（実質的に Direct と等しくなる）．これは [3] の条件式 NOT に関する属性カテゴリに対応する暗号文のように，復号時に $\vec{v}_{P,i,z}$ を知る必要がある．つまり，各 AA_t は $\vec{v}_{P,i,z}$ を公開するか，あるいは $\hat{\mathbb{B}}^P_t := (\mathbf{b}^{(P)}_{t,1},\ldots,\mathbf{b}^{(P)}_{t,2n_t^{(P)}},\mathbf{b}^{(P)}_{t,5n_t^{(P)}+1},\ldots,\mathbf{b}^{(P)}_{t,6n_t^{(P)}+1})$ として，そもそも Encryptor 自身に失効者を暗号文に規定させるかの，いずれかを行う必要が生じる．よって，Encryptor は失効者情報を意識しなくてはならず，結果として Direct と等しくなる．

5 安全性証明

定理 1 (RS-DMA-FE の安全性)．提案方式 *RS-DMA-FE* は，ランダムオラクルモデルにて *DLIN* 仮定の下で，選択的平文攻撃に対し，適応的平文秘匿性を有する．

任意の多項式時間攻撃者 $\mathcal{A}$ に対し，任意のセキュリティパラメータ λ において，実行時に $\mathcal{A}$ 同様に働く確率的アルゴリズム $\mathcal{E}_1,\mathcal{E}_2,\mathcal{E}_3$ が存在する．

このとき，以下の式が成り立つ．

$$\mathsf{Adv}^{RS-DMA-FE,PH}_{\mathcal{A}}(\lambda)$$
$$\leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=1}^{\nu}(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2,h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3,h}}(\lambda)) + \varepsilon$$

ここで，$\mathcal{E}_{2,h}(\cdot) := \mathcal{E}_2(h,\cdot), \mathcal{E}_{3,h}(\cdot) := \mathcal{E}_3(h,\cdot)$,$\nu$ はランダムオラクル H に対するクエリ最大回数とする．また，$\varepsilon := ((2d+10)\nu + 2d + 5)/q$ である．

上記の定理の証明は，紙面の都合上，省略する．証明の大部分は [3] と一致する．しかし，[5] のように攻撃者は 2 種類存在することに注意する．このために，[3] と異なり，暗号文の real part のうち $n_t^{(mode)}+1$ から $2n_t^{(mode)}$ が変化している．それに伴い，証明中の pre-semi CT における hidden part も変化し，[3] の Lemma21 も詳細が異なる．これにより，key query の restriction の問題が解消され，攻撃者からは pre-semi CT と semi-func CT との区別が不可能となる．

6 まとめと今後の課題

本稿では，複数の鍵発行機関が存在可能な関数型暗号を提案した．今後は，インデクシング法 [13] を用いてパラメータのサイズを削減したい．

謝辞

本研究の一部は JSPS 科研費 26330151, 24500084 と公益財団法人倉田記念日立科学技術財団 倉田奨励金の助成を受けたものです．また，本研究の一部は JSPS A3 Foresight Program によって支援されています．

参考文献

[1] A. B. Lewko“Functional Encryption: New Proof Techniques and Advancing Capabilities,” PhD thesis, The University of Texas, 2012.

1. $\mathsf{GSetup}(1^\lambda)$:

$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, \boldsymbol{e}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\ H : \{0,1\}^* \to \mathbb{G},$

$G_0 := H(0^\lambda),\ G_1 := H(0^{\lambda-1}, 1),\ g_T := \boldsymbol{e}(G_0, G_1),$ return $\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, H)$.

2. $\mathsf{ASetup}(\mathsf{gparam}, t, n_t^{(F)}, N_{max,t} = 2^{h_t}(n_t^{(P)} = 4 + 2\log_2 N_{max,t}))$:

$for\ mode = F,\ P : \mathsf{param}_{\mathbb{V}_t^{(mode)}} := (q, \mathbb{V}_t^{(mode)}, \mathbb{G}_T, \mathbb{A}_t^{(mode)}, \boldsymbol{e}) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 6n_t^{(mode)} + 1, \mathsf{param}_{\mathbb{G}}),$

$X_t^{(mode)} \xleftarrow{\mathsf{U}} GL(6n_t^{(mode)} + 1,\ \mathbb{F}_q),\ for\ i = 1,\ \ldots,\ 6n_t^{(mode)} + 1,\ \mathbf{b}_{t,i}^{(mode)} := X_t^{(mode)}((0^{i-1}, G_0, 0^{6n_t^{(mode)}+1-i}))$

