SCIS 2011 The 2011 Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 25-28, 2011
The Institute of Electronics, Information and Communication Engineers

関数型暗号の応用: 検証可能時限式暗号

An Application of Functional Encryption: Verifiable Timed-Release Encryption

星野 文学* 藤岡 淳*
Fumitaka Hoshino Atsushi Fujioka

あらまし 時限式暗号とは, 暗号文の正規の受信者であっても送信者が指定した開封時刻になるまで暗号文が復号できないような特殊な暗号のことである. 2000 年頃に pairing ベースの ID ベース暗号が提案されると, 時報局と呼ばれる信頼できる第三者が存在し, 時報局がユーザと対話せず時報トークンを放送する型の時限式暗号が盛んに研究されるようになった. 本論文では開封時刻以降に時報局より放送される指数的多数の如何なる時報トークンを使用しても暗号文が復号出来る時限式暗号について考察する. そのような時限式暗号は関数型暗号を用いて容易に実現可能である. 関数型暗号とは属性ベース暗号や述語暗号を含む ID ベース暗号の拡張概念で, 近年活発に研究されている. さらに本論文では上記のような時限式暗号について, 敵対的送信者に関するさまざまな問題点を研究し, 時限式暗号の拡張として検証可能時限式暗号の概念を提案する. そして敵対的送信者に関するさまざまな安全性定義をカバーできる安全性である平文拘束の定義を行う. また強秘匿の概念である IND-TR-CCA をこの設定で定義し, 平文拘束および IND-TR-CCA を実現する汎用構成戦略を考える. 最後に DLIN 仮定および強偽造不可能 One-Time 署名の存在の元で, 平文拘束および IND-TR-CCA が証明できる検証可能時限式暗号の効率的実装方法を提案する.

キーワード Functional Encryption, Timed-Release Encryption, Identity-Based Encryption, Attribute-Based Encryption, Predicate Encryption

1 はじめに

1.1 時限式暗号

時限式暗号 (timed-release encryption, TRE) は 1993 年 Timothy May によって初めて議論された特殊な暗号で, 暗号文の正規の受信者であっても, 送信者が指定した開封時刻 (release time) になるまで暗号文が復号できないような暗号のことである [28]. Blake ら, Cheon らおよび Yoshida らのそれぞれの研究グループが 2004 年のほぼ同時期に pairing を用いた構成手法を提案して以来, 信頼できる時報局 (time-server) がユーザと対話せずに, 時報トークンを放送するタイプの時限式暗号が盛んに研究されている [3, 8, 9, 10, 11, 12, 13, 15, 21, 22, 25, 26, 30, 31]. 時限式暗号の安全性の定義は大雑把に捉えると

(0) 部外者に対する秘匿
(1) 時報局に対する秘匿
(2) 開封時刻前の受信者に対する秘匿

の 3 つが良く研究されている. (0) は (1) に含まれており, (1) を考慮すれば自動的に (0) の対策になる事が分かっている [15]. (1) を実現するには送信者と受信者の間に安全な通信路が確立されていれば良い. 暗号学的に安全な通信路は公開鍵暗号や CLE (certificateless encryption) を使って実現する事が出来る. 時限式暗号 (時限式暗号) と云った時 (0)〜(2) のすべてを実現する方式を指す事が多いが, 本稿では必要ならば暗号文の送信者と受信者の間に安全な通信路を仮定し, (2) を実現する機構に集中して議論を行う. 従って, 本稿では (2) を実現する方式を時限式暗号と呼び, 時限式暗号と区別する為に (0)〜(2) のすべてを実現する方式を時限式公開鍵暗号 (timed-release public key encryption, TRPKE) と呼ぶ事にする. 現在では時限式公開鍵暗号を実現する様々な効率の良い構成法が良く知られており, さらに開封時刻秘匿 (release time confidentiality) といった安全性や時間前開封機能 (pre-open capability) なる機能の研究も行われている [11, 13, 22, 21, 26]. 本稿の手法を時限式公開鍵暗号に応用する事は容易である.

* 日本電信電話株式会社 情報流通プラットフォーム研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Information Sharing Platform Laboratories, NTT Corporation, 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan

時報トークン放送型の時限式暗号を実現する基本的なアイディアは, 時刻を識別子 (identity, ID) とした ID ベース暗号 (identity-based encryption, IBE) を用いる所にある. ID ベース暗号とは, 公開鍵の照会といった予備通信を必要とせず受信者識別子を公開鍵として暗号化が可能な公開鍵暗号系のことであり, 一般にセットアップ $\mathtt{Setup}$, 鍵生成 $\mathtt{KeyGen}$, 暗号化 $\mathtt{Enc}$, 復号 $\mathtt{Dec}$ の 4 つのアルゴリズムから構成される. そして, セットアップ, 鍵生成, 暗号化が正常に行われた場合, 復号結果が圧倒的確率で元の平文と一致する時, その ID ベース暗号を正当 (correct) であると云う. 正当 (で安全) な ID ベース暗号 ($\mathtt{Setup}$, $\mathtt{KeyGen}$, $\mathtt{Enc}$, $\mathtt{Dec}$) が利用可能な時, 以下のようにして時限式暗号を得ることが出来る.

- 最初に時報局は $\mathtt{Setup}(1^\lambda)$ を呼んで公開パラメタ P とマスター鍵 K を生成し, P を公開する.
- 送信者は開封時刻 t_r と平文 m に対して $\mathtt{Enc}(P, t_r, m)$ を呼んで暗号文 c_{t_r} を生成し, 受信者に送信する.
- 時刻 t に時報局は $\mathtt{KeyGen}(K, t)$ を呼んで時報トークン k_t を生成し放送する.
- 受信者は時報局より時刻 t_r の時報トークン k_{t_r} を得て, $\mathtt{Dec}(k_{t_r}, c_{t_r})$ を呼んで平文 m を得る.

