総説

直列型多重暗号の安全性とその応用

藤岡　淳

Sequential Multiple Encryption: Security and Application

Atsushi FUJIOKA*

1．はじめに

1970 年代に公開鍵暗号の概念が提示されたことを契機に現代暗号理論は発展してきた．その中で，各種暗号技術に対して安全性定義を厳密に行い，また，その安全性をなんらかの数学的な問題に帰着させる証明可能安全性が整備されつつある．

機密性のある情報を意図した相手にのみ伝達するために，暗号技術を用いることはよく知られている．その際，送信者と受信者の間で秘密裡に共有されている情報を鍵として暗号化を行なうものが**共通鍵暗号**であるが，この手法を用いた場合，暗号化や復号に用いる鍵をどうやって共有するかという，いわゆる，鍵配送の問題が存在する．

一方，送信者と受信者が保持している鍵が異なっているものが**公開鍵暗号**である．公開鍵暗号では，あるユーザが公開鍵と秘密鍵のペアを生成し，公開鍵を公開し，他のユーザが，そのユーザにメッセージを送信したい場合には，この公開鍵暗号を用いて暗号化を行い，ユーザは自身しか知らない秘密鍵を用いて受信した暗号文を復号するというものである．これにより鍵配送の問題を解決することができる．

公開鍵暗号技術において，その概念の提示以降しばらくは，具体的な方式が提案されては，その安全性の不備が指摘されるといった事例が繰り返されていた．しかし，現在では，その方式が破られた場合に，なんらかの数学的な問題の解が求まることを示すことで暗号技術の安全性を証明しようとする，いわゆる，証明可能安全性の考え方が主流となっている．すなわち，ある数学的な問題の求解が困難であると仮定することで，それに基づく暗号技術の安全性を証明しようという試みである．

多重暗号(ME: Multiple Encryption) [1, 2]とは，この公開鍵暗号方式を多重に用いて安全性を向上させる試みであり，大きく分けて二種類の方式に分類される[1]: **直列型**(sequential type)と**並列型**(parallel type).

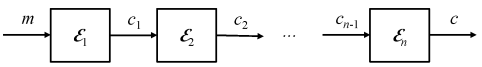

図 1: 直列型多重暗号

直列型とは，平文をある公開鍵暗号方式の暗号化アルゴリズム($\mathcal{E}_i$)で暗号化し，その出力を次の公開鍵暗号方式の暗号化アルゴリズムへの入力として処理を行うもの(図 1)であり，一方，並列型とは，平文をいくつかのピースに分割してそれぞれのピースを平文として複数の公開鍵暗号方式の暗号化アルゴリズムで暗号化するもの(図 2)である．

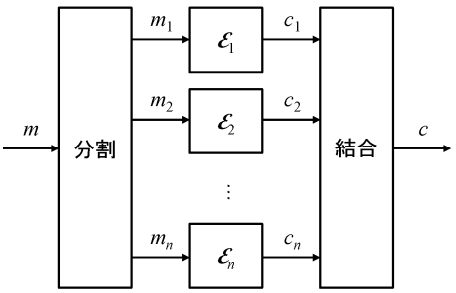

図 2: 並列型多重暗号

従来，素朴なやり方の多重暗号方式は安全でないことが指摘されており，特に，直列型多重暗号では，事前に

*教授　情報システム創成学科
Professor, Department of Information Systems Creation

[1] これらを組み合わせた複合型(hybrid type)も存在する

乱数を指定した方式のみが多重暗号の安全性を個々の公開鍵暗号の安全性に帰着できることが証明されていた[1].

この多重暗号の応用には様々なものがあり，その中に**時限公開鍵暗号**[3]がある．公開鍵暗号では，受信者は自身の秘密鍵で受信した暗号文を直ちに復号することができたが，時限公開鍵暗号では，ある時間を指定した形で暗号文が生成され，受信者は秘密鍵と指定された時間に関連する情報がないと暗号文を開けない，すなわち，指定された時刻まで復号が行なえないというものである．

この時限公開鍵暗号の構成法は二つに分けられ，ある数学的な問題に基づいて具体的な方式を提案する具体的構成法と公開鍵暗号などの一般的な暗号技術を組み合わせて時限公開鍵暗号を構成する一般的構成法が存在する．

本稿は，より素朴なやり方に近い直列型多重暗号方式の構成法[4]とそれに基づく時限公開鍵暗号の一般的構成法[5]をまとめたものである．

2．既存研究

2.1 各種暗号技術

公開鍵暗号(PKE: public-key encryption)とは，あるユーザが公開鍵 pk と秘密鍵 sk のペアを生成し，pk を自身の個人識別情報(以下，ID **情報**と記す)とともに公開し，他のユーザが，そのユーザにメッセージ(平文) m を送信したい場合には，pk を用いて暗号化を行い，ユーザは自身しか知らない sk を用いて受信した暗号文 c を復号するというものである．

公開鍵暗号方式 $\mathcal{PKE}$ は，以下の三つのアルゴリズムからなる．

鍵生成: $(pk, sk) \leftarrow$ PKE. KGen(1^k)．ここで，入力はセキュリティパラメータを k としたときに 1 を k 個並べたもの(1^k と表現する).