$(DMA - FE : mode = F)\ \hat{\mathbb{B}}_t^{(F)} := (\mathbf{b}_{t,1}^{(F)},\ \ldots,\ \mathbf{b}_{t,2n_t^{(F)}}^{(F)},\ \mathbf{b}_{t,5n_t^{(F)}+1}^{(F)},\ \ldots,\ \mathbf{b}_{t,6n_t^{(F)}+1}^{(F)}),$

$ask_t := X_t^{(F)}, apk_t := (\mathsf{param}_{\mathbb{V}_t^{(F)}}, \hat{\mathbb{B}}_t^{(F)}),$ return (ask_t, apk_t).

$(Patch : mode = P)\ \mathbf{CS.Setup}(N_{max,t}),\ \hat{\mathbb{B}}_t^{(P)} := (\mathbf{b}_{t,1}^{(P)},\ \mathbf{b}_{t,n_t^{(P)}+1}^{(P)},\ \mathbf{b}_{t,5n_t^{(P)}+1}^{(P)},\ \mathbf{b}_{t,6n_t^{(P)}+1}^{(P)}),$

$rsk_t := (X_t^{(P)},\ \psi_t),\ rpk_{t,r\ell_{t,1}} := (\mathsf{param}_{\mathbb{V}_t^{(P)}}, \hat{\mathbb{B}}_t^{(P)}, \mathsf{CP}_{t,r\ell_{t,1}} = \{cp_{t,1,j}^{[1]}, cp_{t,1,j}^{[2]}, cp_{t,1,j}^{[3]}\}_{j=1}^{m_1}),$ return $(rsk_t, rpk_{t,r\ell_{t,1}})$.

3. $\mathsf{RLUpdate}(t, rpk_{t,r\ell_{t,k}}, rsk_t, r\ell_{t,k+1})$:

$\mathbf{CS.Cover}(\mathcal{BT}_t, r\ell_{t,k+1}),$

$for\ space = 1,2,3 : d, d_a, r_{t,k+1,j,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^* s.t. d_0 + \ldots + d_{|L_{i,t,j}|} = d, \eta_{t,k+1,j}^{[space]} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$cp_{t,k+1,j}^{[space]} = (\overbrace{\vec{v}_{t,k+1,j}^{(P,1)}}^{n_t^{(P)}}, \overbrace{\vec{v}_{t,k+1,j}^{(P,2)}}^{n_t^{(P)}}, \overbrace{0^{3n_t^{(P)}}}^{3n_t^{(P)}}, \overbrace{\vec{v}_{t,k+1,j}^{(P,3)}}^{n_t^{(P)}}, \overbrace{\eta_{t,k+1,j}^{[space]}}^{1})_{\mathbb{B}_t^{(P)}},\ \vec{v}_{t,k+1,j}^{(P,space')} := (v_{t,k+1,j,1}^{(P,space')}, \ldots, v_{t,k+1,j,n_t^{(P)}}^{(P,space')})$

$1 \leqq i \leqq n_t^{(P)}$:

$$v_{t,k+1,j,i}^{(P,space')} = \begin{cases} v_{t,k+1,j,i}^{(P)} & (space = space') \\ 0 & (else) \end{cases}, \quad v_{t,k+1,j,i}^{(P)} = \begin{cases} d & (i = 2) \\ -d_a & (i = \Phi_t(L_{i,j,t}[a], a); 0 \leqq a \leqq |L_{i,j,t}|) \\ r_{t,k+1,j,i} & (i = n_t^{(P)}) \\ 0 & (else) \end{cases}$$

return $rpk_{t,r\ell_{t,k+1}} := (\mathsf{param}_{\mathbb{V}_t^{(P)}}, \hat{\mathbb{B}}_t^{(P)}, \mathsf{CP}_{t,r\ell_{t,k+1}} = \{cp_{t,k+1,j}^{[1]}, cp_{t,k+1,j}^{[2]}, cp_{t,k+1,j}^{[3]}\}_{j=1}^{m_{k+1}})$

4. $\mathsf{KeyGen}(\mathsf{gparam}, t, ask_t, rsk_t, gid, \vec{x}_t^{(F)} := (x_{t,1}^{(F)}, \ldots, x_{t,n_t^{(F)}}^{(F)}) \in \mathbb{F}_q^{n_t^{(P)}} \setminus \{\vec{0}\})$:

$\varsigma_{L_{gid,t}} \in \mathbb{F}_q^*, G_{gid}(= \delta G_1) := H(gid) \in \mathbb{G},$