Naor の IBE-to-Signature 変換 [4] を考えれば, 時報トークン k_t は直ちに時刻 t に対する時報局の署名と考えることが出来る. 時報トークンの受信者は, この署名の検証手続きを行う事により時報トークン k_t が時報局から送られてきたのか否かを判定できる. 簡単の為本稿ではこの署名の検証手続きの記述は全て省略するが, 本稿の時限式暗号でも全く同様の事が出来る.

1.2 関数型暗号

近年, 関数型暗号 (Functional Encryption, FE) なる, ID ベース暗号の拡張が話題となっている. 関数型暗号と ID ベース暗号には構文の違いは無い. 即ち関数型暗号も以下の 4 つのアルゴリズム

- $\mathtt{Setup}(1^\lambda) \xrightarrow{\$} (P, K)$: セットアップ - セキュリティパラメータ 1^λ を入力とし公開パラメタ P とマスター鍵 K を出力する確率的多項式時間アルゴリズム.
- $\mathtt{KeyGen}(K, x) \xrightarrow{\$} k_x$: 鍵生成 - マスター鍵 K と文字列 x を入力とし, その文字列 x に対応する秘密鍵 k_x を出力する確率的多項式時間アルゴリズム.
- $\mathtt{Enc}(P, y) \xrightarrow{\$} c_y$: 暗号化 - 公開パラメタ P と文字列 y を入力とし, 暗号文 c_y を出力する確率的多項式時間アルゴリズム.
- $\mathtt{Dec}(k_x, c_y) \xrightarrow{\$} m$: 復号 - 秘密鍵 k_x と暗号文 c_y を入力とし, 文字列 m を出力する確率的多項式時間アルゴリズム.

から構成される. 関数型暗号では, 正当性が ID ベース暗号に比べて拡張されており, 暗号文の受信者は $\mathtt{KeyGen}$ の入力文字列 x に対応する秘密鍵 k_x と $\mathtt{Enc}$ の入力文字列 y に対応する暗号文 c_y から何らかの関数 $f(x, y)$ を評価する事が出来るようになっている. 即ち, ある関数 $f(\cdot, \cdot)$ が存在し $\forall x, \forall y \in \{0,1\}^{\mathtt{poly}(\lambda)}$ に対して

$$\Pr\left[\, m = f(x,y) \;\middle|\; \begin{array}{l} (P, K) \xleftarrow{\$} \mathtt{Setup}(1^\lambda); \\ k_x \xleftarrow{\$} \mathtt{KeyGen}(K, x); \\ c_y \xleftarrow{\$} \mathtt{Enc}(P, y); \\ m \xleftarrow{\$} \mathtt{Dec}(k_x, c_y); \end{array} \right]$$

なる確率が λ に関して圧倒的 (overwhelming) であるとき, 関数型暗号 ($\mathtt{Setup}, \mathtt{KeyGen}, \mathtt{Enc}, \mathtt{Dec}$) は f に関し正当であると云う [6, 27]. 特に, ある関係 $R(\cdot, \cdot)$ が存在し,

$$f(i, j \| m) = \begin{cases} m & (R(i,j) = 1 \text{ の時}) \\ \perp & (R(i,j) = 0 \text{ の時}) \end{cases}$$

なる型の f を持つ関数型暗号類 (sub-class of functional encryption) は様々な暗号を包含している [6, 27, 24, 20]. 例えば

$$f(i, j \| m) = \begin{cases} m & (i = j \text{ の時}) \\ \perp & (i \neq j \text{ の時}) \end{cases}$$

を利用して ID ベース暗号を関数型暗号の一種として再定義する事ができる. 一般的な ID ベース暗号の正当性では復号アルゴリズム $\mathtt{Dec}$ に $i \neq j$ なる秘密鍵と暗号文を入力したとき, どのような出力が得られるか定義されない. 出力 $\perp$ の意味をどのように捉えるか明確でない事もあるが, ここでは定義どおりに $\perp$ という特殊記号が出力されるとする. $\perp$ は $\mathtt{Enc}$ の入力平文空間には存在せず $\mathtt{Dec}$ の出力平文空間にのみ存在するとする. 一般的な ID ベース暗号の定義には無い入出力仕様が定義されるので, 幾らか強い定義となる.

より高度な R を持つ関数型暗号類が研究されており, その中でも汎用性の高いものとして属性ベース暗号 (attribute-based encryption, ABE) あるいは述語暗号 (predicate encryption, PE) 等がよく研究されている. i を述語, j を述語変数のインスタンスとして,

$$f(i, j \| m) = \begin{cases} m & (j \text{ が述語 } i \text{ を充足する時}) \\ \perp & (j \text{ が述語 } i \text{ を充足しない時}) \end{cases}$$

なる f を持つ関数型暗号は KP-ABE (key-policy attribute-based encryption) と呼ばれる. j を述語, i を述語変数のインスタンスとして,

$$f(i, j \| m) = \begin{cases} m & (i \text{ が述語 } j \text{ を充足する時}) \\ \perp & (i \text{ が述語 } j \text{ を充足しない時}) \end{cases}$$

なる f を持つ関数型暗号は CP-ABE (ciphertext-policy attribute-based encryption) と呼ばれる. $\mathtt{Enc}$ の入力

$j\|m$ に関して, 平文 m の秘匿を payload-hiding, 受信者識別子 j の秘匿を attribute-hiding と呼ぶ. 2005 年頃から, このような高機能な暗号が様々な名称で導入されており, それらを統一的に解釈する定式化として関数型暗号の概念が研究されている [6].

2010 年に岡本らは標準的な暗号学的仮定の下, 選択暗号文攻撃に対し適応的 payload-hiding (CCA-PH) (即ち fully secure) が証明できる汎用的な関数型暗号 (属性ベース暗号) を提案したが, それ以前にはそのような安全性を達成した方式は知られていなかった [24]. 本稿では, そうした特に汎用性が高く, 高度な情報処理機能を実現できる関数型暗号を時限式暗号に応用する事を考える.

