情報処理学会論文誌 Vol.62 No.12 2060–2068 (Dec. 2021)

合成数位数双線形群を用いた復号時刻指定可能な階層的IDベース暗号の構成と安全性の検討

岸本 渡[1,a)] 榎本 雄介[1,†1]

受付日 2020年12月24日, 採録日 2021年9月9日

概要：Timed-Relase 暗号（TRE）は，暗号化の際に復号可能な時刻をあらかじめ指定できる暗号方式で，インターネットを介した新作映画の封切りや試験問題の配布などの応用が考えられる．合成数位数双線型群を用いて HIBE において復号可能時刻を指定できるようにした時限機能付階層的 ID ベース暗号方式（TRHIBE）の具体的構成法を提案した．さらに，提案方式はスタンダードモデルで選択平文攻撃に対して安全であることを示した．また，提案方式は，Boyen らの方法などを適用することにより，選択暗号文攻撃に対しても安全である方式に変換することが可能である．

キーワード：階層的 ID ベース暗号，復号時刻指定可能暗号，dual system encryption，合成位数双線形群

Timed-Release Hierarchical Identity Based Encryption Using Composite Order Bilinear Group

Wataru Kishimoto[1,a)] Yusuke Enomoto[1,†1]

Received: December 24, 2020, Accepted: September 9, 2021

Abstract: We construct a timed-release hierarchical ID-base encryption scheme by using composite order bilinear functions. We show the proposed scheme is IND-ID-CPA Secure and also is IND-TR-CPA Secure based on a dual system encryption system.

Keywords: Hierarchical ID-based encryption, Timed-Release encryption, dual system encryption, composite order bilinear group

1. はじめに

ID ベース暗号（IBE）は，ユーザの ID（email アドレスなど）を公開鍵として用いる公開鍵暗号方式で，ペアリング写像を持つ双線形群を利用したものも提案されており [1]．鍵生成機関の負担を軽減する方式として，階層的 ID ベース暗号（HIBE）が 2002 年に Gentry らにより提案された [2]．

一方，Timed-Release 暗号（TRE）とは，暗号化の際に復号可能な時刻をあらかじめ指定できる暗号方式である [3], [4]．ここでは，時刻サーバが時刻鍵を一定の間隔で公開情報として送信し，時刻鍵とユーザの秘密鍵によって指定された時刻以降は復号ができる方式を対象とする．

[1] 千葉大学大学院
Chiba University, Inage, Chiba 263–8522, Japan
[†1] 現在，株式会社大都技研
Presently with DAITO GIKEN, INC.
[a)] wkishi@faculty.chiba-u.jp

1.1 提案方式

筆者らは [5] において合成数位数双線型群を用いた Waters らの階層的 ID ベース暗号方式に，時限機能を付加した階層的 ID ベース暗号方式（TR-HIBE）の具体的構成法を示し，選択平文攻撃に対する安全性（IND-ID-CPA 安全性と IND-TR-CPA 安全性）を示したが，TRE に対応する安全性（IND-TR-CPA 安全性）はランダムオラクルモデルにおいてのみ示した．

本研究では，この方式を改良した TR-HIBE を提案する．提案方式は合成数位数双線型群 [6] を用いた HIBE を基にしており，IND-ID-CPA 安全性と IND-TR-CPA 安全性をスタンダートモデルで示す．提案方式は，文献 [7], [8], [9] などの方法を適用することにより，IND-ID-CCA 安全性と IND-ID-TR-CCA 安全性を満たす方式に変換することが可能である．

Oshikiri ら [10] は，IND-hID-CCA 安全な 2 つの HIBE と OT-sEUFCMA 安全な one-time signature を用いて，CCA 安全な TR-HIBE の一般的な構成法を示している．筆者ら

の知る範囲ではCCA安全（IND-hID-CCA安全）なHIBEはCPA安全な方式に文献[7], [8], [9]などの方法を適用して構成する方法しか知られていない．Oshikiriらの方法を適用してCCA安全なTR-HIBEを構成するとした場合には，文献[7], [8], [9]などの方法を2つのCPA安全なHIBEのそれぞれに適用し，2つのCCA安全なHIBEを構成する必要がある．そのため，CCA安全なTR-HIBEを構成する際にもCPA安全なTR-HIBEを構成したうえで，文献[7], [8], [9]などの方法を適用してCCA安全なTR-HIBEを構成した方が効率が良いと考えられる．

たとえば，提案方式で利用しているLewkoらのHIBE[6]に文献[9]の方法を適用してCCA安全なHIBEを構成したうえで，Oshikiriらの方法を適用してCCA安全なTR-HIBEを構成するとした場合を考える．文献[9]の方法はその適用によって暗号文の要素数を変えない．さらに，2つのHIBEのそれぞれに適用してからTR-HIBEを構成した場合と，提案方式に適用した場合では，暗号化，復号の際に増加する計算量にそれほどの差は起きないと考えられる．しかし，Oshikiriらの方法では2つのHIBEを結合する際にOT-sEUFCMA安全なone-time signatureを必要とし，出力される暗号文がLewkoらのHIBE方式2個分の暗号文とone-time signatureの検証鍵と署名からなる．これに対して提案方式では2つのHIBE方式を合成して1つの方式としているため，利用しているLewkoらのHIBE方式2個分の暗号文よりも暗号文の長さを抑えることができている．また，2つのHIBE方式を$(2,2)$閾値秘密分散法を用いて合成した場合ではHIBE方式2個分の暗号文となるため，この場合と比較しても暗号文の長さを抑えることができている．

1.2 関連研究

階層的IDベース暗号（HIBE）はIDベース暗号の短所であったPKG（鍵生成局）の負担を軽減する方式として2002年にGentryらが提案した[2]．HIBEではユーザのIDは階層構造を持っており，階層の上位ノードの秘密鍵から，下位ノードのユーザ秘密鍵を生成することができる．2010年にWatersらはComposite Order Groupを用いることでselective IDモデルではないスタンダードモデルでのIND-ID-CPA安全性を証明可能な方式を提案した[6]．

TREは開封鍵（Pre-Open Key）と呼ばれる秘密情報を受信者に送ることにより，復号できる時刻になっていなくとも（時刻鍵を得ていなくても）暗号文を復号することができるPre-Open機能付きTRE[11]や，受信者が復号可能な期間を指定できるTime-Specific暗号[12]などもが提案されている．

合成数位数双線型群は，楕円曲線上のペアリング演算を持つ群の位数を合成数位数とすることによって構成することができる．しかし，合成数位数双線型群の位数は非常に大きな値となってしまうため，効率性の観点から実用性に問題を持つ．合成位数双線形群を素数位数双線形群に置き換える手法も研究されている[13]．

2. 準備

2.1 合成数位数双線型群

合成数位数双線型群[6]は以下の群生成アルゴリズム$\mathcal{G}$によって生成される．

群生成アルゴリズム$\mathcal{G}$.