$for\ mode = F, P : \vec{\varphi}_{mode,t} := (\varphi_{mode,t,1}, \ldots, \varphi_{mode,t,n_t^{(mode)}}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t^{(mode)}},$

$\mathbf{k}_{mode,t}^* := (X_{mode,t}^{-1})^T((\overbrace{x_{mode,t,1}G_1, \ldots, x_{mode,t,n_t^{(mode)}}G_1}^{n_t^{(mode)}}, \overbrace{x_{mode,t,1}G_{gid}, \ldots, x_{mode,t,n_t^{(mode)}}G_{gid}}^{n_t^{(mode)}},$

$\overbrace{0^{2n_t^{(mode)}}}^{2n_t^{(mode)}}, \overbrace{\varphi_{mode,t,1}G_1, \ldots, \varphi_{mode,t,n_t^{(mode)}}G_1}^{n_t^{(mode)}}, \overbrace{\varsigma_{L_{gid,t}} x_{mode,t,1}G_1, \ldots, \varsigma_{L_{gid,t}} x_{mode,t,n_t^{(mode)}}G_1}^{n_t^{(mode)}}, \overbrace{0}^{1})),$

$(DMA - FE : mode = F)$ return $uak_{gid,(t,\vec{x}_{F,t})} := (gid, (t, \vec{x}_{F,t}), \mathbf{k}_{F,t}^*).$

$$(Patch : mode = P)\quad for\ 1 \leqq i \leqq n_t^{(P)} :\ x_{P,t,i} = \begin{cases} 1 & (i = 1) \\ \gamma & (i = 2, \Phi_t(L_{gid,t}[a], a); 0 \leqq a \leqq |L_{gid,t}|) \\ 0 & (else) \end{cases}$$

return $uik_{gid,L_t} := (gid, t, \mathbf{k}_{P,t}^*)$.

return $usk_{gid,(t,\vec{x}_t),L_t} = (uak_{gid,(t,\vec{x}_{F,t})}, uik_{gid,L_t})$

図 1: 提案方式

5. $\mathsf{Enc}(\{apk_t, rpk_{t,r\ell_{t,k_i}}\}, m, \mathbb{S})$:

$\vec{f}_F, \vec{f}_P \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$,

$\vec{s}_F^T := (s_{F,1}, \ldots, s_{F,\ell})^T := M \cdot \vec{f}_F^T,\ s_{F,0} := \vec{1} \cdot \vec{f}_F^T, \vec{s}_P^T := (s_{P,1}, \ldots, s_{P,\ell})^T := M \cdot \vec{f}_P^T,\ s_{P,0} := \vec{1} \cdot \vec{f}_P^T$

$\vec{f'}_F \xleftarrow{\mathsf{R}} \mathbb{F}_q^r\ s.t.\ \vec{1} \cdot \vec{f'}_F^T = s'_0, \vec{s'}_F^T := (s'_{F,1}, \ldots, s'_{F,\ell})^T := M \cdot \vec{f'}_F^T$,

$\vec{f'}_P \xleftarrow{\mathsf{R}} \mathbb{F}_q^r\ s.t.\ \vec{1} \cdot \vec{f'}_P^T = -s'_0, \vec{s'}_P^T := (s'_{P,1}, \ldots, s'_{P,\ell})^T := M \cdot \vec{f'}_P^T$

$\eta_{F,i}, \eta_{P,i,k_i,z}, \theta_{F,i}, \theta_{P,i,k_i,z}, \theta'_{F,i}, \theta'_{P,i,k_i,z}, \theta''_{F,i}, \theta''_{P,i,k_i,z}, w_i \xleftarrow{\mathsf{U}} \mathbb{F}_q (i = 1, \ldots, \ell; z = 1, \ldots, m_{k_i})$,

$(DMA-FE)\quad for\ i\ =\ 1, \ldots, \ell,$

$$\mathbf{c}_{F,i} = \begin{cases} (\overbrace{s_{F,i}\vec{e}_{t,F,1} + \theta_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{s'_{F,i}\vec{e}_{t,F,1} + \theta'_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{0^{2n_t^{(F)}}}^{2n_t^{(F)}}, & (\rho(i) = (t, \vec{v}_{F,i})) \\ \overbrace{0^{n_t^{(F)}}}^{n_t^{(F)}}, \overbrace{w_i\vec{e}_{t,F,1} + \theta''_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{\eta_{F,i}}^{1})_{\mathbb{B}_{F,t}} & \\ (\overbrace{s_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{s'_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{0^{2n_t^{(F)}}}^{2n_t^{(F)}}, \overbrace{0^{n_t^{(F)}}}^{n_t^{(F)}}, \overbrace{w_i\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{\eta_{F,i}}^{1})_{\mathbb{B}_{F,t}} & (\rho(i) = \neg(t, \vec{v}_{F,i})) \end{cases}$$

$c_{d+1} := mg_T^{s_{F,0}+s_{P,0}}, \mathbf{ct}_{\mathbb{S}} := (\mathbb{S}, \mathbf{c}_{F,1}, \ldots, \mathbf{c}_{F,\ell}, c_{d+1})$.