1.3 関数型暗号に基づく時限式暗号

ID ベース暗号に基づく時限式暗号の素朴な構成で先ず問題となるのは, 時報局が放送した開封時刻の時報トークン k_{t_r} を受信できなかった場合, 暗号が復号出来ないことである. 時報局が時報トークンを保存したりユーザと対話するなどの手段を用いなければ, ID ベース暗号を用いた構成でこの問題に対処するのは自明な事では無い. 2005 年頃にはこの問題への対処が良く研究され様々な解が提案されている [9, 31, 25].

ところで指定時刻以降に放送された時報トークンが, そのまま復号に利用できれば, こうした問題は起こらない. 現在では安全で比較的効率的で汎用性の高い関数型暗号が利用できるので, この問題に対してはずっと簡単で汎用的な解が存在する. 即ち, t を現在時刻, t_r を開封時刻として

$$f(t, t_r\|m) = \begin{cases} m & (t \geq t_r \text{の時}) \\ \perp & (t < t_r \text{の時}) \end{cases}$$

なる f を持つ関数型暗号があれば良い. 現在時刻 t が開封時刻 t_r より小さい時は復号時に $\perp$ が出力され, t_r 以上の時は平文 m が出力される. ID ベース暗号とこの関数型暗号の構文は完全に一致するので, 同じような安全性を持つなら, 前述の時限式暗号の構成で ID ベース暗号の代わりに関数型暗号を利用しても全く問題ない. 属性ベース暗号を用た大小比較の実現は良く知られており [2], 適応的安全性が証明できる [24] でも同じ技法が利用可能な為, こうした $f(t, t_r\|m)$ を持つ安全な関数型暗号は容易に実現できる. 詳細は附録を参照のこと. この構成は一般的な時限式暗号よりは演算コストが幾分大きいが, 少なくとも参加者が全員正直なら, 時刻 $t \geq t_r$ 以降に時報局から放送される指数的多数の如何なる時報トークンを使用しても暗号文 c_{t_r} が復号出来る十分実用的な時限式暗号が構成できる. 関数型暗号の構文は ID ベース暗号と全く同じなので, この構成を時限式公開鍵暗号に応用する事も容易である. こうした, 関数型暗号を属性ベース暗号に基づいて構成する方法は 2 通り存在する. 一つは KP-ABE を用いる方法である. この場合, 時報局は, t を現在時刻, T を述語変数として $t \geq T$ なる述語 (鍵識別子) に関して時報トークン k_t を発行する. 暗号文の送信者は目的の開封時刻 t_r を属性に持つ暗号文 c_{t_r} を生成する. もう一つは CP-ABE を用いる方法である. この場合, 時報局は, 現在時刻 t を属性に持つ時報トークン k_t を発行する. 暗号文の送信者は T を述語変数, t_r を開封時刻として $T \geq t_r$ なる述語 (受信者識別子) に関して暗号文 c_{t_r} を生成する. いずれの場合も時報トークン k_t および暗号文 c_{t_r} を持つ受信者は $t \geq t_r$ なる時, 暗号文を復号できる.

1.4 問題点

上記のような時限式暗号の構成に関し, 暗号の送信者が攻撃者となるシナリオについて以下で考察する.

【平文保証】 本稿のような時限式暗号の構成では (ID ベース暗号による構成も含めて) 暗号文を貰った受信者は, 復号するまで, 平文が本当に意味ある面白い情報であるか否かを知りようが無い. 受信者は暗号文を貰ってから時報トークンが放送されるまでの間, 長い間待たされるが, いざ開封時刻に時報トークンを得て復号を実行してみると, 復号に失敗したり出てきた平文がつまらない乱数だったりする事が往々にして起こりうる. 時報トークンを手に入れる前にそうした失敗が分からない場合は, 復号時に大いに興が削がれ, その落胆は計り知れない.

【開封時刻抽出可能性】 $t < t_r$ なる時報トークン k_t を使用して復号を行った場合に, 一般的な ID ベース暗号の正当性の定義ではその動作は定義されない. 受信者にとって復号結果が目的の平文と区別が付くか否かと云った問題は, 安全性の定義から定理として導かれる事はあっても, 必ずしも明確ではない. 一方, 関数型暗号の定義では, 任意の (正しく作成された) 暗号文と鍵のペアに対して, 復号アルゴリズムの出力が明確に定義される. 従って少なくとも参加者が全員正直なら, 開封時刻以降の時報トークンが手に入った時点での復号結果とそれ以前の復号結果は明確に区別できる. では, 開封時刻以降の時報トークンを入手する前にその時刻を知ることが出来るだろうか? あるいはそうして入手した時刻以降に復号を行った時必ず価値ある平文が入手出来るであろうか? せっかく面白い平文の入った暗号文を貰っても, 未来永劫開封出来ないのでは意味がない. 鍵を入手する前に開封時刻が確信出来ることが望ましい [14].

【平文拘束性】 $t \geq t_r$ の如何なる t についても, 正しく復号できるか否かは良く分らない. $t \geq t_r$ なる, ある時刻では復号結果 m が得られ, 他の時刻では別の復号結果 m' $(\neq m)$ が得られるというような状況は望ましくない. 時限式暗号は一種のコミットメントであり, どの時

刻でも復号結果が等しい事が求められる. 従来時間前開封機能を持つ時限式暗号では平文の拘束性が研究されてきたが, 本稿の構成のようなもっと素朴な時限式暗号でも, この安全性を取り扱う必要がある. さらに受信者が開封時刻前に平文の拘束を納得できる事が望ましい.

2 定義

2.1 モデル

(時間前開封機能付き) 時限式公開鍵暗号の設定で暗号文の正規の受信者に対する安全性を考える時, 時報局を信頼できる第三者と考え, 如何なる暗号文も開封時刻前に勝手に復号される事は無いとする事が多い [15, 22, 21]. 時限式公開鍵暗号の設定では, 暗号文には必ず対象となる個別の受信者 (ターゲットユーザ) が存在し, そうした受信者と時報局が結託して開封時刻前に暗号文を復号する事は攻撃としては意味を持たないと考えられている. 従って正規の受信者に対する平文の秘匿に関しては CPA で十分とされる [15]. この設定では時報局とユーザは鍵生成を正しく実行する事が求められ rogue key attack [19] のような攻撃は許されないし, ターゲットユーザの偽造といった攻撃も許されない. 従って攻撃的受信者が自分宛に送られたチャレンジ暗号文を他人宛ての暗号文に変換し, そうした暗号文が時間前に復号されるといった状況は考慮していない.