暗号化: $c \leftarrow$ PKE. Enc(pk, m). ここで，入力は公開鍵 pk，平文 m.

復号: $m' =$ PKE. Dec(sk, c)．ここで，入力は秘密鍵 sk，暗号文 c.

復号されたメッセージは m' である．

ここで，これら三つのアルゴリズムは入力長に関する多項式時間アルゴリズムであり，結果，k に関する多項式時間アルゴリズムとなる． $b \leftarrow A(a)$は，A が入力を a として b を出力する確率的アルゴリズムであることを意味し，$b = A(a)$ は，A が確定的アルゴリズムであることを示している．確率的アルゴリズムを，ランダム文字列 r を用いて $b = A(a; r)$と書くこともある．

しかし，公開鍵暗号では，秘密鍵所有者のIDと公開鍵に関する認証が必要となる．ある不正者が生成した公開鍵を他人の ID とリンクさせることができれば，その ID 宛の暗号文を自由に復号することができてしまうからである．そこで，ID 情報に基づく暗号が考案された．

ID **情報に基づく暗号**(IBE: Identity-Based Encryption) とは，鍵生成局が，公開情報 *params* とマスター秘密鍵 *msk* のペアを生成し，*params* を公開し，ユーザ ID に対して秘密鍵 sk_{ID} を与え，他のユーザが，そのユーザに平文 m を送信したい場合には，ID (と *params*)を用いて暗号化を行い，ユーザは自身しか知らない sk_{ID} (と *params*)を用いて受信した暗号文 c を復号するというものである．これにより公開鍵認証の問題を解決することができる．

ID 情報に基づく暗号方式 $\mathcal{IBE}$ は，以下の四つの多項式時間アルゴリズムからなる．

設定: (*params; msk*) ← IBE. Setup(1^k)．ここで，入力は 1^k (k はセキュリティパラメータ).

利用者鍵生成: $sk_{\mathrm{ID}} \leftarrow$ IBE. Extract(*params, msk,* ID).
ここで，入力は公開情報 *params*，マスター秘密鍵 *msk*，ID 情報 ID.

暗号化: $c \leftarrow$ IBE. Enc(*params*, ID, m)．ここで，入力は公開情報 *params*，ID 情報 ID，平文 m.

復号: $m' =$ IBE. Dec(*params*; sk_{ID}; c)．ここで，入力は公開情報 *params*，秘密鍵 sk_{ID}，暗号文 c.

復号されたメッセージは m' である．

2.2 暗号の安全性

暗号の安全性は様々に定義されているが，現在，主流となっている定義は識別不可能性に基づくものである．

識別不可能性とは，ある安全性に関するゲームにおいて攻撃者(Adv)が二つの平文 x_0, x_1 に対するどちらかの暗号文 c^* (**挑戦暗号文**と呼ばれる)が与えられたとき，その暗号文がどちらの平文のものかを当てることができないことをいう．

このとき，攻撃者に対して，付加的な情報を与えないものを**選択平文攻撃**(CPA: Chosen Plaintext Attack)，攻撃者から問われた(挑戦暗号文以外の)暗号文に対する平文を答えることを許す**選択暗号文攻撃**(CCA: Chosen Ciphertext Attack)が存在する(ここで，攻撃者から問われた暗号文に対する平文を答える部分を復号オラクルと呼ぶ). 特に，暗号文を適応的に選ぶことができるものを**適応的選択暗号文攻撃**(ACCA: Adaptively ChosenCiphertext Attack)とよび，CCA2 と記することもあるが，そうでないものと混乱することがない場合には，単に CCA と書くこともある．

以上より，公開鍵暗号において，二つの平文を区別で

きないとき IND-CPA 安全といい，攻撃者に復号オラクルを与えても区別できないとき IND-CCA 安全という(図 3).

同様に, ID 情報に基づく暗号においても, IND-ID-CPA 安全のようにいう.

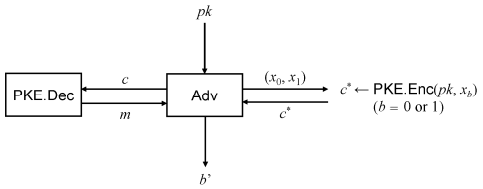

図 3: IND-CCA ゲーム

公開鍵暗号や ID 情報に基づく暗号において IND-CPA 安全な方式から IND-CCA 安全な方式を構成することは, 一般的には難しいが，ランダムオラクルモデル[6]という安全性証明モデルを用いると，比較的容易に実現できることが知られている．ここで，ランダムオラクルモデルとは，ある関数の出力を攻撃者は自身で計算できず，外部からその計算値をもらわなければならないという安全性証明モデルで，例えば，ハッシュ関数などをランダムオラクルとして扱うことにより安全性証明を行うことが多い.