セキュリティパラメータλを入力として，以下の条件を満足する双線型群$G=(N,G,G_T,e)$を出力する．

- $N=p_1p_2p_3$であり，p_1,p_2,p_3は異なる素数である．
- GとG_Tは位数$N=p_1p_2p_3$の巡回群である．
- $e:G^2\to G_T$は以下のような双線型写像である．
  - (1)（双線型）$\forall g,h\in G,\ a,b\in\mathbb{Z}_N,\ e(g^a,h^b)=e(g,h)^{ab}$.
  - (2)（非退化）$\exists g\in G$，G_Tでの$e(g,g)$の位数がNである．
- G, G_Tにおける群の計算と双線形写像eの計算はλに関して多項式時間である．
- 巡回群GとG_Tはそれぞれの原始元も一緒に与えられるものとする．

性質1 G_{p_i}でGの位数p_iの部分群を表すこととし，$G_{p_ip_j}$でGの位数p_ip_jの部分群を表す．ここで，$i\neq j$，$i,j\in\{1,2,3\}$に対して，$h_i\in G_{p_i}$かつ$h_j\in G_{p_j}$であるとき，$e(h_i,h_j)$はG_Tの単位元$1\in G_T$となる．

ここで，$W\in G_{p_ip_j}$（$i\neq j$）はG_{p_i}の要素とG_{p_j}の要素の積として一意に表すことができる．それぞれの要素をWのG_{p_i}部分，WのG_{p_j}部分と呼ぶことにする．

2.2 計算の複雑さの仮定

提案方式の安全性は$N=p_1p_2p_3$の素因数分解問題が計算量的に困難である仮定の下にジェネリック群モデルにおいて成り立つ以下の仮定1，2，3に基づいている．

以下において，$A\xrightarrow{R}a$という表記はAが集合のときはAから要素aが一様な確率で選ばれ，AがアルゴリズムのときはAの出力集合から要素aが一様な確率で選ばれることを表す．

仮定1 群生成アルゴリズム$\mathcal{G}$が与えられたとき，以下の分布を考える．

$$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G},g\xleftarrow{R}G_{p_1},X_3\xleftarrow{R}G_{p_3},$$
$$D=(\mathbb{G},g,X_3),W_0\xleftarrow{R}G_{p_1p_2},W_1\xleftarrow{R}G_{p_1}.$$

任意のアルゴリズム$\mathcal{A}$の利得を以下のように定める．

$$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)=|\Pr[\mathcal{A}(D,W_0)=1]-\Pr[\mathcal{A}(D,W_1)=1]|$$

いかなる多項式時間のアルゴリズム$\mathcal{A}$に対しても$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)$が$\lambda$について無視可能な関数である．

仮定 2 群生成アルゴリズム $\mathcal{G}$ が与えられたとき，以下の分布を考える．

$$\mathbb{G} = (N = p_1p_2p_3, G, G_T, e) \xleftarrow{R} \mathcal{G}$$
$$g, X_1 \xleftarrow{R} G_{p_1}, X_2, Y_2 \xleftarrow{R} G_{p_2}, X_3, Y_3 \xleftarrow{R} G_{p_3},$$
$$D = (\mathbb{G}, g, X_1X_2, X_3, Y_2Y_3),$$
$$W_0 \xleftarrow{R} G, W_1 \xleftarrow{R} G_{p_1p_3}.$$

アルゴリズム $\mathcal{A}$ の利得を以下のように定める．

$$Adv2_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, W_0) = 1] - \Pr[\mathcal{A}(D, W_1) = 1]|$$

いかなる多項式時間のアルゴリズム $\mathcal{A}$ に対しても $Adv2_{\mathcal{G},\mathcal{A}}(\lambda)$ が λ について無視可能な関数である．

我々は，文献 [6] の仮定 3 を変形した以下の仮定を用いる．

仮定 3 群生成アルゴリズム $\mathcal{G}$ が与えられたとき，以下の分布を考える．

$$\mathbb{G} = (N = p_1p_2p_3, G, G_T, e) \xleftarrow{R} \mathcal{G},\ \alpha, s \xleftarrow{R} \mathbb{Z}_N,$$
$$g, f, \xleftarrow{R} G_{p_1}, X_2, Y_2, Z_2 \xleftarrow{R} G_{p_2}, X_3 \xleftarrow{R} G_{p_3},$$
$$D = (\mathbb{G}, g, f, g^\alpha, f^\alpha X_2, X_3, g^s Y_2, Z_2),$$
$$W_0 = e(g, f)^{\alpha s}, W_1 \xleftarrow{R} G_T.$$

アルゴリズム $\mathcal{A}$ の利得を以下のように定める．

$$Adv3_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, W_0) = 1] - \Pr[\mathcal{A}(D, W_1) = 1]|$$

いかなる多項式時間のアルゴリズム $\mathcal{A}$ に対しても $Adv3_{\mathcal{G},\mathcal{A}}(\lambda)$ が λ について無視可能な関数である．

ジェネリック群モデル

$N = p_1p_2p_3$ の素因数分解問題が計算量的に困難であると仮定する．仮定 1, 仮定 2 はジェネリック群モデルにおいて，成り立つことが示されている [6]．本論文の仮定 3 の成り立つことも文献 [14] の定理 A.1 を用いて示すことができる．

G_{p_1}，G_{p_2}，G_{p_3} の原始元をそれぞれ選び，g_{p_1}，g_{p_2}，g_{p_3} とする．G のすべての要素は値 $a_1 \in \mathbb{Z}_{p1}$，$a_2 \in \mathbb{Z}_{p2}$，$a_3 \in \mathbb{Z}_{p3}$ を用いて，$g_{p_1}^{a_1} g_{p_2}^{a_2} g_{p_3}^{a_3}$ と表すことができるため，G の要素を (a_1, a_2, a_3) と表す．さらに，G_T の要素 $e(g_{p_1}, g_{p_1})^{a_1} e(g_{p_2}, g_{p_2})^{a_2} e(g_{p_3}, g_{p_3})^{a_3}$ は $[a_1, a_2, a_3]$ と表す．確率変数は A_1，A_2，A_3 などの大文字で表し，要素間の関係も表すことにする．たとえば，$X = (X_1, Y_1, Z_1)$，$Y = (X_1, Y_2, Z_2)$ は，G_{p_1} 部分に共通要素を持つ G のランダムな要素を表す．与えられた確率変数 X，$\{A_i\}$ をこの形式で表し，形式的確率変数として，$X = \sum_i \lambda_i A_i$ を満たす $\lambda_i \in \mathbb{Z}_n$ が存在するならば X は $\{A_i\}$ に従属するという．従属していないとき X は $\{A_i\}$ と独立であるという．

定理 1 （文献 [14] の定理 A.1）$N = \prod_{i=1}^{m} p_i$ をそれぞれが 2^λ より大きい異なる素数の積とする．$\{A_i\}$ を G 上の確率変数，$\{B_i\}$，W_0，W_1 を G_T 上の確率変数とし，すべての確率変数の次数はたかだか t とする．ジェネリック群モデルで以下の試行を考える．

（試行）アルゴリズム A には N，$\{A_i\}$，$\{B_i\}$ が与えられる．1 ビット b がランダム選ばれ，A には W_b が与えられる．アルゴリズム A は 1 ビット b' を出力し，$b' = b$ なら A は成功したとする．アルゴリズム A の利得は成功確率と $\frac{1}{2}$ の差の絶対値とする．

W_0 と W_1 は $\{B_i\} \cup \{e(A_i, A_j)\}$ に対して独立であるとする．試行において，たかだか q 回の任意の命令を実行する利得 δ を持つアルゴリズムを用いると，λ と A の実行時間の多項式時間で，少なくとも確率 $\delta - O(q^2t/2^\lambda)$ で，N の非自明な因数を求めることができる．

$N = p_1p_2p_3$ の素因数分解問題が計算量的に困難である仮定の下に定理 1 を用いて仮定 3 が成り立つことを示す．

仮定 3 の証明 仮定 3 の分布は以下のように表せる．

$$A_1 = (1, 0, 0), A_2 = (C, 0, 0), A_3 = (B, 0, 0),$$
$$A_4 = (BC, 1, 0), A_5 = (0, 0, 1), A_6 = (S, X_2, 0),$$
$$A_7 = (0, Y_2, 0), W_0 = [BCS, 0, 0], W_1 = [Z_1, Z_2, Z_3].$$

Z_1, Z_2, Z_3 は $\{A_i\}$ には現れないので，W_1 は $\{e(A_i, A_j)\}$ に対して独立である．BCS を 1 番目の要素に得るためには $e(A_4, A_6)$ としなければならないが，X_2 が 2 番目の要素に残ってしまい，この要素を消すことはできない．よって，定理 1 を適用できるので，$Adv3_{\mathcal{G},\mathcal{A}}(\lambda)$ が無視できない値であるならば，N の非自明な因数を求めることができる．すなわち，N の非自明な因数を求めることが難しいと仮定すると仮定 3 はジェネリック群モデルにおいて成り立つ． （証明終）

3. 時限機能を付加した階層的 ID ベース暗号方式

筆者らは合成数位数双線型群を用いた Lewko らの階層的 ID ベース暗号方式 [6] を基にして，時限機能を付加した階層的 ID ベース暗号方式（TR-HIBE）の具体的構成法を示し，スタンダードモデルにおいて IND-ID-CPA 安全性を，ランダムオラクルモデルにおいて IND-ID-RTR-CPA 安全性を示した [5].