一方, 本稿の時限式暗号の設定ではターゲットユーザの概念そのものが存在しない. 暗号文の正規の受信者に対する安全性を考える時, やはり時報局は信頼できるとし, 必要なら送信者と受信者の間に安全な通信路を仮定するが, 安全な通信路を用いずに公開掲示板などを利用して一般に公開される暗号文が存在すると仮定する. そして攻撃者は未来の時報トークンを手に入れる事は出来ないが, 時報局に対して公開された暗号文を開封時間前に復号するよう命令出来るとする. 即ち攻撃的受信者は暗号文を公開することと引き換えに, 未来の時刻に関する復号オラクルが利用できるとする. このような状況では正規の受信者に対する平文の秘匿であっても CPA では不十分であり CCA を考える必要がある. 時限式公開鍵暗号の IND-CTCA[8] の設定に近いが, ターゲットユーザの概念は無い.

また, 本稿では送信者が攻撃者となり得るシナリオについて考察するので, 悪意ある送信者に対する安全性を考える必要がある. 受け取った暗号文に含まれる平文が期待はずれであるか否かを科学的に定義する事は容易では無いが, 簡単のため面白さの傾向は受信者に依存せず一意に決まっており, 面白い平文は誰が見ても面白いと仮定する. また, 受信者が平文を見たとき, その平文が面白いのか面白くないのかよく分らないという状況はここでは考えない事とする. そうした平文はつまらないと断罪し, 面白さの判定は効率的に行えると仮定する. 即ち, 面白い平文 x は何らかの言語 $L \in \mathbf{P}$ に所属すると考え, L は事前に分かっているとする. また明らかに詰らない平文 $\perp$ は L に属さないとし, 簡単のため L に属さない平文は $\perp$ と同一視して考える.

2.2 構文

以下の 6 つのアルゴリズムの組 ($\mathtt{Setup}$, $\mathtt{KeyGen}$, $\mathtt{Enc}$, $\mathtt{Verify}$, $\mathtt{Ext}$, $\mathtt{Dec}$) を検証可能時限式暗号 (verifiable timed-release encryption) と呼ぶ.

- $\mathtt{Setup}(1^\lambda) \xrightarrow{\$} (P, K)$: セットアップ - セキュリティパラメータ 1^λ を入力とし公開パラメタ P とマスター鍵 K を出力する確率的多項式時間アルゴリズム.
- $\mathtt{Enc}(P, t_r, m) \xrightarrow{\$} c$: 暗号化 - 公開パラメタ P と開封時刻識別子 t_r と平文 m を入力とし, 暗号文 c を出力する確率的多項式時間アルゴリズム.
- $\mathtt{Verify}(P, c) \xrightarrow{\$} b$: 検証 - 公開パラメタ P と暗号文 c を入力とし, 平文がある面白い言語 $L \in \mathbf{P}$ に属するか否かの判定 $b \in \{0, 1\}$ を出力する確率的多項式時間アルゴリズム.
- $\mathtt{Ext}(P, c) \xrightarrow{\$} t$: 開封時刻抽出 - 公開パラメタ P と暗号文 c を入力とし, 暗号文の最小復号可能時刻 t_e を出力する確率的多項式時間アルゴリズム.
- $\mathtt{KeyGen}(K, t) \xrightarrow{\$} k$: 鍵生成 - マスター鍵 K と鍵時刻識別子 t を入力とし, t に対応する時刻鍵 k を出力する確率的多項式時間アルゴリズム.
- $\mathtt{Dec}(k, c) \xrightarrow{\$} m'$: 復号 - 時刻鍵 k と暗号文 c を入力とし, 平文 m' を出力する確率的多項式時間アルゴリズム.

2.3 正当性

検証可能時限式暗号の正当性について, 次のように定義する. 任意の $t, t_r \in \{0,1\}^{\mathtt{poly}(\lambda)}, m \in L$ に対して

$$\Pr\left[\begin{array}{l|l} & (P, K) \xleftarrow{\$} \mathtt{Setup}(1^\lambda); \\ (b = 1) \wedge & c \xleftarrow{\$} \mathtt{Enc}(P, t_r, m); \\ (t_e = t_r) \wedge & b \xleftarrow{\$} \mathtt{Verify}(P, c); \\ ((t \geq t_r \wedge m' = m) \vee & t_e \xleftarrow{\$} \mathtt{Ext}(P, c); \\ \quad (t < t_r \wedge m' = \perp)) & k \xleftarrow{\$} \mathtt{KeyGen}(K, t); \\ & m' \xleftarrow{\$} \mathtt{Dec}(k, c); \end{array}\right]$$

なる確率が λ に関し圧倒的である時, その検証可能時限式暗号を正当であると呼ぶ.

2.4 平文保証

平文保証は, 暗号文を復号した時平文が L に入っている事を保証する為の安全性定義である. $\mathcal{A}$ を攻撃者とし

て $\mathrm{Adv}^{\mathtt{guarantee}}_{\mathcal{A},t}(\lambda)$ を

$$\mathrm{Adv}^{\mathtt{guarantee}}_{\mathcal{A},t}(\lambda) = \Pr\left[\begin{array}{l|l} & (P,K) \xleftarrow{\$} \mathtt{Setup}(1^\lambda); \\ & c \xleftarrow{\$} \mathcal{A}(P,K); \\ (b=1) \wedge & b \xleftarrow{\$} \mathtt{Verify}(P,c); \\ (t \geq t_e \wedge m \notin L) & t_e \xleftarrow{\$} \mathtt{Ext}(P,c); \\ & k \xleftarrow{\$} \mathtt{KeyGen}(K,t); \\ & m \xleftarrow{\$} \mathtt{Dec}(k,c); \end{array}\right]$$

と定義する. 如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ および如何なる時刻 t に対しても $\mathrm{Adv}^{\mathtt{guarantee}}_{\mathcal{A},t}(\lambda)$ が λ に関する無視可能関数である時, その検証可能時限式暗号を言語 L に関して平文保証であると呼ぶ.