ここで一つ，暗号の性質を表すパラメータを定義しておく．k をセキュリティパラメータ，$\mathcal{PKE}$= (PKE. KGen, PKE. Enc, PKE. Dec)を公開鍵暗号方式とする．与えられた $x \in \{0,1\}^*$, $y \in \{0,1\}^*$, PKE. KGen(1^k)で生成された pk に対して，$\Pr[r \leftarrow \{0,1\}^{rlen(k)} : y = \text{PKE. Enc}(pk; x; r)]$ を $g(x, y)$ で記す(ここで $rlen(k)$ は k に関する多項式であり，暗号化に必要なランダム文字列の長さである). このとき，任意の $x \in \{0,1\}^*, y \in \{0,1\}^*, (pk; sk) \leftarrow$ KGen(1^k) に対して， $g(x, y) \leqq \gamma$ が成り立つならば, $\mathcal{PKE}$ は γ-**一様性**を持つという[10].

この確率 $g(x, y)$ は内部で$(pk, sk) \leftarrow$ KGen(1^k) に関する確率的な振舞を行っている点に注意されたい．すなわち，ある公開鍵暗号方式が，セキュリティパラメータ k に関して無視できる大きさの γ-一様性を持つとき，多くの pk に対して無視できる大きさとなるのであって, すべての pk に対して成り立つ必要はない.

2.3 多重暗号の安全性

多重暗号で，同様に適応的選択暗号文攻撃の元での識別不可能性を考えてみる．すなわち，攻撃者に対して多重暗号に対する復号オラクルが与えられているものとする.

まず，図 1 において，それぞれの暗号化が独立に行われていた場合を考える.

ここで，最終段の暗号 $\mathcal{E}n$ に対する秘密鍵 sk_n を入手した(それ以外の秘密鍵は知らない) 攻撃者を想定する．この攻撃者は自身では，挑戦暗号文を平文まで復号することはできないかもしれないが，最終段 $\mathcal{E}n$ に関しては復号が可能である．そこで，挑戦暗号文に対して，sk_n を用いて復号し，それを再度 $\mathcal{E}n$ に関して暗号化した場合，この暗号が少なくとも IND-CPA 安全であるならば，セキュリティパラメータ k に関して無視できる大きさの γ-一様性を持つので，結果，得られた暗号文は高い確率で挑戦暗号文とは異なることになる．そこで，この暗号文を復号オラクルに尋ねることで平文を入手することができ，最終的に，多重暗号に対する識別不可能性を破ることができる.

このような攻撃を**再暗号化攻撃**といい，素朴な直列型多重暗号方式はこの攻撃に対して脆弱であり，そのために，なんらかの工夫が必要となる.

2.4 多重暗号の定義

多重暗号方式 $\mathcal{ME}^n$は, 以下の三つの多項式時間アルゴリズムからなる.

鍵生成: $(PK^n, SK^n) \leftarrow$ ME.KGen$^n(1^k)$. ここで，入力は 1^k (k はセキュリティパラメータ).

暗号化: $c \leftarrow$ ME.Enc$^n(PK^n, m)$. ここで, 入力は公開鍵 PK^n, 平文 m.

復号: $m' =$ ME.Dec$^n(SK^n, c)$. ここで，入力は秘密鍵 SK^n, 暗号文 c.

復号されたメッセージは m' である.

多重暗号方式 $\mathcal{ME}^n$に対する安全性としては，先に，述べたように多重暗号に対する復号オラクルのみが与えられているモデルが考えられる(図 4). このモデルに基づく安全性は, 独立に提案され, それぞれ, IND-ME-CCA 安全性[1], wMCCA 安全性[2]と呼ばれている．この安全性は, 直列・並列いずれの型の多重暗号にも適用できる.

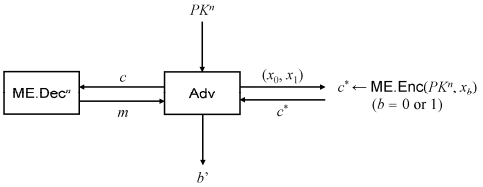

図 4: IND-ME-CCA ゲーム

次に，並列型多重暗号に対してのみ定義可能な安全性

を紹介する．wMCCA 安全性では多重暗号に関する暗号文に対する復号結果を入手可能であったのに対して，MCCA 安全性では，復号結果(平文)ではなく，それを分割したもの(個々の部分情報)が入手でき，sMCCA 安全性では，多重暗号に関する暗号文に対する復号結果だけでなく，(多重暗号を構成している) 個々の公開鍵暗号に対する復号結果も入手できるというモデルである[2].

これらの安全性の関係は,

wMCCA (=IND-ME-CCA) ≦ MCCA ≦ sMCCA

となり，これらの中では，sMCCA 安全性が最も強い安全性となる.

2.5 時限公開鍵暗号

公開鍵暗号においては，暗号文を受信したユーザは自身の秘密鍵を用いて, 直ちに, 復号を行うことができる. そこで，正規のユーザであっても，指定された時刻まで復号が行えない時限公開鍵暗号が考案された.