$(Patch)\quad for\ i\ =\ 1, \ldots, \ell; z = 1, \ldots, m_{k_i},$

$$\begin{aligned} &\mathbf{c}_{P,i,k_i,z} \\ &= s_{P,i}\mathbf{b}_{P,1} + \theta_{P,i,k_i,z}cp^{[1]}_{t,k_i,z} + s'_{P,i}\mathbf{b}_{P,n_t^{(P)}+1} + \theta'_{P,i,k_i,z}cp^{[2]}_{t,k_i,z} + (-w_i)\mathbf{b}_{P,5n_t^{(P)}+1} + \theta''_{P,i,k_i,z}cp^{[3]}_{t,k_i,z} \\ &\qquad + \eta_{P,i,k_i,z}\mathbf{b}_{P,6n_t^{(P)}+1} \\ &= (\overbrace{s_{P,i}\vec{e}_{t,P,1} + \theta_{P,i,k_i,z}\vec{v}_{P,i,k_i,z}}^{n_t^{(P)}}, \overbrace{s'_{P,i}\vec{e}_{t,P,1} + \theta'_{P,i,k_i,z}\vec{v}_{P,i,k_i,z}}^{n_t^{(P)}}, \overbrace{0^{2n_t^{(P)}}}^{2n_t^{(P)}}, \\ &\qquad \overbrace{0^{n_t^{(P)}}}^{n_t^{(P)}}, \overbrace{-w_i\vec{e}_{t,P,1} + \theta''_{P,i,k_i,z}\vec{v}_{P,i,k_i,z}}^{n_t^{(P)}}, \overbrace{\theta_{P,i,k_i,z}\eta^{[1]}_{t,k_i,z} + \theta'_{P,i,k_i,z}\eta^{[2]}_{t,k_i,z} + \theta''_{P,i,k_i,z}\eta^{[3]}_{t,k_i,z} + \eta_{P,i,k_i,z}}^{1})_{\mathbb{B}_{P,t}} \end{aligned}$$

return $ct_{\mathbb{S},\{r\ell_{t,k_i}\}} = (\mathbf{ct}_{\mathbb{S}}, \{\mathbf{c}_{P,i,k_i,z}, rpk_{t,k_i}\})$

6. $\mathsf{Delegate}(ct_{\mathbb{S},\{r\ell_{t,k}\}}, rpk_{t,r\ell_{t,k+1}})$:

$\vec{f}_{P,D} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$,

$\vec{s}_{P,D}^T := (s_{P,D,1}, \ldots, s_{P,D,\ell})^T := M \cdot \vec{f}_{P,D}^T, s_{P,D,k_{i_D}+1} := \vec{1} \cdot \vec{f}_{P,D}^T$,

$\vec{f'}_{F,D} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r\ s.t.\ \vec{1} \cdot \vec{f'}_{F,D}^T = s'_{D,0}, \vec{s'}_{F,D}^T := (s'_{F,D,1}, \ldots, s'_{F,D,\ell})^T := M \cdot \vec{f'}_{F,D}^T$

$\vec{f'}_{P,D} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r\ s.t.\ \vec{1} \cdot \vec{f'}_{P,D}^T = -s'_{D,0}, \vec{s'}_{P,D}^T := (s'_{P,D,1}, \ldots, s'_{P,D,\ell})^T := M \cdot \vec{f'}_{P,D}^T$

$\theta_{P,D,i_D,k_{i_D}+1,z}, \theta'_{P,D,i_D,k_{i_D}+1,z}, \theta''_{P,D,i_D,k_{i_D}+1,z}, w_{D,i_D} \xleftarrow{\mathsf{U}} \mathbb{F}_q (i = 1, \ldots, \ell; z = 1, \ldots, m_{k_{i_D}+1})$,