2.5 開封時刻抽出可能性

開封時刻抽出可能性は, 暗号文から Ext アルゴリズムによって抽出した開封時刻 t_e が, 本当に最小の復号可能時間である事を保証する為の安全性定義である. $\mathcal{A}$ を攻撃者として $\mathrm{Adv}^{\mathtt{ext}}_{\mathcal{A},t}(\lambda)$ を

$$\mathrm{Adv}^{\mathtt{ext}}_{\mathcal{A},t}(\lambda) = \Pr\left[\begin{array}{l|l} & (P,K) \xleftarrow{\$} \mathtt{Setup}(1^\lambda); \\ & c \xleftarrow{\$} \mathcal{A}(P,K); \\ (b=1) \wedge & b \xleftarrow{\$} \mathtt{Verify}(P,c); \\ ((t \geq t_e \wedge m \notin L) \vee & t_e \xleftarrow{\$} \mathtt{Ext}(P,c); \\ (t < t_e \wedge m \in L)) & k \xleftarrow{\$} \mathtt{KeyGen}(K,t); \\ & m \xleftarrow{\$} \mathtt{Dec}(k,c); \end{array}\right]$$

と定義する. 如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ および如何なる時刻 t に対しても $\mathrm{Adv}^{\mathtt{ext}}_{\mathcal{A},t}(\lambda)$ が λ に関する無視可能関数である時, その時限式暗号を開封時刻抽出可能と呼ぶ.

系 1 上記の定義で検証可能時限式暗号が開封時刻抽出可能なら平文保証であるが, 平文保証であっても開封時刻抽出可能とは限らない.

2.6 平文拘束性

自然な平文拘束性の定義では 2 つの復号時刻 t_1, t_2 における平文の等しさに関する安全性を検討しなくてはならない. 一般性を失わず $t_1 < t_2$ として良い. Ext によって暗号文から抽出された開封時刻 t_e と t_1, t_2 の大小に関して 3 つの場合を考える事が出来る.

(1) $t_e \leq t_1 < t_2$ の場合.
(2) $t_1 < t_2 < t_e$ の場合.
(3) $t_1 < t_e \leq t_2$ の場合.

時刻 t_1 に開封した平文を m_1, 時刻 t_2 に開封した平文を m_2 とすると. (1) の場合は平文拘束を最も自然な形 $m_1 = m_2$ で定義できる. (2) の場合は $m_i \notin L$ ではあるが, 平文拘束の概念を幾分拡張すれば, やはり $m_1 = m_2$ で定義できる. (3) のような場合はそもそも $m_1 \neq m_2$ であるので, 拘束の概念を幾分超えるかもしれないが $m_1 \notin L$ でかつ $m_2 \in L$ を平文拘束の定義として考えることにする. 以下では, こうした拡張概念を取り入れた形で平文拘束の定義を行う. $t_1 < t_2$ を仮定し $\mathcal{A}$ を攻撃者として $\mathrm{Adv}^{\mathtt{bind}}_{\mathcal{A},t_1,t_2}(\lambda)$ を

$$\mathrm{Adv}^{\mathtt{bind}}_{\mathcal{A},t_1,t_2}(\lambda) = \Pr\left[\begin{array}{l|l} & (P,K) \xleftarrow{\$} \mathtt{Setup}(1^\lambda); \\ & c \xleftarrow{\$} \mathcal{A}(P,K); \\ (b=1) \wedge & b \xleftarrow{\$} \mathtt{Verify}(P,c); \\ ((t_2 \geq t_e \wedge m_2 \notin L) \vee & t_e \xleftarrow{\$} \mathtt{Ext}(P,c); \\ (t_1 < t_e \wedge m_1 \in L) \vee & k_1 \xleftarrow{\$} \mathtt{KeyGen}(K,t_1); \\ ((t_1 \geq t_e \vee t_2 < t_e) \wedge & k_2 \xleftarrow{\$} \mathtt{KeyGen}(K,t_2); \\ (m_1 \neq m_2))) & m_1 \xleftarrow{\$} \mathtt{Dec}(k_1,c); \\ & m_2 \xleftarrow{\$} \mathtt{Dec}(k_2,c); \end{array}\right]$$

と定義する. 如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ および如何なる $t_1 < t_2$ なる時刻 t_1, t_2 に対しても $\mathrm{Adv}^{\mathtt{bind}}_{\mathcal{A},t_1,t_2}(\lambda)$ が λ に関する無視可能関数である時, その検証可能時限式暗号を平文拘束と呼ぶ.

系 2 上記の定義で検証可能時限式暗号が平文拘束なら開封時刻抽出可能であるが, 開封時刻抽出可能であっても平文拘束とは限らない.

従って, 上記の定義では平文保証, 開封時刻抽出可能性, 平文拘束の 3 つのうち平文拘束のみを考えれば良い.

