条件付き関数型代理人再暗号化方式

川合 豊† 高島 克幸†

† 三菱電機株式会社，〒 247-0056 神奈川県鎌倉市大船 5-1-1,
Kawai.Yutaka@da.MitsubishiElectric.co.jp
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

あらまし 代理人再暗号化方式（Proxy-Re-Encryption, PRE）は，再暗号化鍵と呼ばれる鍵を用いることで，暗号文の宛先を変更可能な公開鍵暗号方式である．PRE では受信者 A は自分宛の暗号文を受信者 B 宛に変更するための再暗号化鍵を作成し，それを代理人と呼ばれる第三者に送る．そして，A 宛の暗号文はすべて代理人が復号することなく B 宛の再暗号化暗号文に変換できる．通常の PRE では，A が作成した再暗号化鍵で A 宛のいかなる暗号文でも再暗号化できる．そのため，受信者 A は再暗号化する暗号文を選ぶことができない．これを解決する一つの技術として，再暗号化鍵に再暗号化する暗号文の条件を指定する，条件付き代理人再暗号化方式があるが，既存方式は設定可能な条件が柔軟でない．

そこで本稿では，利便性の高い代理人再暗号化の実現を目指し，柔軟な条件が設定可能な条件付き関数型代理人再暗号化方式を提案する．具体的に，条件付き関数型代理人再暗号化方式のモデルとその安全性を定義し，内積述語暗号を基にした具体的方式を構成する．提案した方式は，CRYPTO2010 で Okamoto, Takashima によって提案された技法を用いて関数型暗号へ拡張可能である．

Functional Conditional Proxy-Re-Encryption

Yutaka Kawai† Katsuyuki Takashima†

†Mitsubishi Electric, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501 Japan.
Kawai.Yutaka@da.MitsubishiElectric.co.jp
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

Abstract Proxy-re-encryption (PRE) is an interesting extension of traditional public key encryption (PKE). In addition to the normal operations of PKE, with a dedicated re-encryption key (generated by an original receiver A), a proxy can turn ciphertexts originally destined for user A (called original ciphertexts) into those for user B. A remarkable property of PRE is that the proxy carrying out the transform is totally ignorant of the plaintext. In the PRE scheme, *any* original ciphertext destined for user A can be turned into re-encrypted ciphertext for user B with re-encryption key which is generated by the user A. So, the user A cannot control a policy which an original ciphertext is re-encrypted. In order to control over the delegation, several previous works propose the notion of conditional proxy-re-encryption (CPRE). In CPRE scheme, only original ciphertext satisfying a specific *condition* set by the user A can be re-encrypted by the proxy. However, in all previous schemes, conditions which are not flexible. In this paper, we introduce a new notion of functional conditional-proxy-re-encryption (F-CPRE). We first formulate such a model of F-CPRE scheme and a security notion (payload-hiding properties) of F-PRE. We then propose the first inner-product conditional PRE (IP-CPRE) scheme.

1 はじめに

背景. 近年の各種クラウドサービスの浸透により，様々な機密・個人情報がネットワーク上に暗号化して保管される機会が増えている．しかし，データを暗号化しクラウド上に保管すると，他ユーザがその暗号かれたデータを復号できずデータの共有ができないといった利便性の問題がある．

この問題を解決する公開鍵暗号技術として，代理人再暗号化方式 (Proxy-Re-Encryption，PRE) がある．PRE は，Blaze らによって提案された技術で，暗号文を復号せずに暗号文受信者を変更可能な公開鍵暗号方式である [3, 1, 5, 8, 14, 13, 12, 20, 6, 9]．通常の公開鍵暗号の場合，受信者 A 宛の暗号文は受信者 A の復号鍵を用いることでのみ復号することが可能だが，PRE の場合，受信者 A は自分宛の暗号文を受信者 B 宛に変更するための再暗号化鍵を作成し，それを代理人と呼ばれる第三者に送る．そして，A 宛の暗号文はすべて代理人が復号することなく B 宛に変更可能となる．代理人再暗号化方式には，通常の公開鍵暗号を基にした方式 [3, 1, 5, 13, 6, 9]，ID ベース暗号を基にした方式 [8, 14, 20]，属性ベース暗号・関数型暗号を基にした方式 [12, 10]，などがある．

代理人再暗号化方式では，ユーザ A がユーザ B へ再暗号化するために作成した再暗号化鍵 $\mathsf{rk}_{A\to B}$ を用いることで，ユーザ A が復号できるいかなる暗号文もユーザ B 宛に再暗号化することができる．そのため，ユーザ A はどの暗号文を再暗号化するかを制御することが全くできない．この問題を解決する一つの手段として条件付き代理人再暗号化 (Conditional Proxy-Re-Encryption, CPRE) がある [21, 22]．これは，暗号文と再暗号化鍵に「再暗号化する暗号文の条件」w を設定し，暗号文に設定されている条件 w と，再暗号化鍵に設定されている条件 w' が一致する時のみ正しく再暗号化される PRE 方式である．既存の CPRE は，再暗号化鍵に設定した条件と暗号文に設定した条件が一致することのみが再暗号化する条件とされ，柔軟な再暗号化の条件の設定をすることができない．