時限公開鍵暗号(TRPKE: Timed-Release Public-Key Encription) とは, 時報局が, 公開鍵 tpk と秘密鍵 tsk のペアを生成し, tpk を公開し，あるユーザが公開鍵 upk と秘密鍵 usk のペアを生成し， upk を自身の ID と共に公開し，他のユーザが，そのユーザにメッセージ(平文) m を送信したい場合には，upk, tpk と時刻情報 T を用いて暗号化を行い，時刻 T に達したら，時報局が時刻鍵 s_T を発行し，ユーザは自身しか知らない sk と発行された s_T, 公開されていた tpk を用いて受信した暗号文 c を復号するというものである．これにより時刻 T が来るまで，指定されたユーザに対してもメッセージの秘匿性を保つことができる.

このとき，安全性は時報局に対するものとユーザに対するものの二種類を考える必要がある.

それぞれに対して，適応的選択暗号文攻撃の元で識別不可能性を満足ことが望ましく，また，その際，復号オラクルに対して，様々なユーザの公開鍵を選べるようにするより強い安全性を考慮する必要がある.

2.6 時限公開鍵暗号の定義

時限公開鍵暗号方式 $\mathcal{TRPKE}$ は，以下の五つの多項式時間アルゴリズムからなる.

設定: $(tpk, tsk) \leftarrow$ TRE. Setup(1^k). ここで, 入力は 1^k(k はセキュリティパラメータ).

利用者鍵生成: $(upk; usk) \leftarrow$ TRE. KGen(tpk). ここで，入力は時報局の公開鍵 tpk.

解除: $s_T \leftarrow$ TRE. Release(tpk, tsk, T). ここで，入力は時報局の公開鍵 tpk，時報局の秘密鍵 tsk，時刻情報 T.

暗号化: $c \leftarrow$ TRE. Enc(tpk, T, upk, m). ここで，入力は時報局の公開鍵 tpk，時刻情報 T，ユーザの公開鍵 upk，平文 m.

復号: $m' =$ TRE. Dec(tpk, s_T, usk, c), 入力は時報局の公開鍵 tpk，時刻鍵 s_T ，ユーザの秘密鍵 usk，暗号文 c.
復号されたメッセージは m' である.

時限公開鍵暗号に対する安全性としては，先に，述べたように時報局に対するものとユーザに対するものの二種類を考える必要があるが，それぞれに二つの安全性が定義されている.

IND-RTR-CCA2 安全性[7]は，時報局の秘密鍵を持たない攻撃者が時限公開鍵暗号の識別不可能性を破ろうとするもので，復号オラクルへの問い合わせに際に，暗号文 c と共に，時刻情報 T とその暗号文の受信者における秘密鍵 usk を送信するモデルである．一方，IND-CTCA 安全性[8]は，復号オラクルへの問い合わせに際に，受信者における秘密鍵 usk ではなく，受信者における公開鍵 upk を付加するモデルである(図 5). IND-CTCA 安全性では，攻撃者は upk に対する秘密鍵を入手していなくてもよく，そのため， IND-CTCA 安全性は IND-RTR-CCA2 安全性よりも強い安全性を保証できる.

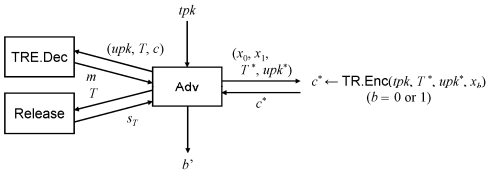

図 5: IND-CTCA ゲーム

IND-CCA-TS 安全性[7, 8]は，不正な時報局が正規のユーザに関する時限公開鍵暗号の識別不可能性を破ろうとするもので，復号オラクルへの問い合わせに際に，暗号文 c と共に，時刻情報 T と時刻鍵 s_T を送信するモデルである[2]. 一方，IND-SCCA-TS 安全性[9]は，復号オラクルへの問い合わせに際に，時刻鍵 s_T ではなく，受信者における公開鍵 upk を付加するモデルである(図 6). IND-CCA-TS 安全性では，攻撃者は指定されたユーザに関する質問しかできないため，IND-SCCA-TS 安全性は IND-CCA-TS 安全性よりも強い安全性を保証できる.

[2] Cathalo による IND-CCA-TS 安全性の定義[8]では，s_T を付加しているのに対して，Cheon らによる IND-CCA-TS 安全性の定義[7]では，s_T を付加していない．しかし，時報局に対する安全性を考慮しているので, s_T を付加する必要はないことに注意されたい.

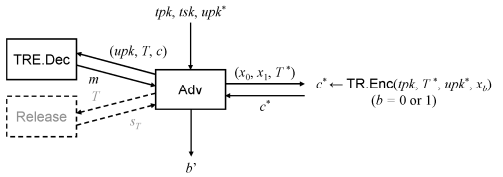

図 6: IND-SCCA-TS ゲーム

以上より，時限公開鍵暗号の安全性は以下の関係となる．

IND-RTR-CCA2 ≦ IND-CTCA

IND-CCA-TS ≦ IND-SCCA-TS

また，それぞれの安全性定義の違いを表 1 にまとめておく．

表 1: 時限公開鍵暗号の安全性

定義	攻撃者	問い合わせの形式
IND-RTR-CCA2	受信者	(*usk*, *T*, *c*)
IND-CTCA	受信者	(*upk*, *T*, *c*)
IND-CCA-TS	時報局	(*T*, s_T, *c*)
IND-SCCA-TS	時報局	(*upk*, *T*, *c*)