2.7 IND-TR-CCA

D, E をそれぞれオラクル照会履歴保存用テーブルとして, 復号オラクル $\mathcal{O}_d$, 鍵生成オラクル $\mathcal{O}_k$, チャレンジオラクル $\mathcal{O}_c^{(b)}$, をそれぞれ

$$\begin{array}{l} \mathcal{O}_d(t,c) := \{\ D[c] \xleftarrow{\cup} \{t\};\ \mathtt{return\ Dec}(\mathtt{KeyGen}(K,t),c);\ \} \\ \mathcal{O}_k(t) := \{\ E \xleftarrow{\cup} \{t\};\ \mathtt{return\ KeyGen}(K,t);\ \} \\ \mathcal{O}_c^{(b)}(t,x_0,x_1) := \mathtt{if}\ \ (c^* = \perp)\ \{ \\ \quad t^* \leftarrow t;\ c^* \xleftarrow{\$} \mathtt{Enc}(P,t,x_b);\ \mathtt{return}\ c^*; \\ \} \end{array}$$

と定義し, $\mathcal{A}$ を攻撃者として実験 $\mathrm{Exp}^{\mathtt{IND\text{-}TR\text{-}CCA}}_{\mathcal{A}}(\lambda)$ を

$$\begin{array}{l} \mathrm{Exp}^{\mathtt{IND\text{-}TR\text{-}CCA}}_{\mathcal{A}}(\lambda) := \\ \quad \mathtt{clear}\ D,E;\ t^* \leftarrow \infty;\ c^* \leftarrow \perp; \\ \quad (P,K) \xleftarrow{\$} \mathtt{Setup}(1^\lambda); \\ \quad b \xleftarrow{\$} \{0,1\};\ b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_d,\mathcal{O}_k,\mathcal{O}_c^{(b)}}(P); \\ \quad \mathtt{if}\ \ (t^* \leq \max(D[c^*] \cup E \cup \{-\infty\}))\ b' \xleftarrow{\$} \{0,1\}; \\ \quad \mathtt{return}\ \ b \stackrel{?}{=} b'; \end{array}$$

と定義し, 標本空間を $\mathrm{Exp}_{\mathcal{A}}^{\texttt{IND-TR-CCA}}(\lambda)$ に与えるランダムテープの空間として攻撃者の利得 $\mathrm{Adv}_{\mathcal{A}}^{\texttt{IND-TR-CCA}}(\lambda)$ を

$$\mathrm{Adv}_{\mathcal{A}}^{\texttt{IND-TR-CCA}}(\lambda) = 2\Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\texttt{IND-TR-CCA}}(\lambda) = 1\right] - 1$$

とする. 如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても $\mathrm{Adv}_{\mathcal{A}}^{\texttt{IND-TR-CCA}}(\lambda)$ が λ に関する無視可能関数である時, その時限式暗号 は IND-TR-CCA を満たすという. 一般に ID ベース暗号に基づく時限式暗号の構成では攻撃者はチャレンジオラクルに指定した時刻 t^* の時刻鍵を鍵生成オラクルに聞く事が許されない. 自明なことではあるが, 本稿の関数型暗号ベースの構成では, 攻撃者はチャレンジオラクルに指定した時刻 t^* 以降の如何なる時刻鍵をも鍵生成オラクルに聞く事は許されないし, チャレンジ暗号文に関してはそうした時刻鍵を指定して復号オラクルを呼ぶことも許されない.

3 具体的構成法

3.1 汎用構成法

平文が L に属しているので, 正しい暗号文は r を $\texttt{Enc}$ のランダムテープ, R をその空間として

$$C_t = \{c \mid m \in L; r \in R;\ c \leftarrow \texttt{Enc}(P, t, m; r)\}$$

なる言語 $C_t \in \mathbf{NP}$ に属している. これを言語の非対話零知識証明 [16] で証明する事を考える.

(1) 適応的 payload-hiding (CCA-PH) な属性ベース暗号の述語として述語変数と定数の大小比較を実装した関数型暗号を構成する.
(2) 暗号文に付随する受信者識別子 (時刻)t(属性または述語) を抽出可能にする (例えば添付する).
(3) 暗号文が言語 C_t に所属する非対話零知識証明を暗号文に添付する.

なる検証可能時限式暗号の汎用構成法を考えることが出来る. 一般の $L \in \mathbf{P}$ に関する非対話零知識証明を行うためには, 汎用の非対話零知識証明を用いれば良い. 二重暗号化の手法 [23] あるいは知識の非対話零知識証明 [29] を使用して復号オラクルをシミュレートするなら, (適応的) CPA-PH の関数型暗号でも十分である.

3.2 効率的方式

汎用の非対話零知識証明は多項式時間であるとはいえ, 実装面で効率が悪い. 以下では, 実装に特化した効率の良い方式を考える. 簡単のため最も単純な L として仕様する属性ベース暗号の $\texttt{Dec}$ の出力平文空間から $\perp$ を除いたもの, 即ち $L = \overline{\{\perp\}}$ を考える. CCA-PH な属性ベース暗号として [24] を採用する. このとき, CCA-PH な属性ベース暗号を得る方法は CHK 変換 [7] に基づく方法と BK 変換 [5] に基づく方法の 2 通りがある. BK 変換に基づく方法の方が属性ベース暗号としての演算コストは有利であるが, public-verifiability が無いので非対話零知識証明が面倒となる. 一方 CHK 変換に基づく方法は public-verifiability を持つので, これを利用する.

(1) [24] の KP-ABE に [2] を適用し整数変数と定数の大小比較に基づく関数型暗号を実現する.
(2) 上記の関数型暗号に publicly-verifiable な CCA 変換 (CHK 変換) を施す [24].
(3) 使用した乱数をコミットし暗号文が抽出時刻で正しく暗号化された暗号文の集合に所属している事を非対話零知識証明で証明する (DLIN ベースの GS-proof (linear multi-scalar multiplication))[18].