本稿では，関数型代理人再暗号化方式 [10] の条件付き代理人再暗号化方式へ拡張を行う．関数型暗号 (Functional Encryption, FE) は，公開鍵暗号や ID ベース暗号の機能を一般化した暗号方式である．FE は，暗号文，秘密鍵にそれぞれパラメータ x, v が対応しており，v と x に適切な関係 R が成り立つ，すなわち $R(v, x) = 1$ が成立するときのみ復号が成立するような暗号方式である．関数型暗号は Sahai-Waters [19] の方式から始まり様々な方式や安全性，効率化が研究されている [2, 7, 11, 15, 16, 17, 18]. 文献 [10] では，関数型暗号に代理人再暗号化を付加した方式を提案している．

貢献. 本稿では，初めに，条件付き関数型代理人再暗号化方式を定義する．本稿で提案する CPRE 方式は，再暗号化する条件も上記関係 R で記述することができ，既存方式よりも柔軟な条件設定が可能となっている．提案する代理人再暗号化方式では，オリジナル暗号文に属性パラメータ x と再暗号化属性パラメータ y を対応させる．再暗号化鍵に述語パラメータ v，属性パラメータ x'，再暗号化可能述語パラメータ w を対応させる．再暗号化時は，$R(v, x) = 1$ かつ $R(w, y) = 1$ であれば，再暗号化鍵を用いて x' に対応した暗号文へと変換でき，$R(v', x') = 1$ が成立する v' と対応した秘密鍵を用いることで，変換された再暗号化暗号文を復号することができる．$R(v, x) = 1$, $R(w, y) = 1$ のどちらか一方でも成立しなければ正しく再暗号化をすることができない．

次に，内積述語暗号に条件付き代理人再暗号化機能を付与した方式（Inner Product Conditional Proxy-Re-Encryption, IP-CPRE）の具体的構成を示す．提案した方式は [10] を基としている．また文献 [15] で用いられている非単調一般的なアクセス構造に対応した関数型暗号の構成方法を用いることで，代理人再暗号化機能を持った関数型暗号を構成することができる．提案した IP-CPRE は Decisional Linear (DLIN) 仮定と内部で用いるワンタイム署名が強偽造不可能性を持つならば，オリジナル及び再暗号化暗号文の平文秘匿性を持つ．

2 準備

記法 A が分布であるときに $y \xleftarrow{\mathsf{R}} A$ は y を A からその分布に従ってランダムに選ぶことを指す．A が集合であるときに，$y \xleftarrow{\mathsf{U}} A$ は y を A から一様に選ぶことを指す．位数 q の有限体を $\mathbb{F}_q$ と表し，$\mathbb{F}_q \setminus \{0\}$ を $\mathbb{F}_q^\times$ と表す．$\mathbb{F}_q$ 上のベクトル $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ を $\vec{x}$ と表記する．二つのベクトル $\vec{x}$ と $\vec{v}$ の内積 $\sum_{i=1}^n x_i v_i$ を $\vec{x} \cdot \vec{v}$ と表す．$\mathbb{F}_q^n$ での零ベクトルを $\mathbf{0}$ と表す．X^{T} は行列 X の転置行列を表し，I_ℓ と 0_ℓ はそれぞれ ℓ 行 ℓ 列の単位行列と零行列を指す．ベクトル空間 $\mathbb{V}$ の要素は $\boldsymbol{x} \in \mathbb{V}$ と表す．$\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$ である時，$\boldsymbol{b}_i, \ldots, \boldsymbol{b}_n$ によって作られる部分空間は $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ と表される．また，$\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ と $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$ に対して，$(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \boldsymbol{b}_i$，及び $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \boldsymbol{b}_i^*$ と定義する．$\vec{e}_j$ は $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n-j}) \in \mathbb{F}_q^n$ $(j = 1, \ldots, n_t)$ を指す．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．行列 $W := (w_{i,j})_{i,j=1,\ldots,n} \in \mathbb{F}_q^{n \times n}$ と n 次元ベクトル空間 $\mathbb{V}$ における要素 $\boldsymbol{g} := (G_1, \ldots, G_n)$ に対して，$\boldsymbol{g}W := (\sum_{i=i}^n G_i w_{i,1}, \ldots, \sum_{i=i}^n G_i w_{i,n}) = (\sum_{i=i}^n w_{i,1} G_i, \ldots, \sum_{i=i}^n w_{i,n} G_i)$ と定義する．

Dual Pairing Vector Spaces (DPVS)

定義 1 (対称ペアリング群) : 対象ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ は素数 q，位数 q の加法的巡回群 $\mathbb{G}$ と乗法的巡回群 $\mathbb{G}_T$ 及び $G \neq 0 \in \mathbb{G}$ と多項式時間で計算可能な非退化性を持つ双線形写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ からなる．セキュリティパラメータ 1^λ を入力として上記対象ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ を出力するアルゴリズムを $\mathcal{G}_{\mathsf{bpg}}$ と書く．

定義 2 (Dual pairing vector spaces) : *Dual pairing vector spaces (DPVS)* は $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ は位数 q，$\mathbb{F}_q$ 上の N 次元ベクトル空間 $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$，位数 q の巡回群 $\mathbb{G}_T$，$\mathbb{V}$ の標準基底 $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$（但し $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$）とペアリング演算 $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$ から構成される．