3．直列型多重暗号の一構成法

3.1 概要

素朴な直列型多重暗号方式は再暗号化攻撃に対して脆弱であり，これを回避するやり方として，直列型多重暗号における各段の暗号化に必要なランダム文字列を事前に指定する構成法が提案されていた．

本章では，この構成法よりもより素朴な直列型多重暗号方式に近く，暗号化に必要な情報は直前の暗号文だけでよい方式[4]を紹介し，この方式が IND-ME-CCA 安全性に加えてより強い安全性も満足することを示す．

3.2 IND-sME-CCA 安全性

並列型多重暗号方式に対しては，多重暗号方式に関する暗号文に対する復号結果だけでなく，(多重暗号方式を構成している)個々の公開鍵暗号方式に対する復号結果も入手できるという sMCCA 安全性が定義されていた．

そこで，同様に直列型多重暗号方式に対しても，類似の安全性を定義する．すなわち，多重暗号方式に関する暗号文に対する復号結果だけでなく，(多重暗号方式を構成している)個々の公開鍵暗号方式に対する復号結果も入手できるとするもので，これを **IND-sME-CCA 安全性**という(図 7).

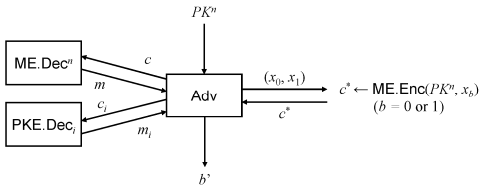

図 7: IND-sME-CCA ゲーム

この安全性と sMCCA 安全性の相違点は，個々の公開鍵暗号方式に関する復号オラクル(PKE. Dec$_i$)に対する禁止事項である．sMCCA 安全性では，挑戦暗号文に関する部分情報の暗号文が問い合わせ不可なのに対して，IND-sME-CCA 安全性では，挑戦暗号文の復号列($c^* \rightarrow c^*_{n-1} \rightarrow \cdots \rightarrow c^*_1$) に属する暗号文($c^*_i$) を問い合わせすることは許されない．

3.3 乱数性拘束構成

以下に，**乱数性拘束構成**と呼ぶ多重暗号の直列構成を記述する[3].

$\mathcal{PKE}_i$ = (PKE. KGen$_i$, PKE. Enc$_i$, PKE. Dec$_i$) ($1 \leqq i \leqq n$, $n \geqq 2$) を公開鍵暗号方式，H_{h_i} ($1 \leqq i \leqq n$) を $\{0,1\}^*$ から $\{0,1\}^{rlen_i(k)}$ へのハッシュ関数とする．ここで，$rlen_i(k)$, $ilen_i(k)$ は k に関する多項式，$ilen_i(k)$ はハッシュ関数のインデックスの長さ，$rlen_i(k)$ は PKE.Enc$_i$ で用いられるランダム文字列の長さの上限，h_i はハッシュ関数のインデックスであり $\{0,1\}^{ilen_i(k)}$ から選ばれる．

このとき，多重暗号方式 $\mathcal{ME}^n$ = (ME.KGen^n, ME.Enc^n, ME.Dec^n) を以下のように構成する．

鍵生成 ME.KGen^n: 入力は 1^k (k はセキュリティパラメータ).

Step 1: PKE. KGen$_i$ に 1^k を入力し，(pk_i, sk_i) を生成($i = 1, \ldots, n$).

Step 2: ハッシュ関数のインデックス$h_i \in \{0,1\}^{ilen_i(k)}$をランダムに選択($i = 1, \ldots, n$).

Step 3: $PK_i = (pk_i, h_i)$, $SK_i = (sk_i, h_i)$ に設定 ($i = 1, \ldots, n$).

Step 4: $PK^n = (PK_1, \ldots, PK_n)$ に設定.

Step 5: $SK^n = (SK_1, \ldots, SK_n)$ に設定.

Step 6: (PK^n, SK^n) を出力.

$\mathcal{ME}^n$ の公開鍵は PK^n, 対応する秘密鍵は SK^n である．

[3] 正確には，文献[4]に記述された乱数性拘束構成と藤崎-岡本変換[10]を合成したものとなっている．この変更により，構成要素をすべて IND-CPA 安全な公開鍵暗号から IND-ME-CCA 安全な多重暗号を構成できることが[4]において指摘されている．

暗号化 $\mathrm{ME.Enc}^n$: 入力は公開鍵 PK^n, メッセージ m,
ランダム文字列 $r \in \{0,1\}^{rlen^n(k)}$. ここで $rlen^n(k)=rlen_1(k)$.
Step 1: PK^n を $(PK_1,\ldots,PK_n)$ に展開.
Step 2: PK_i を (pk_i, h_i) に展開$(i=1,\ldots,n)$.
Step 3: $c_0 = m \,||\, r$ に設定.
Step 4: $i=1$ から n まで以下を繰り返す:
$c_i = \mathrm{PKE.Enc}_i(pk_i, c_{i-1}; H_{hi}(c_{i-1}))$ を実行.
Step 5: $c=c_n$ に設定し，c を出力.
c が m の暗号文である.