4 安全性

4.1 Decisional Linear Assumption (DLIN)

簡単の為以下では対称ペアリングを用いるとする. 非対称ペアリングで GS-proof を用いる時の同様の仮定については [17] を参照のこと. $\mathcal{G}(1^\lambda)$ を対称ペアリングパラメタ生成アルゴリズムとする. $\mathcal{A}$ を攻撃者として実験 $\mathrm{Exp}_{\mathcal{A}}^{\texttt{dlin}}(\lambda)$ を

$$\begin{aligned}
&\mathrm{Exp}_{\mathcal{A}}^{\texttt{dlin}}(\lambda) := \\
&\quad (q, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{\$} \mathcal{G}(1^\lambda); \\
&\quad (P_1, P_2, P_3) \xleftarrow{\$} \mathbb{G}^3;\ (a_1, a_2, a_3) \xleftarrow{\$} (\mathbb{F}_q)^3; \\
&\quad c_0 \leftarrow (P_1, P_2, P_3, a_1P_1, a_2P_2, a_3P_3); \\
&\quad c_1 \leftarrow (P_1, P_2, P_3, a_1P_1, a_2P_2, (a_1+a_2)P_3); \\
&\quad b \xleftarrow{\$} \{0,1\};\ b' \xleftarrow{\$} \mathcal{A}(c_b); \\
&\quad \texttt{return}\ b \stackrel{?}{=} b';
\end{aligned}$$

と定義し, 標本空間を $\mathrm{Exp}_{\mathcal{A}}^{\texttt{dlin}}(\lambda)$ に与えるランダムテープの空間として攻撃者の利得 $\mathrm{Adv}_{\mathcal{A}}^{\texttt{dlin}}(\lambda)$ を

$$\mathrm{Adv}_{\mathcal{A}}^{\texttt{dlin}}(\lambda) = 2\Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\texttt{dlin}}(\lambda) = 1\right] - 1$$

とする. 以下では次を仮定する.

仮定 1 (DLIN 仮定) 如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても $Adv_{\mathcal{A}}^{dlin}(\lambda)$ は λ に関する無視可能関数である.

仮定 2 (CHK 変換用) 強偽造不可能 *One-Time* 署名が存在する.

以下の定理を参照する.

定理 1 ([24]) 強偽造不可能 *One-Time* 署名が存在するとき *DLIN* 仮定の下適応的 *CCA-PH (fully secure)* な *KP-ABE* および *CP-ABE* が存在する.

定理 2 ([18]) *DLIN* 仮定の下, 効率的な *(quadratic) multi-scalar multiplication* に関する非対話零知識証明が存在する.

4.2 提案法の安全性

上記の仮定の元, 提案の検証可能時限式暗号は言語 $L = \overline{\{\perp\}}$ に関して次の性質を満たす.

定理 3 提案法は平文拘束性を満たす.

検証可能時限式暗号が正当性を満たし, 暗号文が正しく暗号化されるならその暗号文の平文は拘束される. 従って暗号文が必ず C に属するなら, その検証可能時限式暗号は平文拘束である. もし敵対的送信者が受信者に暗号文が C に属する事を納得させつつ, 平文拘束を破るなら, 非対話零知識証明の健全性が破られる.

定理 4 提案法は *IND-TR-CCA* を満たす.

提案法の IND-TR-CCA をベースとなる属性ベース暗号の CCA-PH に帰着させる. 復号オラクルへの照会は非対話零知識証明の部分を削って CCA-PH の攻撃環境に転送し, 戻り値をそのまま $\mathcal{A}$ に返せば良い. 鍵生成オラクルへの照会はそのまま CCA-PH の攻撃環境に転送し, 戻り値をそのまま $\mathcal{A}$ に返せば良い. チャレンジオラクルへの照会はそのまま CCA-PH の攻撃環境に転送し, 戻り値にシミュレーションで生成された非対話零知識証明を付けて $\mathcal{A}$ に返せば良い.

5 結論

本論文では開封時刻以降に時報局より放送される指数的多数の如何なる時報トークンを使用しても暗号文が復号出来る時限式暗号について考察した. そのような時限式暗号を関数型暗号 (属性ベース暗号) を用いて容易に実現可能である事を示し, さらにそのような時限式暗号について, 敵対的送信者に関するさまざまな問題点を研究した. そして時限式暗号の拡張として検証可能時限式暗号の概念を提案し, 敵対的送信者に関するさまざまな安全性定義をカバーできる安全性である平文拘束の定義を行った. また強秘匿の概念である IND-TR-CCA をこの設定で定義し, 平文拘束および IND-TR-CCA を実現する汎用構成戦略を考え, DLIN 仮定および強偽造不可能 One-Time 署名の存在の元で, 言語 $L = \overline{\{\perp\}}$ に関する平文拘束および IND-TR-CCA が証明できる検証可能時限式暗号の効率的実装方法を提案した. より効率の良い検証可能時限式暗号の構成は今後の課題である.

参考文献

[1] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988.

[2] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07, pages 321–334, Washington, DC, USA, 2007. IEEE Computer Society.

[3] I. F. Blake and A. C.-F. Chan. Scalable, server-passive, user-anonymous timed release public key encryption from bilinear pairing. Cryptology ePrint Archive, Report 2004/211, 2004. `http://eprint.iacr.org/`.

[4] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[5] D. Boneh and J. Katz. Improved efficiency for cca-secure cryptosystems built using identity-based encryption. In A. Menezes, editor, *CT-RSA*, volume 3376 of *Lecture Notes in Computer Science*, pages 87–103. Springer, 2005.

[6] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. Cryptology ePrint Archive, Report 2010/543, 2010. `http://eprint.iacr.org/`.

[7] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In C. Cachin and J. Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 207–222. Springer, 2004.

[8] J. Cathalo, B. Libert, and J.-J. Quisquater. Efficient and non-interactive timed-release encryption. In S. Qing, W. Mao, J. Lopez, and G. Wang, editors, *ICICS*, volume 3783 of *Lecture Notes in Computer Science*, pages 291–303. Springer, 2005.

[9] K. Chalkias and G. Stephanides. Timed release cryptography from bilinear pairings using hash chains. In H. Leitold and E. P. Markatos, editors, *Communications and Multimedia Security*, volume 4237 of *Lecture Notes in Computer Science*, pages 130–140. Springer, 2006.

[10] A. C.-F. Chan and I. F. Blake. Scalable, server-passive, user-anonymous timed release cryptography. In *ICDCS*, pages 504–513. IEEE Computer Society, 2005.

[11] J. H. Cheon, N. Hopper, Y. Kim, and I. Osipkov. Timed-release and key-insulated public key encryption. Cryptology ePrint Archive, Report 2004/231, 2004. `http://eprint.iacr.org/`.