$for\ i\ =\ 1, \ldots, \ell$

$(i = i_D)$

$$\mathbf{c}_{F,D,i_D} = \begin{cases} \mathbf{c}_{F,i_D} + s'_{F,D,i_D}\mathbf{b}_{F,t,n_t^{(F)}+1} + w_{D,i_D}\mathbf{b}_{F,t,5n_t^{(F)}+1} & (\rho(i_D) = (t, \vec{v}_{F,i_D})) \\ \mathbf{c}_{F,i_D} + s'_{F,D,i_D}(\mathbf{b}_{F,t,n_t^{(F)}+1} + \ldots + \mathbf{b}_{F,t,2n_t^{(F)}}) & \\ \quad + w_{D,i_D,k_{i_D}+1}v_{F,i_D,1}\mathbf{b}_{F,t,5n_t^{(F)}+1} \ldots + w_{P,D,i_D,k_{i_D}+1}v_{F,i_D,n_t^{(F)}}\mathbf{b}_{F,t,6n_t^{(F)}} & (\rho(i_D) = \neg(t, \vec{v}_{F,i_D})) \end{cases}$$

$$\begin{aligned} for\ z\ =\ 1, \ldots, m_{k_{i_D}+1} : \mathbf{c}_{P,D,i_D,k_{i_D}+1,z} &= s_{P,D,i_D}\mathbf{b}_{P,t,1} + \theta_{P,D,i_D,k_{i_D}+1,z}cp^{[1]}_{t,k_{i_D}+1,z} \\ &\quad + s'_{P,D,i_D}\mathbf{b}_{P,t,n_t^{(P)}+1} + \theta'_{P,D,i_D,k_{i_D}+1,z}cp^{[2]}_{t,k_{i_D}+1,z} \\ &\quad + (-w_{D,i_D})\mathbf{b}_{P,t,5n_t^{(P)}+1} + \theta''_{P,D,i_D,k_{i_D}+1,z}cp^{[3]}_{t,k_{i_D}+1,z} \end{aligned}$$

図 1: 提案方式 (続き 1)

$(i \neq i_D)$

$$\mathbf{c}_{F,D,i} = \begin{cases} \mathbf{c}_{F,i} + {s'}_{F,D,i}\mathbf{b}_{F,t,n_t^{(F)}+1} & (\rho(i) = (t, \vec{v}_{F,i})) \\ \mathbf{c}_{F,i} + {s'}_{F,D,i_D}(\mathbf{b}_{F,t,n_t^{(F)}+1} + \ldots + \mathbf{b}_{F,t,2n_t^{(F)}}) & (\rho(i_D) = \neg(t, \vec{v}_{F,i_D})) \end{cases}$$

$for\ i\ =\ 1, \ldots, \ell;\ j\ =\ k_i\ s.t.\ rpk_{i,k_i}; z = 1, \ldots, m_j,$

$$\mathbf{c}_{P,D,i,j,z} = \mathbf{c}_{P,i,k_i,z} + s_{P,D,i}\mathbf{b}_{P,t,1} + s'_{P,D,i}\mathbf{b}_{P,t,n_t^{(P)}+1}$$

$$c_{D,d+1} = c_{d+1} \cdot g_T^{s_{P,D,k_{i_D}+1}}$$

return $ct_{\mathbb{S},\{r\ell_{t,k}\}} := (c_{D,d+1}, \mathbf{c}_{F,1}, \ldots, \mathbf{c}_{F,D,i_D}, \ldots, \mathbf{c}_{F,\ell}, \{\mathbf{c}_{P,D,i,j,z}, rpk_{r\ell_{t,k}}\})$.

7. $\mathsf{Rand}(ct_{\mathbb{S},\{r\ell_{t,k_t}\}})$:

$k_{max} = \max\{k_i | rpk_{i,k_i}, i = 1, \ldots, \ell\}, \vec{\tilde{f}}_F, \vec{\tilde{f}}_{P,1}, \ldots, \vec{\tilde{f}}_{P,k_{max}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r,$

$\vec{\tilde{s}}_F^T := (\tilde{s}_{F,1}, \ldots, \tilde{s}_{F,\ell})^T := M \cdot \vec{\tilde{f}}_F^T, \tilde{s}_{F,0} := \vec{1} \cdot \vec{\tilde{f}}_F^T,$

$\vec{\tilde{s}}_{P,j}^T := (\tilde{s}_{P,j,1}, \ldots, \tilde{s}_{P,j,\ell})^T := M \cdot \vec{\tilde{f}}_{P,j}^T, \tilde{s}_{P,j,0} := \vec{1} \cdot \vec{\tilde{f}}_{P,j}^T (j = 1, \ldots, k_{max}),$