3.1 TR-HIBE（時限機能を付加した階層的 ID ベース暗号方式）

ユーザの ID ベクトル $(ID_1, \ldots, ID_j)$ は階層的となっており，要素 ID_i および，時刻 T は $\mathbb{Z}_N$ の要素であるとする．$ID = (ID_1, \ldots, ID_j)$，$ID' = (ID_1, \ldots, ID_j, ID_{j+1})$ のとき，$ID' = ID||ID_{j+1}$ と表す．このとき，ID は ID' の親，ID' は ID の子であるという．さらに，$ID = (ID_1, \ldots, ID_j)$ と $i \leq j$ である i に対して，$ID_i = (ID_1, \ldots, ID_i)$ は ID の先祖であるという．ID を先祖として持つ ID_k は ID の子孫であるという．ここでは，ID は ID 自身の先祖であり，子孫でもあるとする．

定義 1 TR-HIBE（時限機能を付加した階層的 ID ベース暗号方式）は以下の 5 つのアルゴリズムからなる．

Setup：セキュリティパラメータ 1^k を入力とし，公開パラメータ $params$，マスター秘密鍵 msk と時刻サーバの秘密鍵 tsk を出力する．

Release：時刻サーバの秘密鍵 tsk，時刻 T を入力とし，時刻 T に対応する時刻鍵 R_T を出力する．

KeyGen：$params$，ID ベクトル $ID = (ID_1, \ldots, ID_j)$，$msk$ を入力として，ID 鍵 sk_{ID} を出力する．

Delegate：$params$，sk_{ID}，ID ベクトル $ID' = ID||ID_{j+1}$ を入力として，ID 鍵 $sk_{ID'}$ を出力する．

Encryption：$params$，ID，T，平文 M を入力として，暗号文 C を出力する．

Decryption：$params$，sk_{ID}，R_T，C を入力として，平文 M を出力する．

3.2 TR-HIBE の安全性

TR-HIBE の安全性として，本研究では，時刻サーバ（第 3 者を含めた）に対する安全性である IND-ID-CPA 安全性と，(時刻鍵を持たない) 正当な受信者に対する安全性である IND-TR-CPA 安全性の 2 つを考察する．これらの安全性は文献 [10] の IND-hID-CCA$_{\mathrm{TS}}$ 安全性と IND-hID-CCA$_{\mathrm{CR}}$ 安全性にそれぞれ対応する．

3.2.1 IND-ID-CPA 安全性

時刻サーバより放送された時刻鍵を入手したとしても，受信者の正当な ID 鍵を持っていなければ復号できないことを示す安全性である．以下のチャレンジャ $\mathcal{C}$ と攻撃者 $\mathcal{A}$ のゲーム（IND-ID-CPA ゲーム）を用いて定義される．

IND-ID-CPA ゲーム

Setup $\mathcal{C}$ は Setup アルゴリズムを実行し params を $\mathcal{A}$ に与え，チャレンジャが生成した ID 鍵をセットするための $S = \emptyset$ を生成する．

Phase1 攻撃者は以下のクエリを実行できる．

- **Create クエリ** ID ベクトル ID を入力として与える．返答としてこのベクトル ID の ID 鍵を KeyGen アルゴリズムによって生成し，S の中にセットする．この鍵を指定するための識別子であるリファレンスだけを出力し，鍵そのものは出力しない．
- **Delegate クエリ** S の中の鍵 sk_{ID} のリファレンスと $ID||ID'$ を入力として与える．チャレンジャは返答として，$ID||ID'$ の ID 鍵を Delegate アルゴリズムによって生成する．この鍵を S にセットして，その鍵のリファレンスだけを出力する．
- **Reveal クエリ** S の要素のリファレンスを入力として与える．鍵を S から取り除き，出力する．
- **Release クエリ** 任意の時刻 T を入力として与える．Release アルゴリズムを実行して時刻鍵 R_T を生成し，出力する．クエリする時刻に制限はなく，攻撃対象とする時刻であるチャレンジ時刻 T^* をクエリしても良い．

Challenge 攻撃者はチャレンジャに対し 2 つのメッセージ M_0，M_1，攻撃対象とする ID であるチャレンジ ID ベクトル ID^*，チャレンジ時刻 T^* を送る．ID^* は Phase1 で Reveal クエリに入力された ID の子孫であってはならない．チャレンジャは $\eta \in \{0,1\}$ を選び，M_η を ID^*，T^* のもとで暗号化したチャレンジ暗号文を攻撃者に送る．

Phase2 Phase1 と同様にクエリを行う．ID^* の先祖の ID ベクトルを Reveal クエリしてはいけない．

Guess 攻撃者は η に対し η' を出力する．攻撃者 $\mathcal{A}$ の利得を $Pr[\eta' = \eta] - \frac{1}{2}$ とする．

定義 2 すべての多項式時間の攻撃者の上記のゲームでの利得が無視できるとき，提案方式は IND-ID-CPA 安全である．

3.2.2 IND-TR-CPA 安全性

ID 鍵を持っていても，送信者の指定した時刻以前には復号できないことを示す安全性である．以下のチャレンジャ $\mathcal{C}$ と攻撃者 $\mathcal{A}$ のゲーム（IND-TR-CPA ゲーム）を用いて定義される．

IND-TR-CPA ゲーム

Setup チャレンジャは Setup アルゴリズムを実行し，公開パラメータ $params$ を攻撃者に与える．

Phase1 攻撃者は以下のクエリを実行できる．

- **KeyGen クエリ** ID ベクトル ID を入力として与える．ID を入力として KeyGen アルゴリズムを実行し ID 鍵 sk_{ID} を生成し，出力する．
- **Release クエリ** 時刻 T を入力として与える．T を入力として Release アルゴリズムを実行し時刻鍵 R_T を生成し，出力する．

Challenge 攻撃者はチャレンジャに対し 2 つのメッセージ M_0，M_1，チャレンジ ID ベクトル ID^*，チャレンジ時刻 T^* を送る．T^* は Phase1 で Release クエリに入力した時刻であってはならない．チャレンジャは $\eta \in \{0,1\}$ を選び，M_η を ID^*，T^* のもとで暗号化したチャレンジ暗号文を攻撃者に送る．

Phase2 Phase1 と同様にクエリを行う．ただし，Challenge で出力したチャレンジ時刻 T^* を Release クエリに入力することはできない．

Guess 攻撃者は η に対して，η' を出力する．
攻撃者の利得を $Pr[\eta = \eta'] - \frac{1}{2}$ とする．

定義 3 すべての多項式時間の攻撃者のゲームでの利得が無視できるとき，提案方式は IND-TR-CPA 安全である．

4. 提案方式

4.1 提案方式の構成

Setup：セキュリティパラメータ 1^k を入力とし，p_1，p_2，p_3 を互いに異なる素数とし，$N = p_1p_2p_3$ と置く．G を合成数位数 N の双線型性群とする．ユーザ ID の最大の階層の深さを ℓ とする．$ID = (ID_1, \ldots, ID_j)$ と

する．$g, f_d, f_t, h_d, h_t, U, u_1, \ldots, u_\ell$ を G_{p_1}，X_3 を G_{p_3} からランダムに選ぶ．α，β を $\mathbb{Z}_N$ からランダムに選ぶ．公開パラメータは $params = [N, g, g_d\ (= g^\alpha), g_t\ (= g^\beta), f_d, f_t, h_d, h_t, U, u_1, \ldots, u_\ell, X_3]$ とし，マスター鍵は $msk = f_d^\alpha$，時刻サーバの秘密鍵は $tsk = f_t^\beta$ とする．