復号 $\mathrm{ME.Dec}^n$: 入力は秘密鍵 SK^n, 暗号文 c'.
Step 1: SK^n を $(SK_1,\ldots,SK_n)$ に展開.
Step 2: SK_i を (sk_i, h_i) に展開$(i=1,\ldots,n)$.
Step 3: $c'_n = c'$ に設定.
Step 4: $i=n$ から 1 まで以下を繰り返す:
$c'_{i-1} = \mathrm{PKE.Dec}_i(sk_i, c'_i)$ を実行.
$c'_i = \mathrm{PKE.Enc}_i(pk_i, c'_{i-1}; H_{hi}(c'_{i-1}))$ の成立を確認.
不成立の場合は，$\perp$ を出力して停止.
Step 5: c'_0 を $m' \,||\, r'$ に展開し，m' を出力.
復号されたメッセージは m' である.

3.4 乱数性拘束構成による多重暗号の安全性

乱数性拘束構成による多重暗号の復号過程においては, $c'_i = \mathrm{PKE.Enc}_i(pk_i, {}_{i\text{-}1}c' ; H_{hi}({}_{i\text{-}1}c'))$ の成立が確認される必要があるが，この暗号化は入力 ${}_{i\text{-}1}c'$ に関して確定的な操作となっている．すなわち，挑戦暗号文を再暗号化しても元の暗号文に戻ることになり．これは再暗号化攻撃が有効にはならないことを意味している.

実際に，乱数性拘束構成による多重暗号の安全性は，以下の二定理にて証明される.

定理 1 公開鍵暗号方式 $\mathcal{PKE}_1,\ldots,\mathcal{PKE}_n$ $(n \geq 2)$ がすべて IND-CPA 安全であるとする．このとき，多重暗号方式 $\mathcal{ME}^n$ はランダムオラクルモデルの元で IND-ME-CCA 安全となる.

二つの攻撃者を構成することで証明を行う.

一つは，$\mathcal{ME}^n$ の IND-ME-CCA 安全性を破る攻撃者から $\mathcal{PKE}_1$ の IND-CPA 安全性を破る攻撃者を構成するもので，もう一つは，$\mathcal{ME}^n$ の IND-ME-CCA 安全性を破る攻撃者から $\mathcal{PKE}_i$ $(2 \leqq i \leqq n)$ の IND-CPA 安全性を破る攻撃者を構成するものである.

これらが構成できるということは，$\mathcal{PKE}_i$ が IND-CPA 安全であることに反し，よって，そのような $\mathcal{ME}^n$ の IND-ME-CCA 安全性を破る攻撃者が存在しないことを意味している．結果，$\mathcal{ME}^n$ の IND-ME-CCA 安全性が証明されたことになる.

ここで，どちらの場合も，$\mathcal{PKE}_i$ がセキュリティパラメータ k に関して無視できる大きさの γ-一様性を持つことを証明に利用していることを指摘しておく.

定理 2 公開鍵暗号方式 $\mathcal{PKE}_1,\ldots,\mathcal{PKE}_n$ $(n \geqq 2)$ がすべて IND-CCA 安全であるとする．このとき，多重暗号方式 $\mathcal{ME}^n$ はランダムオラクルモデルの元で IND-sME-CCA 安全となる.

この定理も二つの攻撃者を構成することで証明できる．すなわち，一つは，$\mathcal{ME}^n$ の IND-sME-CCA 安全性を破る攻撃者から $\mathcal{PKE}_1$ の IND-CCA 安全性を破る攻撃者を構成するもので，もう一つは，$\mathcal{ME}^n$ の IND-sME-CCA 安全性を破る攻撃者から $\mathcal{PKE}_i$ $(2 \leqq i \leqq n)$ の IND-CCA 安全性を破る攻撃者を構成するものである.

4．時限公開鍵暗号の一構成法

4.1 概要

先にのべたように時限公開鍵暗号の安全性として強い定義となっているのは，IND-CTCA 安全性と IND-SCCA-TS 安全性である．この両者を満たす方式として，ある数論上の問題に基づく方式が提案されている[9]が，これは具体的構成であって，公開鍵暗号方式と ID 情報に基づく暗号方式を組み合わせて構成するような一般的構成ではなかった.

本章では，乱数性拘束構成に基づく時限公開鍵暗号の構成法について記述する．本構成は，二段の乱数性拘束構成において，一段目を ID 情報に基づく暗号方式，二段目を公開鍵暗号方式と見なすことができる．この際，乱数性拘束構成においては，ハッシュ関数への入力を直前の情報(暗号文ないしは平文とランダム文字列を連結したもの)のみに限定して暗号化に必要なランダム文字列を生成していたが，ここで記述する時限公開鍵暗号の構成法においては，直前の情報に加えて，受信者の公開鍵や時刻情報もハッシュ関数への入力としている．このような変更を加えることにより IND-CTCA 安全性や IND-SCCA-TS 安全性で求められていた攻撃者が復号オラクルに問い合わせる暗号文において公開鍵や時刻情報を自由に選ぶことができるという点に対応することができる.