$\vec{\tilde{f}}'_F \xleftarrow{\mathsf{R}} \mathbb{F}_q^r\ s.t.\ \vec{1} \cdot \vec{\tilde{f}}'^T_F = \tilde{s'}_0, \vec{\tilde{s}}'^T_F := (\tilde{s'}_{F,1}, \ldots, \tilde{s'}_{F,\ell})^T := M \cdot \vec{\tilde{f}}'^T_F,$

$\vec{\tilde{f}}'_{P,1}, \ldots, \vec{\tilde{f}}'_{P,k_{max}} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r\ s.t.\ \vec{1} \cdot \vec{\tilde{f}}'^T_{P,j} = \tilde{s'}_{0,j},\ (\tilde{s'}_{,0} - (\sum_{j=1}^{k_{max}} \tilde{s'}_0) = 0, \tilde{s'}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \tilde{s'}_{0,j} \xleftarrow{\mathsf{R}} \mathbb{F}_q^\times),$

$\vec{\tilde{s}}'^T_{P,j} := (\tilde{s}'_{P,j,1}, \ldots, \tilde{s}'_{P,j,\ell})^T := M \cdot \vec{\tilde{f}}'^T_P,$

$\tilde{\eta}_{F,i}, \tilde{\eta}_{P,i,j,z}, \tilde{\theta}_{F,i}, \tilde{\theta}_{P,i,j,z}, \tilde{\theta'}_{F,i}, \tilde{\theta'}_{P,i,j,z}, \tilde{\theta''}_{F,i}, \tilde{\theta''}_{P,i,j,z}, \tilde{w}_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q (i = 1, \ldots, \ell; j = 1, \ldots, k_i s.t. rpk_{i,k_i}; z = 1, \ldots, m_j),$

$(DMA-FE)\quad for\ i\ =\ 1, \ldots, \ell;$

$$\mathbf{c'}_{F,i} = \begin{cases} \mathbf{c}_{F,i} + (\overbrace{\tilde{s}_{F,i}\vec{e}_{t,F,1} + \tilde{\theta}_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{\tilde{s'}_{F,i}\vec{e}_{t,F,1} + \tilde{\theta'}_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \\ \overbrace{0^{2n_t^{(F)}}}^{2n_t^{(F)}}, \overbrace{0^{n_t^{(F)}}}^{n_t^{(F)}}, \overbrace{(\tilde{w}_{i,1} + \ldots + \tilde{w}_{i,k_i})\vec{e}_{t,F,1}}^{n_t^{(F)}}, \overbrace{\tilde{\eta}_{F,i}}^{1})_{\mathbb{B}_{F,t}} & (\rho(i) = (t, \vec{v}_{F,i})) \\ \mathbf{c}_{F,i} + (\overbrace{\tilde{s}_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{\tilde{s'}_{F,i}\vec{v}_{F,i}}^{n_t^{(F)}}, \\ \overbrace{0^{2n_t^{(F)}}}^{2n_t^{(F)}}, \overbrace{0^{n_t^{(F)}}}^{n_t^{(F)}}, \overbrace{(\tilde{w}_{i,1} + \ldots + \tilde{w}_{i,k_i})\vec{v}_{F,i}}^{n_t^{(F)}}, \overbrace{\tilde{\eta}_{F,i}}^{1})_{\mathbb{B}_t} & (\rho(i) = \neg(t, \vec{v}_{F,i})) \end{cases}$$

$$c'_{d+1} := mg_T^{\tilde{s}_{F,0} + \tilde{s}_{P,1} + \tilde{s}_{P,2} + \ldots + \tilde{s}_{P,k_{max}}}$$

$(Patch|k_i = k_{max})\quad for\ i\ =\ 1, \ldots, \ell; j\ =\ 1, \ldots, k_i\ s.t.\ rpk_{i,k_i}; z = 1, \ldots, m_j;$