KeyGen（$msk, ID, params$）：ランダムに $r \in_R \mathbb{Z}_N$, R_3, R'_3, Q_{j+1}, …, $Q_\ell \in_R G_{p_3}$ を選択し，

$$K_1 = g^r R_3, \quad K_2 = f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r R'_3,$$
$$E_{j+1} = u_{j+1}^r Q_{j+1}, \cdots, E_\ell = u_\ell^r Q_\ell.$$

ID 鍵 $sk_{ID} = (K_1, K_2, E_{j+1}, \ldots, E_\ell)$ を出力する．

Release（$tsk, T_C, params$）：ランダムに $v \in_R \mathbb{Z}_N$, R_{3t}, $R'_{3t} \in G_{p_3}$ を選択する．

$$K_{t,1} = g^v R_{3t}, \quad K_{t,2} = f_t^\beta (U^{T_C} h_t)^v R'_{3t}.$$

時刻鍵 $R_T = (K_{t,1}, K_{t,2})$ を出力する．

Delegate（$ID||ID_{j+1}, sk_{ID}, params$）：$sk_{ID} = (K_1, K_2, E_{j+1}, \ldots, E_\ell)$ とする．ランダムに $r' \in_R \mathbb{Z}_N$, R''_3, Q'_{j+2}, …, $Q'_\ell \in_R G_{p_3}$ を選択する．

$$K_1 = K'_1 g^{r'} R''_3 = g^r R_3 g^{r'} R''_3 = g^{r+r'} R_3 R''_3,$$
$$K_2 = K'_2 (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^{r'} (E'_{j+1})^{ID_{j+1}} u_{j+1}^{r' ID_{j+1}} R''_3,$$
$$= f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^{r+r'} u_{j+1}^{ID_{j+1}(r+r')} Q_{j+1}^{ID_{j+1}} R'_3 R''_3,$$
$$E_{j+2} = E'_{j+2} u_{j+2}^{r'} Q'_{j+2} = u_{j+2}^{r+r'} Q_{j+2} Q'_{j+2},$$
$$\vdots$$
$$E_\ell = E'_\ell u_\ell^{r'} Q'_\ell = u_\ell^{r+r'} Q_\ell Q'_\ell.$$

$sk_{ID||ID_{j+1}} = (K_1, K_2, E_{j+2}, \ldots, E_\ell)$ を出力する．

Encryption（$M, ID, T_C, params$）：ランダムに $s \in_R \mathbb{Z}_N$ を選ぶ．

$$C_0 = M(e(g_t, f_t) e(g_d, f_d))^s = M e(g, f_t)^{\beta s} e(g, f_d)^{\alpha s},$$
$$C_1 = (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^s,$$
$$C_2 = g^s, \qquad C_3 = (U^{T_C} h_t)^s.$$

$C = (C_0, C_1, C_2, C_3)$ を出力する．

Decryption（$C, sk_{ID}, R_T, params$）：時刻サーバが放送した時刻鍵 $R_T = (K_{t,1}, K_{t,2})$ と，ID 鍵 $sk_{ID} = (K_1, K_2, E_{j+1}, \ldots, E_\ell)$ を用いて，暗号文 $C = (C_0, C_1, C_2, C_3)$ を以下のように復号する．

$$C_0 \frac{e(K_1, C_1) e(K_{t,1}, C_3)}{e(C_2, K_2 K_{t,2})} = M.$$

4.2 提案方式の正当性

時刻サーバが放送した時刻鍵 $R_T = (K_{t,1}, K_{t,2})$ と，正当な ID 鍵 $sk_{ID} = (K_1, K_2, E_{j+1}, \ldots, E_\ell)$ を用いて，暗号文 (C_0, C_1, C_2, C_3) を復号すると以下のようになる．

$$C_0 \frac{e(K_1, C_1) e(K_{t,1}, C_3)}{e(C_2, K_2 K_{t,2})}$$
$$= M e(g, f_t)^{\beta s} e(g, f_d)^{\alpha s}$$
$$\frac{e(g^r R_3, (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^s) e(g^v R_{3t}, (U^{T_C} h_t)^s)}{e(g^s, f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r R'_3 f_t^\beta (U^{T_C} h_t)^v R'_{3t})}$$
$$= M \frac{e(g, f_t)^{\beta s} e(g, f_d)^{\alpha s}}{e(g, f_d)^{\alpha s} e(g, u_1^{ID_1} \cdots u_j^{ID_j} h_d)^{rs}}$$
$$\frac{e(g, u_1^{ID_1} \cdots u_j^{ID_j} h_d)^{rs} e(g, U^{T_C} h_t)^{vs}}{e(g, f_t)^{\beta s} e(g, U^{T_C} h_t)^{vs}} = M.$$

5. 提案方式の安全性

提案式の安全性として，standard model において IND-ID-CPA 安全性と IND-TR-CPA 安全性を証明する．

5.1 Dual System Encryption

Dual system encryption [6] では，提案方式には存在しない鍵と暗号文である semi-functional な ID 鍵（sf-IK），semi-functional な時刻鍵（sf-RK）と semi-functional な暗号文（sf-CT）を用いる．通常の ID 鍵，時刻鍵，暗号文はそれぞれ IK，RK，CT と表す．sf-CT は IK，RK で復号できるが sf-IK，sf-RK のどちらか一方でも用いると復号できない．

ランダムに $g_2 \in_R G_{p_2}$，$x, \gamma, \zeta, z_d, z_{j+1}, \ldots, z_\ell, z_t, z_c, z_s \in_R Z_N$ を選ぶものとする．

定義 4 暗号化アルゴリズムで生成された通常の暗号文を $C' = (C'_0, C'_1, C'_2, C'_3)$ と表すと，sf-CT $C = (C_0, C_1, C_2, C_3)$ は以下のように定義される．

$$C_0 = C'_0 = M(e(g_t, f_t) e(g_d, f_d))^s = M e(g, f_t)^{\beta s} e(g, f_d)^{\alpha s},$$
$$C_1 = C'_1 g_2^{x z_c} = (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^s g_2^{x z_c},$$
$$C_2 = C'_2 g_2^x = g^s g_2^x, \qquad C_3 = C'_3 g_2^{x z_s} = (U^{T_C} h_t)^s g_2^{x z_s}.$$

定義 5 鍵生成アルゴリズム KeyGen で生成された，ID に対する IK を $sk'_{ID} = (K'_1, K'_2, E'_{j+1}, \cdots, E'_\ell)$ と表すと，sf-IK $sk_{ID} = (K_1, K_2, E_{j+1}, \cdots, E_\ell)$ は以下のように定義される．

$$K_1 = K'_1 g_2^\gamma = g^r g_2^\gamma R_3,$$
$$K_2 = K'_2 g_2^{\gamma z_d} = f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r g_2^{\gamma z_d} R'_3,$$
$$E_{j+1} = E'_{j+1} g_2^{\gamma z_{j+1}} = u_{j+1}^r g_2^{\gamma z_{j+1}} Q_{j+1},$$
$$\vdots$$
$$E_\ell = E'_\ell g_2^{\gamma z_\ell} = u_\ell^r g_2^{\gamma z_\ell} Q_\ell.$$

$z_c = z_d$ ならば sf-IK と通常の時刻鍵を用いて sf-CT を復号できる．この場合の sf-IK を擬似 sf-IK と呼ぶ．

定義 6 鍵生成アルゴリズムで生成された時刻 T_C に対する RK を $R'_T = (K'_{t,1}, K'_{t,2})$ と表すと，sf-RK $R_T = (K_{t,1}, K_{t,2})$ は以下のように定義される．

$K_{t,1} = K'_{t,1} g_2^{\zeta} = g^v g_2^{\zeta} R_{3t}$,
$K_{t,2} = K'_{t,2} g_2^{\zeta z_t} = f_t^{\beta} (U^{T_C} h_t)^v g_2^{\zeta z_t} R'_{3t}$.