ここで，N 次元ベクトル $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ と $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$ のペアリング演算 $e(\boldsymbol{x}, \boldsymbol{y})$ を $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^N e(G_i, H_i) \in \mathbb{G}_T$ と定義する．また，上記演算は非退化性をもつ．$e(G, G) \neq 1 \in \mathbb{G}_T$ であれば任意の i と j に対して，$e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G, G)^{\delta_{i,j}}$ である．ここで $\delta_{i.j}$ は $i = j$ の時に $\delta_{i.j} = 1$ であり，$i \neq j$ の時 $\delta_{i.j} = 0$ である．*DPVS*生成アルゴリズム $\mathcal{G}_{\mathsf{dpvs}}$ は，セキュリティパラメータ $1^\lambda (\lambda \in \mathbb{N})$ と $\mathbb{V}$ の次元 $N \in \mathbb{N}$ を入力として，$\mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ を出力する．このアルゴリズムは $\mathcal{G}_{\mathsf{bpg}}$ から構成することができる．

Dual Orthonormal Basis Generator 以下に，本方式で用いる双対基底生成器（dual orthonormal basis generator）を示す．

$\mathcal{G}_{\mathsf{ob}}(1^\lambda, N)$:
- $\mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N)$,
- $\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, g_T := e(G, G)^\psi$,
- $X := (\chi_{i,j}) \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q)$,
- $(\vartheta_{i,j}) := \psi \cdot (X^{\mathrm{T}})^{-1}$,
- $\mathsf{param}_{\mathbb{V}} := (\mathsf{param}'_{\mathbb{V}}, g_T)$,
- $\boldsymbol{b}_i := \sum_{j=1}^N \chi_{i,j} \boldsymbol{a}_j, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$,
- $\boldsymbol{b}_i^* := \sum_{j=1}^N \vartheta_{i,j} \boldsymbol{a}_j, \mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$,
- return $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*)$.

Decisional Linear (DLIN) 仮定

定義 3 (DLIN: Decisional Linear 仮定 [4]) DLIN 問題は $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$ を入力として $\beta \in \{0, 1\}$ を推定する問題であり，各パラメータは $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$ に対して以下のように決定される．

$\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$:
- $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$,
- $\kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $Y_0 := (\delta + \sigma)G$, $Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}$,
- return $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$

任意の確率的アルゴリズム $\mathcal{E}$ に対して，
$\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left| \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda) \right] \right.$

$-\ \mathsf{Pr}\left[\mathcal{E}(1^\lambda,\varrho)\to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right]\Big|$ を $\mathcal{E}$ のアドバンテージとして定義する．DLIN 仮定とは，任意の確率的多項式時間攻撃者 $\mathcal{E}$ に対し，上記のアドバンテージ $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ がセキュリティパラメータ λ に対し無視できることと定義する．

3 条件付き関数型代理人再暗号化

本章では，条件付き関数型代理人再暗号化方式（Functional Conditional Proxy-Re-Encryption, F-CPRE）のモデル及び安全性を定義する．

3.1 モデル

x, x' を属性，v を述語，y を再暗号化属性，w を再暗号化可能述語とする．F-CPRE では，オリジナル暗号文に x, y が，再暗号化鍵には v, w, x' が対応づいている．再暗号化時には，x と v，y と w それぞれに適切な関係 R が成り立つ，すなわち $R(x,v)=1$ かつ $R(y,w)=1$ が成立する時のみ再暗号化が成立し x' と対応する再暗号化暗号文が生成される．

定義 4 F-CPRE 方式は（Setup, KG, Enc, RKG, REnc, $\mathsf{Dec}_{\mathsf{oct}}$, $\mathsf{Dec}_{\mathsf{rct}}$）の 7 つのアルゴリズムから定義される．

Setup: セキュリティパラメータ λ とフォーマットパラメータ Λ を入力とし，マスター秘密鍵 sk と公開鍵 pk を出力する確率的アルゴリズム．

KG: 公開鍵 pk，マスター秘密鍵 sk，述語 v を入力とし，復号鍵 sk_v を出力する確率的アルゴリズム．

Enc: 公開鍵 pk，平文 m，属性 x，再暗号化属性 y を入力とし，オリジナル暗号文 oct_x^y を出力する確率的アルゴリズム．

RKG: 公開鍵 pk，復号鍵 sk_v，属性 x'，再暗号化可能述語 w を入力とし，再暗号化鍵 $\mathsf{rk}_{v,x'}^w$ を出力する確率的アルゴリズム．

REnc: 公開鍵 pk，再暗号化鍵 $\mathsf{rk}_{v,x'}^w$，及びオリジナル暗号文 oct_x^y を入力とし，再暗号化暗号文 $\mathsf{rct}_{x'}$ もしくは識別記号 $\perp$ を出力する確率的アルゴリズム．

$\mathsf{Dec}_{\mathsf{oct}}$: 公開鍵 pk，復号鍵 sk_v，オリジナル暗号文 oct_x^y を入力とし，平文 m もしくは識別記号 $\perp$ を出力する確定的アルゴリズム．