[12] J. H. Cheon, N. Hopper, Y. Kim, and I. Osipkov. Timed-release and key-insulated public key encryption. In G. D. Crescenzo and A. D. Rubin, editors, *Financial Cryptography*, volume 4107 of *Lecture Notes in Computer Science*, pages 191–205. Springer, 2006.

[13] J. H. Cheon, N. Hopper, Y. Kim, and I. Osipkov. Provably secure timed-release public key encryption. *ACM Trans. Inf. Syst. Secur.*, 11:4:1–4:44, May 2008.

[14] G. D. Crescenzo, R. Ostrovsky, and S. Rajagopalan. Conditional Oblivious Transfer and Timed-Release Encryption. In *EUROCRYPT*, pages 74–89, 1999.

[15] A. W. Dent and Q. Tang. Revisiting the security model for timed-release encryption with pre-open capability. In J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta, editors, *ISC*, volume 4779 of *Lecture Notes in Computer Science*, pages 158–174. Springer, 2007.

[16] U. Feige, D. Lapidot, and A. Shamir. Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract). In *FOCS*, volume I, pages 308–317. IEEE, 1990.

[17] E. Ghadafi, N. P. Smart, and B. Warinschi. Groth-sahai proofs revisited. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 177–192. Springer, 2010.

[18] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2008.

[19] P. Horster, M. Michels, and H. Petersen. Meta-multisignature schemes based on the discrete logarithm problem, 1994.

[20] 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 H. Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2010.

[21] T. Matsuda, Y. Nakai, and K. Matsuura. Efficient generic constructions of timed-release encryption with pre-open capability. In M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 225–245. Springer, 2010.

[22] Y. Nakai, T. Matsuda, W. Kitada, and K. Matsuura. A generic construction of timed-release encryption with pre-open capability. In T. Takagi and M. Mambo, editors, *IWSEC*, volume 5824 of *Lecture Notes in Computer Science*, pages 53–70. Springer, 2009.

[23] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC*, pages 427–437. ACM, 1990.

[24] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2010.

[25] Y. Okamoto and T. Saito. A Timed-Release Public-Key Encryption with Recovery Signal. In *Computer Security Symposium 2008*, 2008.

[26] Y. Okamoto, T. Saito, and A. Fujioka. Generic Construction of Timed-Release Public-Key Encryption without One-Time Signature. SCIS 2010 The 2010 Symposium on Cryptography and Information Security Takamatsu, Japan, Jan. 19-22, 2C3-2, 2010.

[27] A. O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010. `http://eprint.iacr.org/`.

[28] R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical report, Cambridge, MA, USA, 1996.

[29] A. D. Santis and G. Persiano. Zero-knowledge proofs of knowledge without interaction (extended abstract). In *FOCS*, pages 427–436. IEEE, 1992.

[30] M. Yoshida, S. Mitsunari, and T. Fujiwara. Time-Capsule Encryption. *IEICE Technical Report*, ISEC2004-98:1–5, 2004.

[31] M. Yoshida, S. Mitsunari, and T. Fujiwara. A timed-release key management scheme for backward recovery. In D. Won and S. Kim, editors, *ICISC*, volume 3935 of *Lecture Notes in Computer Science*, pages 3–14. Springer, 2005.

A 大小比較 [2]

KP-ABE ベースの時限式暗号において述語変数 (開封時刻)T と定数 (鍵時刻)t との比較 ($T \leq t$) を実現する回路の生成方法を記述する. T は d ビットの変数とする. $t = 2^d - 1$ はほとんどマスター鍵と同じ意味なので不正な値とする. 述語変数 T および定数 t はそれぞれ述語変数 $T_i \in \{0,1\}$ および定数 $t_i \in \{0,1\}$ により

$$T = \sum_{i=1}^{d} T_i \cdot 2^{i-1}, \quad t = \sum_{i=1}^{d} t_i \cdot 2^{i-1}$$

と定義されるとする. 以下に比較回路合成アルゴリズムを示し, 結果例を図示する.

【比較回路合成アルゴリズム】

Step.0: $i = 1$ とする.

Step.1: $t_i = 1$ の間 $i \leftarrow i + 1$ とする.

Step.2: 原始述語 ($T_i = 0$) を根 (root edge) とする.

Step.3: $i = d$ なら $T \leq t$ の回路が完成して終了.

Step.4: $i \leftarrow i + 1$ とする.

Step.5: $t_i = 1$ なら or, $t_i = 0$ なら and で根と原始述語 ($T_i = 0$) を合成してその出力を新たな根として Step.3 に飛ぶ.

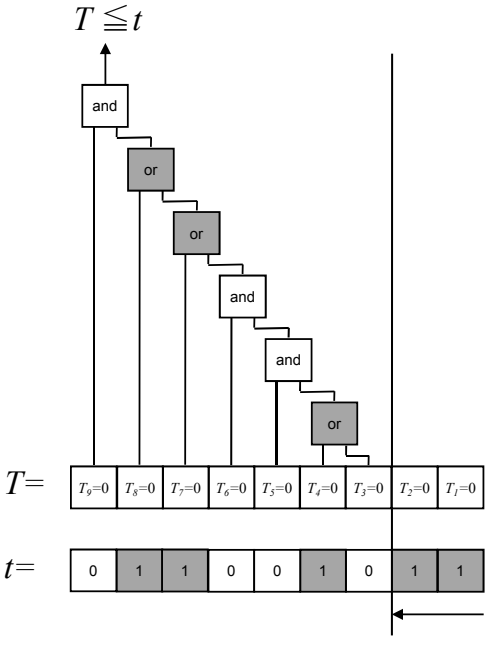

図 1: 述語変数 T と定数 t との比較回路

CP-ABE ベースの時限式暗号では述語変数 T と定数 t の不等号が逆転するが, 似たようなアルゴリズムで実装できる. 線形秘密分散の単調回路構成法は [1] 等を参照のこと.