$z_s = z_t$ ならば IK と sf-RK を用いて sf-CT を復号できる．この場合の sf-RK を擬似 sf-RK と呼ぶ．

5.2 IND-ID-CPA 安全性

IND-ID-CPA ゲームを $Game_{Real}$ とおいて，$Game_{Real}$ から $Game_{Final}$ までを構成する．$Game_X$ におけるアルゴリズム $\mathcal{A}$ の利得を $Game_X Adv_{\mathcal{A}}$ と表す．また，それぞれのゲーム $Game_X$ において，攻撃者 $\mathcal{A}$ の出力 η' がチャレンジャの選択した η と等しくなる確率を $\Pr_X[\eta' = \eta]$ と表すことにすると，$Game_X$ における攻撃者 $\mathcal{A}$ の利得は

$$Game_X Adv_{\mathcal{A}} = \left| \Pr_X[\eta' = \eta] - \frac{1}{2} \right|.$$

5.2.1 IND-ID-CPA ゲームに対するゲーム列

ゲーム中になされるクエリの数を q とし，1 回のクエリでは ID 鍵はたかだか 1 つしか用いられないので，生成される ID 鍵はたかだか q 個である．同じ鍵を用いるクエリを 2 度以上したときには最初にクエリしたときの鍵がそのまま用いられる．以下のゲーム列を考える．

$Game_{Real}$：通常の IND-ID-CPA ゲーム．

$Game_{Real'}$：$Game_{Real}$ と同じだが，すべてのクエリで生成される ID 鍵は KeyGen アルゴリズムで生成される．

$Game_k$ $(0 \le k \le q)$：チャレンジ暗号文に sf-CT を用い，時刻鍵はつねに RK を用いる．さらに，$1, \ldots, k$ 個目までのクエリで生成される ID 鍵に sf-IK を用い，残りのクエリで生成される ID 鍵には IK を用いる．後は $Game_{Real'}$ と同じである（$Game_0$ では，すべてのクエリで生成される ID 鍵に IK を用い，$Game_q$ では，すべてのクエリで生成される ID 鍵に sf-IK を用いることになる）．

$Game_{Final}$：攻撃者から送られてきた 2 つの平文の 1 つを暗号化して返すのではなく，ランダムな平文を暗号化して返す以外は $Game_q$ と同じである．

補題 1 安全性ゲームにおける攻撃者がクエリを行う ID が，ID^* と mod N では異なるが，mod p_2 で等しくなる確率は無視できるくらいに小さい．

証明. この補題が成り立たない場合は，以下を満たす攻撃者 $\mathcal{A}$ が存在することになり，仮定 1 または 2 に矛盾する．

攻撃者 $\mathcal{A}$ は無視できない確率 ε で $ID \not\equiv ID^* \pmod N$ かつ $ID \equiv ID^* \pmod{p_2}$ となるような ID をクエリの入力として生成する．このとき，仮定 1 または仮定 2 を利得 $\frac{\varepsilon}{2}$ 以上で破ることのできるアルゴリズム $\mathcal{B}$ を以下のように構成できる．

$\mathcal{B}$ は $\mathcal{A}$ のクエリに含まれている ID を用いて，$a = gcd(ID - ID^*, N)$ を計算することにより，N の約数 a を求めることができる．$b = \frac{N}{a}$ と置く．このとき，p_2 は a と N（$= ab = p_1 p_2 p_3$）を割り切るので，p_2 は a の因数であり，b の因数には含まれない．ここで，2 つの場合に分けられる．

1. p_1 が b を割り切る（すなわち $b = p_1$ または $b = p_1 p_3$）
2. $a = p_1 p_2$，$b = p_3$.

少なくともどちらかの場合が $\frac{\varepsilon}{2}$ 以上の確率で生起する．

1 の場合，$\mathcal{B}$ は仮定 1 を破る．g $(\in G_{p_1})$，X_3 $(\in G_{p_3})$，W を与えられたとき，$\mathcal{B}$ は g^b が単位元になることを確かめることにより，p_1 が b の約数であることを確かめる．次に W^b を計算し，W^b が単位元になれば，W は G_{p_1} の要素であることが分かる．W^b が単位元にならなければ，W は $G_{p_1 p_2}$ の要素であることが分かる．

2 の場合，$\mathcal{B}$ は仮定 2 を破る．g $(\in G_{p_1})$，$X_1 X_2$，X_3，$Y_2 Y_3$ を与えられたとき，$\mathcal{B}$ は $(X_1 X_2)^a$ を計算し，$(X_1 X_2)^a$ が単位元になれば，$a = p_1 p_2$ であることを確かめる．次に $e((Y_2 Y_3)^b, W)$ を計算し，$e((Y_2 Y_3)^b, W)$ が単位元になれば，W は $G_{p_1 p_3}$ の要素であることが分かる．$e((Y_2 Y_3)^b, W)$ が単位元にならなければ，W は G の要素である．（証明終）

この補題により，各ゲームにおいてクエリされる ID は ID^* と mod N でも mod p_2 でも異なるとして良い．

補題 2 任意の攻撃者のアルゴリズム $\mathcal{A}$ に対して，$Game_{Real} Adv_{\mathcal{A}} = Game_{Real'} Adv_{\mathcal{A}}$ である．

証明. KeyGen アルゴリズムによって生成された ID 鍵と，Delegate アルゴリズムによって鍵階層の親の鍵から生成された ID 鍵の確率分布は同一である．したがって $Game_{Real}$ と $Game_{Real'}$ の間に違いはなく，任意の攻撃者のアルゴリズム $\mathcal{A}$ のそれぞれのゲームにおける利得は等しくなる．（証明終）

補題 3 無視できない値 ε とあるアルゴリズム $\mathcal{A}$ に対して $|Game_{Real'} Adv_{\mathcal{A}} - Game_0 Adv_{\mathcal{A}}| = \varepsilon$. となるならば，仮定 1 を利得 ε 以上で破ることができるアルゴリズム $\mathcal{B}$ を構成できる．

証明. $\mathcal{B}$ は最初に g, X_3, W（$W = W_0 = g^s g_2^x \in G_{p_1 p_2}$ または $W = W_1 = g^s \in G_{p_1}$）が与えられる．$\mathcal{B}$ は $\mathcal{A}$ に対して，$Game_{Real'}$ または $Game_0$ をシミュレートし，$\mathcal{A}$ に見分けさせる．

$\mathcal{B}$ は公開情報を以下のように作成する．ランダムに $\alpha, \beta, a_0, a_1, \ldots, a_\ell$, b_1, b_2, $c_1, c_2 \in \mathbb{Z}_N$ を選び，$g = g$, $u_i = g^{a_i}$ $(i = 1, \ldots, \ell)$, $f_d = g^{c_1}$, $f_t = g^{c_2}$, $g_d = g^{\alpha}$, $g_t = g^{\beta}$, $h_d = g^{b_1}$, $h_t = g^{b_2}$, $U = g^{a_0}$. と設定する．$\mathcal{B}$ はこれらの公開情報を $params = [N, g, g_d\ (= g^{\alpha}), g_t\ (= g^{\beta}), f_d, f_t, h_d, h_t, U, u_1, \ldots, u_\ell, X_3]$ を $\mathcal{A}$ に送信する．

$\mathcal{B}$ は ID $(ID_1, \ldots, ID_j)$ に対する ID 鍵が必要となるクエリが来ると，乱数 $r, t, w, v_{j+1}, \ldots, v_\ell \in \mathbb{Z}_N$ を選び，以下のように設定して $K = (K_1, K_2)$ を答える．

$K_1 = g^r X_3^t, K_2 = f_d^{\alpha} (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r X_3^w$,
$E_{j+1} = u_{j+1}^r X_3^{v_{j+1}}, \ldots, E_\ell = u_\ell^r X_3^{v_\ell}$.