$\mathsf{Dec}_{\mathsf{rct}}$: 公開鍵 pk，復号鍵 sk_v，再暗号化暗号文 rct_x を入力とし，平文 m もしくは識別記号 $\perp$ を出力する確定的アルゴリズム．

F-CPRE は，適切な関係 R に対して，(1) いかなる平文 m，公開鍵とマスター秘密鍵ペア $(\mathsf{pk},\mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$，述語 v，属性 x，再暗号化属性 y，復号鍵 $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk},\mathsf{sk},v)$ に対して，$R(v,x)=1$ が成立するならば $m = \mathsf{Dec}_{\mathsf{oct}}(\mathsf{pk},\mathsf{sk}_v,\mathsf{Enc}(\mathsf{pk},m,x,y))$ が圧倒的確率で成立し，上記関係が成り立たなければ無視できる確率でしか上記の等式は成立しない．また，(2) いかなる平文 m，公開鍵とマスター秘密鍵ペア $(\mathsf{pk},\mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$，述語 v, v'，属性 x, x'，再暗号化可能述語 w，再暗号化属性 y，復号鍵 $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk},\mathsf{sk},v)$，$\mathsf{sk}_{v'} \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk},\mathsf{sk},v')$，再暗号化暗号文 $\mathsf{rct}_{x'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{RKG}(\mathsf{pk},\mathsf{sk}_v,x',w), \mathsf{Enc}(\mathsf{pk},m,x,y))$，に対して，$R(v,x)=1$，$R(w,y)=1$，$R(v',x')=1$，のすべてが成立するのであれば，$m = \mathsf{Dec}_{\mathsf{rct}}(\mathsf{pk},\mathsf{sk}_{v'},\mathsf{rct}_{x'})$ が圧倒的確率で成立し，上記関係が成り立たなければ無視できる確率でしか上記の等式は成立しない．

3.2 安全性要件

本章では，F-CPRE 方式のオリジナル暗号文に対する平文秘匿性（Payload Hiding for Original Ciphertexts, OH-OC）と再暗号化暗号文の平文秘匿性（Payload Hiding for Reencrypted Ciphertexts, OH-RT）を定義する．

定義 5 (オリジナル暗号文に対する安全性)
F-CPRE 方式が選択平文攻撃に対するオリジナル暗号文の平文秘匿性（OH-OC）を持つとは，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても下記の OPH-CPA ゲームにおいて，$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{OH\text{-}OC}}(\lambda) = |\mathsf{Pr}[b=b'] - \frac{1}{2}|$ が λ に対して無視できることを言う．

セットアップ: チャレンジャーは $(\mathsf{pk},\mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda,\Lambda)$ を実行し，攻撃者 $\mathcal{A}$ に対して λ, Λ と公開鍵 pk を与える．

第一フェーズ: 攻撃者 $\mathcal{A}$ は以下のクエリをチャレンジャーに対して多項式回実行することができる．

復号鍵クエリ: $\mathcal{A}$ が述語 v をクエリしてきたならば，チャレンジャーは，$\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v)$ を計算し攻撃者 $\mathcal{A}$ に与える．

再暗号化鍵クエリ: $\mathcal{A}$ が述語と再暗号化属性，属性の組 (v, w, x') をクエリしてきたならば，チャレンジャーは $\mathsf{rk}^w_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_v, w, x')$ (ただし，$\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v)$) を計算し攻撃者 $\mathcal{A}$ に与える．

再暗号化クエリ: $\mathcal{A}$ が属性とオリジナル暗号文のペア (x', oct^y_x) をクエリしてきたならば，チャレンジャーは $\mathsf{rct}_{x'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}^w_{v,x'}, \mathsf{oct}^y_x)$ （ただし，$R(v, x) = 1$ となる v，および $R(w, y) = 1$ となる w であり，$\mathsf{rk}_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v), w, x')$) を計算し攻撃者 $\mathcal{A}$ に与える．

チャレンジクエリ: $\mathcal{A}$ が $(m^{(0)}, m^{(1)}, x^*, y^*)$ をクエリしたならば，チャレンジャーは $b \xleftarrow{\mathsf{U}} \{0, 1\}$ を選び，$\mathsf{oct}^{y^*}_{x^*} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, x^*, m^{(b)})$ を計算する．チャレンジャーは $\mathsf{oct}^{y^*}_{x^*}$ を $\mathcal{A}$ に返答する．ただしチャレンジクエリ $(m^{(0)}, m^{(1)}, x^*, y^*)$ は以下の条件を見たいしているものとする．

- いかなる復号鍵クエリ v も $R(v, x^*) = 0$ を満たす．
- 再暗号化鍵クエリ (v, w, x') が
  - $R(v, x^*) = 0$ もしくは
  - $R(w, y^*) = 0$ もしくは
  - いかなる復号鍵クエリ v' に対しても $R(v', x') = 0$

第二フェーズ: 攻撃者 $\mathcal{A}$ は第一フェーズと同様に，復号鍵クエリ，再暗号化鍵クエリ，再暗号化クエリを実行することができる．ただし再暗号化鍵クエリは以下の条件を満たすものとする．