$$\begin{aligned} \mathbf{c'}_{P,i,j,z} &= \mathbf{c}_{P,i,j,z} + \tilde{s}_{P,i,j}\mathbf{b}_{P,1} + \tilde{\theta}_{P,i,j,z}cp_{t,j,z}^{[1]} + \tilde{s}'_{P_i,j}\mathbf{b}_{P,n_t^{(P)}+1} + \tilde{\theta}'_{P,i,j,z}cp_{t,j,z}^{[2]} \\ &\quad + (-\tilde{w}_{i,j})\mathbf{b}_{P,5n_t^{(P)}+1} + \tilde{\theta}''_{P,i,j,z}cp_{t,j,z}^{[3]} + \tilde{\eta}_{P,i,j,z}\mathbf{b}_{P,6n_t^{(P)}+1} \\ &= \mathbf{c}_{P,i,j,z} + (\overbrace{\tilde{s}_{P,i,j}\vec{e}_{t,P,1} + \tilde{\theta}_{P,i,j,z}\vec{v}_{P,i,j,z}}^{n_t^{(P)}}, \overbrace{\tilde{s}'_{P,i,j}\vec{e}_{t,P,1} + \tilde{\theta}'_{P,i,j,z}\vec{v}_{P,i,j,z}}^{n_t^{(P)}}, \overbrace{0^{2n_t^{(P)}}}^{2n_t^{(P)}}, \overbrace{0^{n_t^{(P)}}}^{n_t^{(P)}}, \\ &\qquad \overbrace{-\tilde{w}_{i,j}\vec{e}_{t,P,1} + \tilde{\theta}'_{P,i,j,z}\vec{v}_{P,i,j,z}}^{n_t^{(P)}}, \overbrace{\tilde{\theta}_{P,i,j,z}\eta_{t,j,z}^{[1]} + \tilde{\theta}'_{P,i,j,z}\eta_{t,j,z}^{[2]} + \tilde{\theta}''_{P,i,j,z}\eta_{t,j,z}^{[3]} + \tilde{\eta}_{P,i,j,z}}^{1})_{\mathbb{B}_{P,t}} \end{aligned} \tag{1}$$

$(Patch|k_i < k_{max})\quad for\ i\ =\ 1, \ldots, \ell; j\ =\ 1, \ldots, k_i - 1\ s.t.\ rpk_{i,k_i}; z = 1, \ldots, m_j :$

$\mathbf{c'}_{P,i,j,z} =$ (式 (1) と同じ)

図 1: 提案方式 (続き 2)

$$
\begin{aligned}
&for\ j\ =\ k_i\ s.t.\ rpk_{i,k_i}; z = 1, \ldots, m_j :\\
&\mathbf{c}'_{P,i,j,z} = \mathbf{c}_{P,i,j,z} + (\tilde{s}_{P,i,j} + \tilde{s}_{P,i,j+1} + \ldots + \tilde{s}_{P,i,k_{max}})\mathbf{b}_{P,1} + \tilde{\theta}_{P,i,j,z} cp^{[1]}_{t,j,z}\\
&\qquad + (\tilde{s}'_{P,i,j} + \tilde{s}'_{P,i,j+1} + \ldots + \tilde{s}'_{P,i,k_{max}})\mathbf{b}_{P,n_t^{(P)}+1} + \tilde{\theta}'_{P,i,j,z} cp^{[2]}_{t,j,z}\\
&\qquad\quad + (-\tilde{w}_{i,j} - \tilde{w}_{i,j+1} - \ldots - \tilde{w}_{i,k_{max}})\mathbf{b}_{P,5n_t^{(P)}+1} + \tilde{\theta}''_{P,i,j,z} cp^{[3]}_{t,j,z} + \tilde{\eta}_{P,i,j,z}\mathbf{b}_{P,6n_t^{(P)}+1}\\
&= \mathbf{c}_{P,i,j,z} + (\overbrace{(s_{P,i,j} + s_{P,i,j+1} + \ldots + s_{P,i,k_{max}})\vec{e}_{t,P,1} + \tilde{\theta}_{P,i,j,z}\vec{v}_{P,i,j,z}}^{n_t^{(P)}},\\
&\qquad \overbrace{(s'_{P,i,j} + s'_{P,i,j+1} + \ldots + s'_{P,i,k_{max}})\vec{e}_{t,P,1} + \tilde{\theta}'_{P,i,j,z}\vec{v}_{P,i,j,z}}^{n_t^{(P)}}, \overbrace{0^{2n_t^{(P)}}}^{2n_t^{(P)}},\\
&\qquad \overbrace{0^{n_t^{(P)}}}^{n_t^{(P)}}, \overbrace{(-\tilde{w}_{i,j} - \tilde{w}_{i,j+1} - \ldots - \tilde{w}_{i,k_{max}})\vec{e}_{t,P,1} + \tilde{\theta}''_{P,i,j,z}\vec{v}_{P,i,j,z}}^{n_t^{(P)}},\\
&\qquad \overbrace{\tilde{\theta}_{P,i,j,z}\eta^{[1]}_{t,j,z} + \tilde{\theta}'_{P,i,j,z}\eta^{[2]}_{t,j,z} + \tilde{\theta}''_{P,i,j,z}\eta^{[3]}_{t,j,z} + \tilde{\eta}_{P,i,j,z}}^{1})_{\mathbb{B}_{P,t}}\\
&\text{return } ct'_{\mathbb{S},\{r\ell'_{t,k}\}} = (\mathbf{ct}'_{\mathbb{S}} := (\mathbb{S}, \mathbf{c}'_{F,1}, \ldots, \mathbf{c}'_{F,\ell}, c'_{d+1}), \{\mathbf{c}'_{P,i,j,z}, rpk_{t,k}\})
\end{aligned}
$$