$\mathcal{B}$ は時刻 T_C に対する Release クエリに答えるために，乱数 $v, u_1, u_2 \in \mathbb{Z}_N$ を選び以下のように設定して $R_T = (K_{t,1}, K_{t,2})$ を答える．

$$K_{t,1} = g^v X_3^{u_1},$$
$$K_{t,2} = f_t^{\beta}(U^{T_C} h_t)^v X_3^{u_2} = g^{c_2\beta}(g^{a_0 T_C} g^{b_2})^v X_3^{u_2}.$$

$\mathcal{A}$ は $\mathcal{B}$ に 2 つの平文 M_0，M_1，チャレンジ ID $(ID_1^*, \ldots, ID_j^*)$ とチャレンジ時刻 T_C^* を送る．

$\mathcal{B}$ はランダムに $\eta \in \{0,1\}$ を選ぶ．暗号文を以下のように構成する．

$$C_0 = M_\eta e(W^\beta, f_t) e(W^\alpha, f_d),$$
$$C_1 = W^{a_1 ID_1^* + \cdots a_j ID_j^* + b_1},\ C_2 = W,\ C_3 = W^{a_0 T_C^* + b_2}.$$

（ここで，W の G_{p_1} 要素が g^s に対応することになる．）

$W \in G_{p_1 p_2}$（$W = g^s g_2^x$）の場合には，以下に示すように $z_c = a_1 ID_1^* + \cdots + a_j ID_j^* + b_1$, $z_s = a_0 T_C^* + b_2$ と置いた sf-CT になる．すなわち，$Game_0$ になる．

$$C_0 = M_\eta e(W^\beta, f_t) e(W^\alpha, f_d) = M_\eta (e(g^\beta, f_t) e(g^\alpha, f_d))^s,$$
$$C_1 = W^{a_1 ID_1^* + \cdots a_j ID_j^* + b_1} = (u_1^{ID_1^*} \cdots u_j^{ID_j^*} h_d)^s g_2^{z_c x},$$
$$C_2 = W = g^s g_2^x,$$
$$C_3 = W^{a_0 T_C^* + b_2} = (g^s g_2^x)^{a_0 T_C^* + b_2} = (U^{T^*} h_t)^s g_2^{z_s x}.$$

また，z_c，z_s の mod p_2 での値は a_i，b_i の mod p_1 の値とは関連しないため，z_c, z_s の値は独立にランダムに選ばれた値として分布するため，ゲームの構成に従っている．

$W \in G_{p_1}$（$W = g^s$）の場合には以下に示すように CT となる．すなわち，$Game_{Real'}$ になる．

$$C_0 = M_\eta e(W^\beta, f_t) e(W^\alpha, f_d) = M_\eta (e(g^\beta, f_t) e(g^\alpha, f_d))^s,$$
$$C_1 = W^{a_1 ID_1^* + \cdots a_j ID_j^* + b_1} = (u_1^{ID_1^*} \cdots u_j^{ID_j^*} h_d)^s,$$
$$C_2 = W = g^s,\quad C_3 = W^{a_0 T_C^* + b_2} = (U^{T_C^*} h_t)^s.$$

以上のことから，$W \in G_{p_1}$ の場合には $\mathcal{A}$ は $Game_{Real'}$ を行うこととなり，$W \in G_{p_1 p_2}$ の場合には $\mathcal{A}$ は $Game_0$ を行うこととなる．

$\mathcal{B}$ は $\mathcal{A}$ の出力 η' が η と等しい場合に 1 を，等しくない場合には 0 を出力して仮定 1 を破ろうと試みるものとする．W が G_{p_1} の要素 W_1 である場合に $\mathcal{B}$ が 1 を出力する確率は，

$$\Pr[\mathcal{B}(D, W_1) = 1] = \Pr_{Real'}[\eta' = \eta]$$

W が $G_{p_1 p_2}$ の要素 W_0 である場合に $\mathcal{B}$ が 1 を出力する確率は，

$$\Pr[\mathcal{B}(D, W_0) = 1] = \Pr_0[\eta' = \eta]$$

となる．このとき，$\mathcal{B}$ の仮定 1 に対する利得は，以下に示すように ε 以上となる．

$$\begin{aligned}
&Adv1_{\mathcal{G},\mathcal{B}}(\lambda) \\
&= |\Pr[\mathcal{A}(D, W_0) = 1] - \Pr[\mathcal{A}(D, W_1) = 1]| \\
&= |\Pr_0[\eta' = \eta] - \Pr_{Real'}[\eta' = \eta]| \\
&= \left|\Pr_0[\eta' = \eta] - \frac{1}{2} - \left(\Pr_{Real'}[\eta' = \eta] - \frac{1}{2}\right)\right| \\
&\geq \left|\left|\Pr_0[\eta' = \eta] - \frac{1}{2}\right| - \left|\left(\Pr_{Real'}[\eta' = \eta] - \frac{1}{2}\right)\right|\right| \\
&= |Game_0 Adv_{\mathcal{A}} - Game_{Real'} Adv_{\mathcal{A}}| = \varepsilon.
\end{aligned}$$

（証明終）

補題 4 無視できない値 ε とあるアルゴリズム $\mathcal{A}$ に対して $Game_{k-1} Adv_{\mathcal{A}} - Game_k Adv_{\mathcal{A}} = \varepsilon$（$1 \leq k \leq q$）となるならば，仮定 2 を利得 ε 以上で破るアルゴリズム $\mathcal{B}$ を構成できる．

証明. $\mathcal{B}$ は入力として g，$X_1 X_2$，X_3，$Y_2 Y_3$，W を受け取る．$\mathcal{B}$ の目的は $\mathcal{A}$ を利用して，$W \in G$ なのか $W \in G_{p_1 p_3}$ なのかを見分けることである．$\mathcal{B}$ はランダムに $\alpha, \beta, a_0, a_1, \ldots, a_\ell, b_1, b_2, c_1, c_2 \in \mathbb{Z}_N$ を選び，公開情報を以下のように設定する．$g = g$, $u_i = g^{a_i}$ $(i = 1, \ldots, \ell)$, $f_d = g^{c_1}$, $f_t = g^{c_2}$, $g_d = g^\alpha$, $g_t = g^\beta$, $h_d = g^{b_1}$, $h_t = g^{b_2}$, $U = g^{a_0}$．$\mathcal{B}$ は公開情報 $params = [N, g, g_d\ (= g^\alpha), g_t\ (= g^\beta), f_d, f_t, h_d, h_t, U, u_1, \ldots, u_\ell, X_3]$ を $\mathcal{A}$ にわたす．

$\mathcal{A}$ の i 番目のクエリにおいてて ID $(ID_1, \ldots, ID_j)$ に対する ID 鍵の生成が必要となったときに，$i < k$ である場合は，$\mathcal{B}$ は sf-IK を生成する．乱数 $r, t, w, v_{j+1}, \ldots, v_\ell \in \mathbb{Z}_N$ を選び，以下のように設定する．

$$K_1 = g^r (Y_2 Y_3)^t,\quad K_2 = f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r (Y_2 Y_3)^w,$$
$$E_{j+1} = u_{j+1}^r (Y_2 Y_3)^{v_{j+1}}, \cdots, E_\ell = u_\ell^r (Y_2 Y_3)^{v_\ell}.$$

このように生成された sf-IK は $g_2^\gamma = Y_2^t$ と置かれた場合に対応し，$t, w, v_{j+1}, \ldots, v_\ell$ の mod p_2 での値と，mod p_3 での値は独立であるので，鍵の分布も通常の $Game_{Real}$ のとおりになっている．