再暗号化クエリ: $\mathcal{A}$ が属性とオリジナル暗号文のペア (x', oct^y_x) をクエリしてきたならば，もし，$\mathsf{oct}^y_x = \mathsf{oct}^{y^*}_{x^*}$ であった場合，いかなる復号鍵クエリ v' も $R(v', x') = 0$ であれば，チャレンジャーは $\mathsf{rct}_{x'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}^w_{v,x'}, \mathsf{oct}^y_x)$ （ただし，$R(v, x) = 1$ となる v，および $R(w, y) = 1$ となる w であり，$\mathsf{rk}_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v), w, x')$) を計算し攻撃者 $\mathcal{A}$ に与える．

出力: 攻撃者 $\mathcal{A}$ は b の推測値 $b' \in \{0, 1\}$ を出力する．もし $b = b'$ であれば $\mathcal{A}$ の勝ちとする．

定義 6 (再暗号化暗号文に対する安全性)
F-CPRE 方式が選択平文攻撃に対する再暗号化暗号文の平文秘匿性（PH-RC）を持つとは，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても，$\mathsf{Adv}^{\mathsf{PH\text{-}RC}}_{\mathcal{A}}(\lambda) = |\mathsf{Pr}[b = b'] - \frac{1}{2}|$ が λ に対して無視できることを言う．

セットアップ，復号鍵クエリ，再暗号化鍵クエリ，再暗号化クエリは，PH-OC 安全性と同じであるため省略する．

チャレンジクエリ: $\mathcal{A}$ が $(m^{(0)}, m^{(1)}, v^*, w^*, x^*, y^*, x'^*)$ をクエリしたなば，$b \xleftarrow{\mathsf{U}} \{0, 1\}$ を選び，$\mathsf{oct}^{y^*}_{x^*} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, x^*, y^* m^{(b)})$，$\mathsf{sk}_{v^*} \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v^*)$，$\mathsf{rk}^{w^*}_{v^*,x'^*} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{sk}_{v^*}, w^*, x'^*)$，$\mathsf{rct}_{x'^*} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}^{w^*}_{v^*,x'^*}, \mathsf{oct}_{x^*})$ を計算する．チャレンジャーは $\mathsf{rct}_{x'^*}$ を $\mathcal{A}$ に返答する．ただしチャレンジクエリ $(m^{(0)}, m^{(1)}, v^*, w^*, x^*, y^*, x'^*)$ は，いかなる復号鍵クエリ v' が $R(v', x'^*) = 0$ を満たさなければならない．

最終的に，$\mathcal{A}$ は b の推測値として $b' \in \{0, 1\}$ を出力し，もし $b = b'$ であれば $\mathcal{A}$ の勝ちとする．

4 提案方式

本稿では，属性や述語をベクトルで表現する内積述語暗号をベースにした F-CPRE を示す．内積述語暗号における属性は属性ベクトル $\vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$ で表される．また，属性ベクトル $\vec{x}$ と述語ベクトル $\vec{v}$ との関係，すなわち $R(\vec{v}, \vec{x}) = 1$ となるのは $\vec{v}$ と $\vec{x}$ との内積が 0 （$\vec{v} \cdot \vec{x} = 0$）の時のみとする．

提案方式は文献 [10] と同様に，DPVS で作られる双対基底を基とし，CHK 変換およびランダムな行列を用いた基底変換を用いている．

本方式は文献 [16] で用いられている公開鍵のパラメータ低減の技法や，文献 [17] で提案されている属性強秘匿性（Fully attribute-hiding）を満たす構成，また文献 [18] で提案されている Unbounded IPE の構成技法を同じように適用することができる．また，文献 [10] と同様の構成をすることによって，再暗号化鍵の述語と属性の秘匿性を達成することができる．

4.1 構成要素

定義 7 (内積述語暗号) 内積述語暗号は $\mathsf{Setup}_{\mathtt{IPE}}$, $\mathsf{KG}_{\mathtt{IPE}}$，$\mathsf{Enc}_{\mathtt{IPE}}$，$\mathsf{Dec}_{\mathtt{IPE}}$ の 4 つのアルゴリズムからなる．$\mathsf{Setup}_{\mathtt{IPE}}$ はセキュリティパラメータ λ と次元 n を入力とし，マスター秘密鍵 $\mathsf{sk}^{\mathtt{IPE}}$ と公開鍵 $\mathsf{pk}^{\mathtt{IPE}}$ を出力する確率的アルゴリズム．$\mathsf{KG}_{\mathtt{IPE}}$ は公開鍵 $\mathsf{pk}^{\mathtt{IPE}}$ とマスター秘密鍵 $\mathsf{sk}^{\mathtt{IPE}}$，述語ベクトル $\vec{v}$ を入力とし，復号鍵 $\mathsf{sk}_{\vec{v}}^{\mathtt{IPE}}$ を出力する確率的アルゴリズム．$\mathsf{Enc}_{\mathtt{IPE}}$ は公開鍵 $\mathsf{pk}^{\mathtt{IPE}}$ と平文 m，属性ベクトル $\vec{x}$ を入力とし，暗号文 ψ を出力する確率的アルゴリズム．$\mathsf{Dec}_{\mathtt{IPE}}$ は公開鍵 $\mathsf{pk}^{\mathtt{IPE}}$，復号鍵 $\mathsf{sk}_{\vec{v}}^{\mathtt{IPE}}$，暗号文 ψ を入力とし，平文 m もしくは識別記号 $\perp$ を出力するアルゴリズムである．