8. $\mathsf{Dec}(\mathsf{gparam}, \{apk_t, rpk_{t,r\ell_{t,k}}\}, usk_{gid,(t,\vec{x}_t),L_t}, ct_{\mathbb{S},\{r\ell_{t,k}\}})$:

$$
\begin{aligned}
K :=& \prod_{i\in I\wedge\rho(i)=(t,\vec{v}_i)} (e(\mathbf{c}_{F,i}, \mathbf{k}^*_{F,t}) \prod_{j=1}^{k_i} \prod_{z\ s.t.\ e(cp^{((1))}_{i,j,z}, \mathbf{k}^*_{P,t})=1} e(\mathbf{c}_{P,i,j,z}, \mathbf{k}^*_{P,t}))^{\alpha_i}\\
&\cdot \prod_{i\in I\wedge\rho(i)=\neg(t,\vec{v}_i)} (e(\mathbf{c}_{F,i}, \mathbf{k}^*_{F,t})^{1/(\vec{v}_i\cdot\vec{x}_t)} \prod_{j=1}^{k_i} \prod_{z\ s.t.\ e(cp^{((1))}_{i,j,z}, \mathbf{k}^*_{P,t})=1} e(\mathbf{c}_{P,i,j,z}, \mathbf{k}^*_{P,t}))^{\alpha_i},
\end{aligned}
$$

return $m' := c_{d+1}/K$.

図 1: 提案方式（続き 3）

[2] T. Okamoto and K. Takashima“Fully Secure Functional Encryption with General relations from the Decisional Linear Assumption,” In Advances in Cryptography - CRYPTO 2010, LNCS vol.6223, pp. 191-208, 2010.

[3] T. Okamoto and K.Takashima“Decentralized Attribute-Based Signatures,” In Public-Key Cryptography - PKC 2013, LNCS vol.7778, pp. 125-142, 2013.

[4] A. Sahai, H. Seyalioglu, and B. Waters“Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption,” In Advances in Cryptography - CRYPTO 2012, LNCS vol.7417, pp. 199-217, 2012.

[5] K. Lee, S. G. Choi, D. H. Lee, J. H. Park, and M. Yung“Self-Updatable Encryption: Time Constrained Access Control with Hidden Attributes and Better Efficiency,” In Advances int Cryptology - ASIACRYPT 2013, pp. 235-254, 2013.

[6] N. Attrapadung and H. Imai“Conunctive Broadcast and Attribute-Based Encryption,” In Pairing-Based Cryptography - Pairing 2009, LNCS vol.5671, pp. 248-265, 2009.

[7] M. Horváth“Attribute-Based Encryption Optimized for Cloud Computing,” Cryptology ePrint Archive, Report 2014/612, 2014.

[8] N. Attrapadung and H. Imai“Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes,” In Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding, LNCS vol.5921, pp278-300, 2009.

[9] T. Nishide“Toward Revocation Mechanism for Multi-Authority CP-ABE,” In SCIS2013, 2013.

[10] T. Ito, S. Ichikawa, T. Mori, Y. Kawai and K. Takashima“Revocation Management in Functional Encryption,” In SCIS2014, 2014.

[11] S. Ichikawa, T. Yamanak, N. Matsuda and T. Sakagami“A Functional Encryption System Supporting Revocation,” In SCIS2012, 2012.

[12] D. Naor, M. Naor, and J. Lotspiech,“Revocation and Tracing Schemes for Stateless Recievers,” In Advances in Crptology - CRYPTO 2001, LNCS vol.2139, pp. 41-62, 2001.

[13] T. Okamoto and K. Takashima“Fully Secure Unbounded Inner-Product and Attribute-Based Encryption,” In Advances in Cryptology - ASIACRYPT 2012, LNCS vol.7658, pp. 349-396, 2012.