$i > k$ の場合には，$\mathcal{B}$ は IK 生成する．ランダムに $r, t, w, v_{j+1}, \ldots, v_\ell \in \mathbb{Z}_N$ を選び，以下のように設定する．

$$K_1 = g^r X_3^t,\quad K_2 = f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r X_3^w,$$
$$E_{j+1} = u_{j+1}^{r_i} X_3^{v_{j+1}}, \cdots, E_\ell = u_\ell^{r_i} X_3^{v_\ell}.$$

k 番目のクエリにおいて ID $(ID_1, \ldots, ID_j)$ に対する ID 鍵の生成が必要な場合には，$\mathcal{B}$ は $z_d = a_1 ID_1 + \cdots a_j ID_j + b_1$ と置き，ランダムに $w, v_{j+1}, \ldots, v_\ell \in \mathbb{Z}_N$ を選び以下のように設定する．

$$K_1 = W,\quad K_2 = f_d^\alpha W^{z_d} X_3^w,$$
$$E_{j+1} = W^{a_{j+1}} X_3^{v_{j+1}}, \cdots, E_\ell = W^{a_\ell} X_3^{v_\ell}.$$

W が $G_{p_1 p_3}$ の要素のときには，この鍵は，g^r が W の G_{p_1} 要素に等しくなる IK となる，すなわち，$Game_{k-1}$ と

なる．W が G の要素のときには，この鍵は，sf-IK となる，すなわち，$Game_k$ となる．

$\mathcal{A}$ が時刻 T_C に対する Release クエリをしてきたときには，$\mathcal{B}$ は時刻鍵生成アルゴリズムを用いて，以下のように RK R_T を生成する．$\mathcal{B}$ はランダムに $v,t,w \in \mathbb{Z}_N$ を選び，以下のように設定する．

$$K_{t,1} = g^v X_3^w, \quad K_{t,2} = f_t^\beta (U^{T_C} h_t)^v X_3^t.$$

ある時点で $\mathcal{A}$ は $\mathcal{B}$ に 2 つの平文 M_0，M_1，チャレンジ ID $(ID_1^*, \ldots, ID_j^*)$，チャレンジ時刻 T_C^* を送ってくる．

$\mathcal{B}$ はランダムに $\eta \in \{0,1\}$ を選び，チャレンジ暗号文を以下のように設定する．

$$\begin{aligned}
C_0 &= M_\eta e((X_1X_2)^\beta, f_t) e((X_1X_2)^\alpha, f_d) \\
&= M_\eta (e(g^\beta, f_t) e(g^\alpha, f_d))^s, \\
C_1 &= (X_1X_2)^{a_1 ID_1^* + \cdots a_j ID_j^* + b_1} \\
&= (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^s g_2^{x z_c}, \\
C_2 &= X_1X_2 = g^s g_2^x, \\
C_3 &= (X_1X_2)^{a_0 T_C^* + b_2} = (U^{T_C^*} h_t)^s g_2^{x z_s}.
\end{aligned}$$

このとき，$g^s = X_1$, $z_s = a_0 T_C^* + b_2$, $z_c = a_1 ID_1^* + \cdots + a_j ID_j^* + b_1$ と設定されたことになる．$\mathcal{B}$ はランダムに $a_i, b_1, b_2, a_0 \in \mathbb{Z}_N$ を選んでいる．z_s と z_d の mod p_2 での値は $\mathcal{A}$ にとってランダムに分布している．

以上のことから，$W \in G_{p_1p_3}$ の場合には $\mathcal{A}$ は $Game_{k-1}$ を行うこととなり，$W \in G$ の場合には $\mathcal{A}$ は $Game_k$ を行うこととなる．よって，$\mathcal{B}$ は $\mathcal{A}$ の出力 η' が η と等しい場合に 1，等しくない場合には 0 を出力することによって，仮定 2 に対する利得が ε 以上となることを補題 3 の証明と同様にして示すことができる． （証明終）

補題 5 無視できない値 ε とあるアルゴリズム $\mathcal{A}$ に対して $Game_q Adv_{\mathcal{A}} - Game_{Final} Adv_{\mathcal{A}} = \varepsilon$. となるならば，仮定 3 を利得 ε 以上で破ることができるアルゴリズム $\mathcal{B}$ を構成できる．

証明. $\mathcal{B}$ は入力として $\mathbb{G}$, f, g, g^α, $f^\alpha X_2$, X_3, $g^s Y_2$, Z_2, W を受け取る．$\mathcal{B}$ の目的は $\mathcal{A}$ を利用して，$W = e(g,f)^{\alpha s}$ なのか W は G_T のランダムな要素なのかを見分けることである．

$\mathcal{B}$ はランダムに β，a_0，$a_1, \ldots, a_\ell$，b_1，b_2，$c_2 \in \mathbb{Z}_N$ を選び，公開情報を以下のように設定する．$g = g$，$u_1 = g^{a_1}$, …, $u_\ell = g^{a_\ell}$，$f_d = f$，$f_t = g^{c_2}$，$g_d = g^\alpha$，$g_t = g^\beta$，$h_d = g^{b_1}$，$h_t = g^{b_2}$，$U = g^{a_0}$．$\mathcal{B}$ は公開情報 $params = [N, g, g_d\ (= g^\alpha), g_t\ (= g^\beta), f_d, f_t, h_d, h_t, U, u_1, \ldots, u_\ell, X_3]$ を $\mathcal{A}$ にわたす．

$\mathcal{A}$ のクエリが ID（$ID_1, \ldots, ID_j$）の ID 鍵の生成が必要ならば，$\mathcal{B}$ はランダムに r，t，w，$v_{j+1}, \ldots, v_\ell \in \mathbb{Z}_N$ を選び sf-IK を以下のように構成する．

$$K_1 = g^r (Z_2X_3)^t, \ K_2 = f_d^\alpha (u_1^{ID_1} \cdots u_j^{ID_j} h_d)^r (Z_2X_3)^w,$$
$$E_{j+1} = u_{j+1}^r (Z_2X_3)^{v_{j+1}}, \cdots, E_\ell = u_\ell^r (Z_2X_3)^{v_\ell}.$$

$\mathcal{A}$ が時刻 T_C に対する Release クエリをしてきたら，$\mathcal{B}$ は $\mathcal{B}$ はランダムに $v,t,w \in \mathbb{Z}_N$ を選び，時刻鍵 $R_T = (K_{t,1}, K_{t,2})$ を以下のように構成する．

$$K_{t,1} = g^v X_3^w, \quad K_{t,2} = f_t^\beta (U^{T_C} h_t)^v X_3^t.$$

$\mathcal{A}$ が $\mathcal{B}$ に 2 つの平文 M_0 と M_1，チャレンジ ID $(ID_1^*, \ldots, ID_j^*)$，チャレンジ時刻 T_C^* をわたしてくる．$\mathcal{B}$ は $\eta \in \{0,1\}$ をランダムに選ぶ．$\mathcal{B}$ はチャレンジ暗号文 $C = (C_0, C_1, C_2, C_3)$ を以下のように構成する．

$$C_0 = M_\eta e(g^s Y_2, f_t)^\beta W, \ \ C_1 = (g^s Y_2)^{a_1 ID_1^* + \cdots a_j ID_j^* + b_1},$$
$$C_2 = g^s Y_2, \qquad C_3 = (g^s Y_2)^{a_0 T_C^* + b_2}.$$

この暗号文では $z_c = a_1 ID_1^* + \cdots + a_j ID_j^* + b_1$, $z_s = a_0 T_C^* + b_2$ と置いたことになる．

z_c と z_s の値は mod p_2 でのみ問題となる．$u_1 = g^{a_1}$, …, $u_\ell = g^{a_\ell}$，$h_d = g^{b_1}$，$U = g^{c_3}$，$h_t = g^{b_2}$ は G_{p_1} の要素であるので，a_0，$a_1, \ldots, a_\ell$，b_1，b_2 が mod N でランダムに選ばれているときには a_1, …, a_ℓ, b_1 の mod p_1 での値と $z_c = a_1 ID1^* + \cdots + a_j ID_j^* + b_1$ の mod p_2 での値には関連がなく，a_0，b_2 の mod p_1 での値と $z_s = a_0 T_C^* + b_2$ の mod p_2 での値には関連がない．