しかし，そのために，公開鍵暗号や ID 情報に基づく暗号に求められる性質としては，「セキュリティパラメータ k に関して無視できる大きさの γ-一様性を持つ」というものだけでは不十分となり，これをより強くした「無視できる大きさの γ-pk-**一様性**を持つ」という性質が必要となる．ここで，γ-pk-一様性とは，γ-一様性で定義された確率 $g(x,y)$ の上限 γ がすべての pk に対して成

り立つとしたものとして定義される．すなわち，無視できる大きさの γ-一様性を持つ公開鍵暗号方式の場合，無視できる数の公開鍵に対しては，γ が無視できる大きさを超えてもよいが，無視できる大きさの γ-pk-一様性を持つ公開鍵暗号方式の場合，すべての公開鍵おいて γ が無視できる大きさとならなければならない．

4.2 乱数性拘束構成を用いた時限公開鍵暗号

$\mathcal{PKE}$ = (PKE. KGen, PKE. Enc, PKE. Dec) を公開鍵暗号方式 $\mathcal{IBE}$ = (IBE.Setup, IBE.Extract, IBE.Enc, IBE.Dec) をID情報に基づく暗号方式，H_{h1} を $\{0,1\}$*から $\{0,1\}^{ibe.rlen(k)}$ へのハッシュ関数，H_{h2} も $\{0,1\}$*から $\{0,1\}^{pke.rlen(k)}$ へのハッシュ関数とする．ここで，$ilen_1(k)$, $ilen_2(k)$, $ibe.rlen(k)$, $pke.rlen(k)$を k に関する多項式，$ilen_i(k)$はハッシュ関数のインデックスの長さ，$ibe.rlen_i(k)$, $pke.rlen_i(k)$ は IBE. Enc, PKE. Enc で用いられるランダム文字列の長さの上限，h_i はハッシュ関数のインデックスであり $\{0,1\}^{ilen_i(k)}$ から選ばれる．このとき，多くの公開鍵暗号方式，ID 情報に基づく暗号方式がそうであるように，pk や $params$ からセキュリティパラメータ k が導出できると仮定しておく．

このとき，時限公開鍵暗号方式 $\mathcal{TRPKE}$ =(TRE. Setup, TRE. KGen, TRE. Release, TRE. Enc, TRE. Dec) を以下のように構成する．

設定 TRE. Setup: 入力は 1^k (k はセキュリティパラメータ).

Step 1: IBE.Setup に 1^k を入力し, ($params$, msk) を生成.

Step 2: ハッシュ関数のインデックス $h_1 \in \{0,1\}^{ilen1(k)}$ と $h_2 \in \{0,1\}^{ilen2(k)}$をランダムに選択.

Step 3: $tpk = (params, h_1, h_2)$, $tsk = msk$ に設定.

Step 4: (tpk, tsk)を出力.

$\mathcal{TRPKE}$ における時報局の公開鍵は tpk であり，対応する秘密鍵は tsk である.

利用者鍵生成 TRE. KGen: 入力は tpk.

Step 1: tpk を($params, h_1, h_2$) に展開し，$params$ からセキュリティパラメータ k を導出.

Step 2: PKE. KGen に 1^k を入力し，(pk, sk) を生成.

Step 3: $upk = pk$, $usk = (pk; sk)$ に設定.

Step 4: (upk, usk) を出力.

$\mathcal{TRPKE}$ における利用者の公開鍵は upk であり，対応する秘密鍵は usk である.

解除 TRE. Release: 入力は時報局の公開・秘密鍵(tpk, tsk) と時刻情報 T.

Step 1: tpk を($params, h_1, h_2$) に展開.

Step 2: d_T = IBE. Extract($params$, tsk, T) を実行.

Step 3: $s_T = d_T$ に設定し，s_T を出力.

時刻情報 T に対する時刻鍵は s_T である.

暗号化 TRE:Enc: 入力は時報局の公開鍵 tpk, 時刻情報 T, 利用者の公開鍵 upk (= pk), メッセージ m, ランダム文字列 $r \in \{0,1\}^{tre.rlen(k)}$.

Step 1: tpk を($params, h_1, h_2$) に展開.

Step 2: 以下を計算:

$\dot{c}$= IBE. Enc($params$, T, $m||r$; H_{h1} ($pk||T||m||r$))

Step 3: $\ddot{c}$ = PKE. Enc(pk, $\dot{c}$; H_{h2} ($pk||T||\dot{c}$)) を計算.

Step 4: $c = \ddot{c}$ に設定し，c を出力.

c が m の暗号文である.

復号 TRE. Dec: 入力は時報局の公開鍵 tpk, 時刻鍵 s_T, 利用者の秘密鍵 usk, 暗号文 c.

Step 1: tpk を($params, h_1, h_2$) に展開.

Step 2: usk を(pk, sk) に展開.

Step 3: $\ddot{c}' = c'$ に設定.

Step 4: $\dot{c}'$ = PKE. Dec(sk, $\ddot{c}'$) を計算.