定義 8 (平文秘匿性) IPE 方式が選択平文攻撃に対する平文秘匿性を持つとは，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても下記の PH-CPA ゲームにおいて，$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE\text{-}PH}}(\lambda) = |\Pr[b = b'] - \frac{1}{2}|$ が λ に対して無視できることを言う．

セットアップ: チャレンジャーは $(\mathsf{pk}^{\mathtt{IPE}}, \mathsf{sk}^{\mathtt{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathtt{IPE}}(1^\lambda, n)$ を実行し，攻撃者 $\mathcal{A}$ に対してセキュリティパラメータ λ と公開鍵 $\mathsf{pk}^{\mathtt{IPE}}$ を与える．

復号鍵クエリ: $\mathcal{A}$ が述語ベクトル $\vec{v}$ をクエリしてきたならば，チャレンジャーは，$\mathsf{sk}_{\vec{v}}^{\mathtt{IPE}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \mathsf{sk}^{\mathtt{IPE}}, \vec{v})$ を計算し攻撃者 $\mathcal{A}$ に与える．

チャレンジクエリ: $\mathcal{A}$ が $(m^{(0)}, m^{(1)}, \vec{x}^*)$ をクエリしたならば，チャレンジャーは $b \xleftarrow{\mathsf{U}} \{0,1\}$ を選び，$\psi^* \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}^*, m^{(b)})$ を計算する．チャレンジャーは ψ^* を $\mathcal{A}$ に返答する．

ただし，$\mathcal{A}$ が復号鍵クエリに $R(\vec{v}, \vec{x}^*) = 1$ となるような $\vec{v}$ をクエリした時はチャレンジャーは識別記号 $\perp$ を $\mathcal{A}$ に返答する．最終的に，$\mathcal{A}$ は b の推測値として $b' \in \{0,1\}$ を出力し，もし $b = b'$ であれば $\mathcal{A}$ の勝ちとする．

定義 9 (ワンタイム署名) ワンタイム署名方式は $\mathtt{SigKG}$，$\mathtt{Sig}$，$\mathtt{Ver}$ の 3 つのアルゴリズムからなる．$\mathtt{SigKG}$ はセキュリティパラメータ λ を入力とし，署名鍵 sigk と検証鍵 verk を出力する確率的アルゴリズム．$\mathtt{Sig}$ は署名鍵 sigk，文書 m を入力とし，署名 S を出力する確率的アルゴリズム．$\mathtt{Ver}$ は検証鍵 verk，文書 m，署名 S を入力とし，署名 S が verk と m に対して正当であれば 1 を，それ以外 0 を出力するアルゴリズムである．

ワンタイム署名方式は，いかなる $(\mathsf{verk}, \mathsf{sigk}) \xleftarrow{\mathsf{R}} \mathtt{SigKG}(1^\lambda)$ と文書 m に対して $\mathtt{Ver}(\mathsf{verk}, m, \mathtt{Sig}(\mathsf{sigk}, m)) = 1$ が確率 1 で成り立つ．

定義 10 (強偽造不可能性) ワンタイム署名方式が，強偽造不可能であるとは，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても下記の攻撃ゲームにおいて，攻撃成功確率 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{OS,SUF}}(\lambda)$ が λ に対して無視できる値であることをいう．

セットアップ: $(\mathsf{verk}, \mathsf{sigk}) \xleftarrow{\mathsf{R}} \mathtt{SigKG}(1^\lambda)$ を実行し verk を攻撃者 $\mathcal{A}$ に与える．

署名クエリ: $\mathcal{A}$ は署名オラクル $\mathtt{Sig}(\mathsf{sigk}, \cdot)$ に最大 *1* 回アクセスする事ができ，クエリした文書 m に対する正当な署名 S を得ることができる．

出力: 最後に，$\mathcal{A}$ は偽造した文書と署名のペア (m', S') を出力する．

$(m', S') \neq (m, S)$ であり，かつ $\mathtt{Ver}(\mathsf{verk}, m', S') = 1$ であれば攻撃者 $\mathcal{A}$ の勝ちとする．

4.2 安全性

図 **??**の IP-CPRE 方式は以下の定理を満たす．

定理 1 DLIN 仮定，IPE の平文秘匿性，ワンタイム署名方式の強偽造不可能性の下で，提案 IP-CPRE 方式は選択平文攻撃の下でオリジナル暗号文に対する平文秘匿性を持つ．

$\mathsf{Setup}(1^\lambda, n)$:
$(\mathsf{pk}^{\mathtt{IPE}}, \mathsf{sk}^{\mathtt{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathtt{IPE}}(1^\lambda, n)$,
$(\mathsf{param}_n, \mathbb{B} = (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+3}), \mathbb{B}^* = (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{4n+3})) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4)$,
$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{2n+2}, \boldsymbol{b}_{4n+3}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_{2n+2}, \boldsymbol{b}^*_{3n+2}, \ldots, \boldsymbol{b}^*_{4n+2})$,
return $\mathsf{pk} := (1^\lambda, \mathsf{pk}^{\mathtt{IPE}}, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*), \quad \mathsf{sk} := (\boldsymbol{b}^*_0, \mathsf{sk}^{\mathtt{IPE}})$.