もし $W = e(g,g)^{\alpha s}$ であるならばこの暗号文は平文 M_η に対する sf-CT として正しい分布となり，$\mathcal{A}$ は $Game_q$ を行うことになる．もし W が G_T のランダムな要素であるならば，この暗号文はランダムな平文の sf-CT となり，$\mathcal{A}$ は $Game_{Final}$ を行うことになる．よって，$\mathcal{B}$ は $\mathcal{A}$ の出力 η' が η と等しい場合に 1，等しくない場合には 0 を出力することによって，仮定 3 に対する利得が ε 以上となることを補題 3 の証明と同様にして示すことができる．（証明終）

補題 2〜補題 5 より，仮定 1，2，3 が成り立つとき，任意の攻撃者の $Game_{Real}$ と $Game_{Final}$ における利得の差は無視できることが示された．これにより，$Game_{Final}$ の攻撃者の利得は明らかに 0 であることを考えると，$Game_{Real}$ の攻撃者の利得は無視できることが証明できた．

定理 2 仮定 1，2，3 が成り立つとき，提案方式はスタンダードモデルにおいて IND-ID-CPA 安全である．

5.3 IND-TR-CPA 安全性

5.3.1 IND-TR-CPA ゲームに対するゲーム列

ゲーム中になされるクエリの数を q とすると生成される時刻鍵はたかだか q 個である．以下のゲーム列を考える．

$Game_{Real}$：通常の IND-TR-CPA ゲーム．

$Game_k$（$0 \le k \le q$）：チャレンジ暗号文に sf-CT を用い，ID 鍵はつねに IK を用いる．さらに，$0, \ldots, k$ 個目までの Release クエリで生成される時刻鍵に sf-RK を用い，残りの Release クエリで生成される時刻鍵には RK

を用いる．後は $Game_{Real}$ と同じである（$Game_0$ では，Release クエリで生成されるすべての時刻鍵として RK を用い，$Game_q$ では，Release クエリで生成されるすべての時刻鍵として sf-RK を用いることになる）．

$Game_{Final}$：攻撃者から送られてきた 2 つの平文の 1 つを暗号化して返すのではなく，ランダムな平文を暗号化して返す以外は $Game_q$ と同じである．

IND-ID-CPA ゲームの場合と同様に以下の補題が成り立ち，定理 3 が証明できる（証明は紙幅の都合で省略する）．

補題 6 安全性ゲームにおける攻撃者が Release クエリを行う時刻 T_C が，チャレンジ時刻 T_C^* と mod N では異なるが，mod p_2 で等しくなる確率は無視できるくらいに小さい．

補題 7 無視できない値 ε とあるアルゴリズム $\mathcal{A}$ に対して $Game_{Real}Adv_{\mathcal{A}} - Game_0Adv_{\mathcal{A}} = \varepsilon$. となるならば，仮定 1 を利得 ε 以上で破るアルゴリズム $\mathcal{B}$ を構成できる．

補題 8 無視できない値 ε とあるアルゴリズム $\mathcal{A}$ に対して $Game_{k-1}Adv_{\mathcal{A}} - Game_kAdv_{\mathcal{A}} = \varepsilon$（$1 \leq k \leq q$）となるならば，仮定 2 を利得 ε で破るアルゴリズム $\mathcal{B}$ を構成できる．

補題 9 無視できない値 ε とあるアルゴリズム $\mathcal{A}$ に対して $Game_qAdv_{\mathcal{A}} - Game_{Final}Adv_{\mathcal{A}} = \varepsilon$. となるならば，仮定 3 を利得 ε で破るアルゴリズム $\mathcal{B}$ を構成できる．

定理 3 仮定 1，2，3 が成り立つとき，提案方式はスタンダードモデルにおいて IND-TR-CPA 安全である．

6. おわりに

時限機能を付加した階層的 ID ベース暗号方式（TR-HIBE）を提案した．TR-HIBE は，階層構造を持つユーザの ID 情報を公開鍵として持ち，時刻サーバが時刻ごとに放送する時刻鍵を用いなければ，正当な受信者でも復号することのできない，復号可能時刻指定機能を持つ階層的 ID ベース暗号方式である．提案方式はスタンダードモデルにおいて IND-ID-CPA 安全性と IND-TR-CPA 安全性を満たしていることを示した．提案方式は，文献 [7], [8], [9] などの方法を適用することにより，IND-ID-CCA 安全性と IND-TR-CCA 安全性を満たす方式に変換することが可能である．また，文献 [10] の一般的な TR-HIBE の構成法よりも暗号文の長さを抑えることができる．

今後の課題としては，素数位数群を用いた同様な方式の構成が望まれる [13].

参考文献

[1] Boneh, D. and Franklin, M.: Identity-Based Encryption from the Weil Pairing, *CRYPTO 2001, LNCS*, Vol.2139, pp.213–229 (2001).

[2] Gentry, C. and Silverberg, A.: Hierarchical ID-Based Cryptography, *ASIACRYPT 2002, LNCS*, Vol.2501, pp.548–566 (2002).

[3] Cathalo, J., Libert, B. and Quisquater, J.: Efficient and Non-interactive Timed-Release Encryption, *ICICS 2005, LNCS*, Vol.3783, pp.291–303 (2005).

[4] Cheon, J., Hopper, N., Kim, Y. and Osipkov, I.: Timed-Release and Key-Insulated Public Key Encryption, *FC 2006, LNCS*, Vol.4107, pp.191–205 (2006).

[5] 榎本雄介，岸本　渡：時限機能を付加した階層的 ID ベース暗号の具体的構成と安全性の検討，*SCIS 2014*, 3E3-2 (2014).

[6] Lewko, A. and Waters, B.: New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts, *TCC 2010, LNCS*, Vol.5978, pp.455–479 (2010).

[7] Boneh, D. and Katz, J.: Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity Based Encryption, *CT-RSA 2005, LNCS*, Vol.3376, pp.87–103 (2005).

[8] Canetti, R., Halevi, S. and Katz, J.: Chosen-Ciphertext Security from Identity-Based Encryption, *EUROCRYPT 2004, LNCS*, Vol.3027, pp.207–222 (2004).

[9] Boyen, X., Mei, Q. and Waters, B.: Direct Chosen Ciphertext Security from Identity-Based Techniques, *ACM CCS 2005*, pp.320–329 (2005).

[10] Oshikiri, T. and Saito, T.: Timed-Release Hierarchical Identity-Based Encryption, *International Journal of Advanced Computer Science and Applications*, Vol.5 (2014).

[11] 菊池　亮, 藤岡　淳, 岡本義明, 齋藤泰一：公開鍵型 Timed-Release 暗号の安全性考察及び効率的かつ一般的な Pre-Open 機能付き公開鍵型 Timed-Release 暗号の構成，*SCIS 2011*, 2A3-5 (2011).

[12] 笠松宏平，ナッタポンアッタラパドゥン，松田隆宏，花岡悟一郎，今井秀樹：Foward-Secure 暗号を用いた Time-Specific 暗号の一般的構成，*SCIS 2012*, 1A2-5 (2012).

[13] Lewko, A.: Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting, *EUROCRYPT 2012, LNCS*, Vol.7237, pp.318–335 (2012).

[14] Katz, J., Sahai, A. and Waters, B.: Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, *Journal of Cryptology*, Vol.26, pp.191–224 (2013).

岸本 渡　（正会員）

1993 年東京工業大学大学院博士課程修了．博士（工学）．現在，千葉大学大学院准教授．暗号理論，グラフ理論の研究に従事．電子情報通信学会会員．

榎本 雄介

2012 年千葉大学工学部情報画像科学科卒業．2014 年同大学大学院修士課程修了．同年株式会社大都技研入社．暗号理論の研究に従事．