Step 5: $\ddot{c}'$ = PKE. Enc(pk, $\dot{c}'$; H_{h2} ($pk||T||\dot{c}'$)) の成立を検証し，不成立なら，$\perp$ を出力し，停止.

Step 6: m' = IBE. Dec($params$; s_T, $\dot{c}'$) を計算.

Step 7: $\dot{c}'$ = IBE. Enc($params$; T, m' ;H_{h1} ($pk||T||m'$))の成立を検証し，不成立なら，$\perp$ を出力し，停止.

Step 8: m' を m'' || r'' に展開.

Step 9: m''を出力.

復号されたメッセージは m''である.

この構成を **IBE-PKE 構成**と呼ぶ.

4.3 IBE-PKE 構成による時限公開鍵暗号の安全性

IBE-PKE 構成による$\mathcal{TRPKE}$は IND-CTCA 安全性と IND-SCCA-TS 安全性を満足する.

定理 3 ID 情報に基づく暗号方式 $\mathcal{IBE}$が IND-ID-CPA 安全，公開鍵暗号方式$\mathcal{PKE}$が IND-CPA 安全で，かつ，セキュリティパラメータ k に関して無視できる大きさの γ-pk-一様性を持つと仮定する．このとき，時限公開鍵暗号方式 $\mathcal{TRPKE}$ はランダムオラクルモデルの元で IND-CTCA 安全となる.

定理 4 ID 情報に基づく暗号方式$\mathcal{IBE}$が IND-ID-CPA 安全，公開鍵暗号方式$\mathcal{PKE}$が IND-CPA 安全で，かつ，セキュリティパラメータ k に関して無視できる大きさの γ-pk-一様性を持つと仮定する．このとき，時限公開鍵暗号方式$\mathcal{TRPKE}$はランダムオラクルモデルの元で IND-SCCA-TS 安全となる.

これらの定理の証明は，**定理 1, 2** の証明とほぼ同様に行うことができる.

５．まとめにかえて

乱数性拘束構成を用いた多重暗号の構成とそれを利用した時限公開鍵暗号の構成について述べた．

時限公開鍵暗号には，受信者が指定時刻前に復号したかった場合，送信者が時間前復号鍵を受信者に送信することで復号が可能となる機能を持つ**時間前開封機能付**時限公開鍵暗号と呼ばれる拡張が存在する．

本稿で紹介した IBE-PKE 構成では時間前開封機能を実現することは難しいが，暗号化の順番を入れ換え PKE-IBE 構成とした場合には，時間前開封機能付時限公開鍵暗号が実現できることが文献[11]に指摘されている．

謝辞

本稿で紹介した多重暗号とその応用に関する一連の研究は東京電機大学工学部齊藤泰一教授との共同研究の成果である．本報をまとめるにあたり研究成果の一部を転載することを快諾頂き感謝する．

参考文献

(1) R. Zhang, G. Hanaoka, J. Shikata, and H. Imai, “On the Security of Multiple Encryption or CCA-security + CCA-security = CCA-security?”, PKC 2004 (LNCS 2947), Springer, (2004), pp.360-374.

(2) Y. Dodis and J. Katz, “Chosen-Ciphertext Security of Multiple Encryption”, TCC 2005 (LNCS 3378), Springer, (2005), pp.188-209.

(3) A.C-F. Chan and I.F. Blake, “Scalable, Server-Passive, User-Anonymous Timed Release Public Key Encryption from Bilinear Pairing”, ICDCS 2005, IEEE, (2005), pp.504-513.

(4) A. Fujioka, Y. Okamoto, and T. Saito, “Security of Sequential Multiple Encryption”, IEICE Transactions on Fundamentals, E95-A (1), (2012-01), pp.57-69.

(5) A. Fujioka, Y. Okamoto, and T. Saito, “Generic Construction of Strongly Secure Timed-Release Public-Key Encryption”, IEICE Transactions on Fundamentals, E96-A (1), (2013-01), pp.76-91.

(6) M. Bellare and P. Rogaway, “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”, ACMCCS '93, ACM, (1993) , pp. 62-73.

(7) J.H. Cheon, N. Hopper, Y. Kim, and I. Osipkov, “Timed-Release and Key-Insulated Public Key Encryption”, FC 2006 (LNCS 4107), Springer, (2006), pp.191-205.

(8) J. Cathalo, B. Libert, and J. J. Quisquater, “ Effcient and Non-Interactive Timed-Release Encryption”, ICICS 2005 (LNCS 3783), Springer, (2005), pp.291-303.

(9) S.S.M. Chow and S.-M. Yiu, “Timed-Release Encryption Revisited”, ProvSec 2008 (LNCS 5324), Springer, (2008), pp.38-51.

(10) E. Fujisaki and T. Okamoto, “How to Enhance the Security of Public-Key Encryption at Minimum Cost”, PKC '99 (LNCS 1560), Springer, (1999), pp. 53-68.

(11) R. Kikuchi, A. Fujioka, Y. Okamoto, and T. Saito, “Strong Security Notions for Timed-Release Public-Key Encryption Revisited”, ICISC 2011 (LNCS 7259), Springer, (2012), pp.88-108.