$\mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \vec{v})$:
$\mathsf{sk}^{\mathtt{IPE}}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \mathsf{sk}^{\mathtt{IPE}}, \vec{v}), \quad \delta \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, \quad \boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^n,\ 0^2,\ 0^n,\ \vec{\eta},\ 0)_{\mathbb{B}^*}$,
return $\mathsf{sk}_{\vec{v}} := (\vec{v}, \boldsymbol{k}^*, \mathsf{sk}^{\mathtt{IPE}}_{\vec{v}})$.

$\mathsf{Enc}(\mathsf{pk}, \vec{x}, \vec{y}, m)$:
$\zeta, \omega, \theta, \rho, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad (\mathsf{sigk}, \mathsf{verk}) \xleftarrow{\mathsf{R}} \mathtt{SigKG}(1^\lambda), \quad \boldsymbol{c}_0 := (\ \zeta,\ \omega\vec{x},\ \theta\vec{y},\ \rho(\mathsf{verk}, 1),\ \ 0^n,\ 0^n,\ \varphi)_{\mathbb{B}}$,
$c_1 := m \cdot g_T^{\zeta}, \quad C := (\vec{x}, \vec{y}, \boldsymbol{c}_0, c_1), \quad S \xleftarrow{\mathsf{R}} \mathtt{Sig}(\mathsf{sigk}, C), \quad$ return $\mathsf{oct}^{\vec{y}}_{\vec{x}} := (C, \mathsf{verk}, S)$.

$\mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \vec{w}, \vec{x}')$:
$\delta', \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{\eta}\,' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$,
$\boldsymbol{d}^*_i := \boldsymbol{b}^*_i W_1 \quad$ for $i = 1, \ldots, 2n+2, 3n+2, \ldots, 4n+3$,
$\widehat{\mathbb{D}}^*_1 := (\boldsymbol{d}^*_1, \ldots, \boldsymbol{d}^*_{2n+2}, \boldsymbol{d}^*_{3n+2}, \ldots, \boldsymbol{d}^*_{4n+3})$
$\boldsymbol{k}^{*\mathsf{rk}} := (\boldsymbol{k}^* + (\ 0,\ \delta'\vec{v},\ \tau\vec{w},\ 0^2,\ 0^n,\ \vec{\eta}\,',\ 0)_{\mathbb{B}^*})W_1$,
$\psi^{\mathsf{rk}} \xleftarrow{\mathsf{R}} \mathtt{Enc}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}', W_1), \quad$ return $\mathsf{rk}^{\vec{w}}_{\vec{v}, \vec{x}'} := (\vec{v}, \vec{w}, \vec{x}', \boldsymbol{k}^{*\mathsf{rk}}, \widehat{\mathbb{D}}^*_1, \psi^{\mathsf{rk}})$.

$\mathsf{REnc}(\mathsf{pk}, \mathsf{rk}^{\vec{w}}_{\vec{v}, \vec{x}'} := (\vec{v}, \vec{w}, \vec{x}', \boldsymbol{k}^{*\mathsf{rk}}, \widehat{\mathbb{D}}^*_1, \psi^{\mathsf{rk}}), \mathsf{oct}^{\vec{y}}_{\vec{x}} := (C := (\vec{x}, \vec{y}, \boldsymbol{c}_0, c_1), \mathsf{verk}, S))$:
If $\mathtt{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$.
$\delta'', \theta', \tau', \sigma, \zeta', \omega', \rho', \varphi' \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{\eta}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, W_2 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$
$\boldsymbol{k}^{*\mathsf{renc}} := \boldsymbol{k}^{*\mathsf{rk}} + (\ 0,\ \delta''\vec{v},\ \theta'\vec{y},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}\,'',\ 0)_{\mathbb{D}^*_1}$,
$\boldsymbol{c}^{\mathsf{renc}}_0 := (\boldsymbol{c}_0 + (\ \zeta',\ \omega'\vec{x},\ \tau'\vec{w},\ \rho'(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi')_{\mathbb{B}})W_2, \qquad c^{\mathsf{renc}}_1 := c_1 \cdot g_T^{\zeta'}$
$\psi^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathtt{Enc}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}', W_2), \quad$ return $\mathsf{rct}_{\vec{x}'} := (\vec{x}', \boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}_0, c^{\mathsf{renc}}_1, \psi^{\mathsf{rk}}, \psi^{\mathsf{renc}})$.

$\mathsf{Dec}_{\mathsf{oct}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\vec{v}, \boldsymbol{k}^*, \mathsf{sk}^{\mathtt{IPE}}_{\vec{v}}), \mathsf{oct}_{\vec{x}} := (C := (\vec{x}, \boldsymbol{c}_0, c_1), \mathsf{verk}, S))$:
If $\mathtt{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp, \quad K := e(\boldsymbol{c}_0, \boldsymbol{k}^*), \quad$ return $\widetilde{m} := c_1 / K$.

$\mathsf{Dec}_{\mathsf{rct}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}'} := (\vec{v}', \boldsymbol{k}^*, \mathsf{sk}^{\mathtt{IPE}}_{\vec{v}'}), \mathsf{rct}_{\vec{x}'} := (\vec{x}', \boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}_0, c^{\mathsf{renc}}_1, \psi^{\mathsf{rk}}, \psi^{\mathsf{renc}}))$:
$\widetilde{W}_1 \xleftarrow{\mathsf{R}} \mathtt{Dec}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \mathsf{sk}^{\mathtt{IPE}}_{\vec{v}'}, \psi^{\mathsf{rk}}), \quad \widetilde{W}_2 \xleftarrow{\mathsf{R}} \mathtt{Dec}_{\mathtt{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \mathsf{sk}^{\mathtt{IPE}}_{\vec{v}'}, \psi^{\mathsf{renc}})$,
$\widetilde{\boldsymbol{k}}^* := \boldsymbol{k}^{*\mathsf{renc}} \widetilde{W}_1^{-1}, \qquad \widetilde{\boldsymbol{c}}_0 := \boldsymbol{c}^{\mathsf{renc}}_0 \widetilde{W}_2^{-1}, \qquad \widetilde{K} := e(\widetilde{\boldsymbol{c}}_0, \widetilde{\boldsymbol{k}}^*), \qquad$ return $\widetilde{m} := c^{\mathsf{renc}}_1 / \widetilde{K}$.

図 1: 代理人再暗号化機能を持つ内積述語暗号

定理 2 IPE が平文秘匿性を持てれば，提案 IP-CPRE 方式は選択平文攻撃の下で再暗号化暗号文に対する平文秘匿性を持つ．

それぞれの定理は文献 [10] と同様の証明によって導かれる．

参考文献

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. *ACM Trans. Inf. Syst. Secur.*, 9(1):1–30, 2006.

[2] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.

[3] M. Blaze, G. Bleumer, and M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In *Advances in Cryptology - EUROCRYPT'98*, volume 1403 of *LNCS*, pages 127–144, 1998.

[4] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55, 2004.

[5] R. Canetti and S. Hohenberger. Chosen-Ciphertext Secure Proxy Re-encryption. In *Proceedings of the 14th ACM conference on Computer and communications security - ACM CCS 2007*, pages 185–194, 2007.

[6] S. Chow, J. Weng, Y. Yang, and R. Deng. Efficient Unidirectional Proxy Re-Encryption. In *Progress in Cryptology - AFRICACRYPT 2010*, volume 6055 of *LNCS*, pages 316–332, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security - ACM CCS 2006*, pages 89–98, 2006.

[8] M. Green and G. Ateniese. Identity-Based Proxy Re-encryption. In *Applied Cryptography and Network Security*, volume 4521 of *LNCS*, pages 288–306, 2007.

[9] G. Hanaoka, Y. Kawai, N. Kunihiro, T. Matsuda, J. Weng, R. Zhang, and Y. Zhao. Generic construction of chosen ciphertext secure proxy re-encryption. In *Topics in Cryptology – CT-RSA 2012*, volume 7178 of *LNCS*, pages 349–364. 2012.

[10] Y. Kawai and K. Takashima. Fully-Anonymous Functional Proxy-Re-Encryption . Cryptology ePrint Archive, Report http://eprint.iacr.org/2013/318, 2013.

[11] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91, 2010. Full version is available at http://eprint.iacr.org/2010/110.

[12] X. Liang, Z. Cao, H. Lin, and J. Shao. Attribute based proxy re-encryption with delegating capabilities. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ASIACCS '09, pages 276–286. ACM, 2009.

[13] B. Libert and D. Vergnaud. Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption. In *Public Key Cryptography - PKC 2008*, volume 4939 of *LNCS*, pages 360–379, 2008.

[14] T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *Pairing-Based Cryptography Pairing 2007*, volume 4575 of *LNCS*, pages 247–267, 2007.

[15] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208, 2010. Full version is available at http://eprint.iacr.org/2010/563.

[16] T. Okamoto and K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In *Cryptology and Network Security - CANS 2011*, volume 7092 of *LNCS*, pages 138–159, 2011. Full version is available at http://eprint.iacr.org/2011/648.

[17] T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *Advances in Cryptology - Eurocrypt 2012*, volume 7237 of *LNCS*, pages 591–608, 2012. Full version is available at http://eprint.iacr.org/2011/543.

[18] T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *Advances in Cryptology - Asiacrypt 2012*, volume 7658 of *LNCS*, pages 349–366, 2012. Full version is available at http://eprint.iacr.org/2011/671.

[19] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473, 2005.

[20] L. Wang, L. Wang, M. Mambo, and E. Okamoto. New identity-based proxy re-encryption schemes to prevent collusion attacks. In *Pairing-Based Cryptography - Pairing 2010*, volume 6487 of *LNCS*, pages 327–346, 2010.

[21] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai. Conditional Proxy Re-Encryption Secure against Chosen-Ciphertext Attack. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pages 322–332. ACM, 2009.

[22] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao. Efficient Conditional Proxy Re-encryption with Chosen-Ciphertext Security. In *Information Security*, pages 151–166. Springer, 2009.