修士論文

公開鍵暗号の平文保持型暗号文変換可能なCCA環境下での安全性概念間の関係性に関する研究

A Study on Relations among Notions of Security under Replayable CCA Environment for Public-Key Encryption

指導教員　　松浦幹太　教授

東京大学大学院 情報理工学系研究科 電子情報学専攻

48-176429　　林田 淳一郎

平成31年1月29日提出

内容梗概

現代社会ではインターネットの急速な普及にともない, 様々な情報がネットワークを介して伝送されるようになっている. その結果, 情報セキュリティへの関心とその重要性が高まっている. 情報の秘匿性や完全性などの確保に暗号技術が用いられ, 安全な暗号技術は情報化社会において必要不可欠な存在である.

暗号技術の安全性は, 安全性の達成度のモデルと, 攻撃者の攻撃法のモデルの二つの強度を考えることによって捉えることができる. 例えば, 公開鍵暗号の安全性の達成度の一つに秘匿性と呼ばれる安全性がある. 秘匿性は, 暗号文から平文の情報が漏れていないことを保証する. また, 秘匿性の他には頑強性 (Non-Malleability, NM) と呼ばれる安全性がある. 頑強性は, 暗号文に対し悪意のある改変をすることができないという事を保証する安全性である. 攻撃者のモデルの例としては, 選択平文攻撃 (Chosen Plaintext Attack, CPA) や, 適応的選択暗号文攻撃 (Adaptive Chosen Ciphertext Attack, CCA2) などが挙げられる. このように, 公開鍵暗号の概念が提案されてから現在に至るまで, 様々な安全性の達成度と攻撃者のモデルが提案されている.

本稿では攻撃者のモデルの中でも平文保持型暗号文変換可能な CCA 環境 (Replayable CCA, RCCA) における安全性概念間の関係性を取り上げる. RCCA 環境では, 攻撃者が特定の暗号文を復号クエリした場合に, 復号オラクルが特殊なシンボル “Test” を返すという定式化がされている. この定式化は, 暗号文のリプレイを許容する定式化になっており, 暗号文の再ランダム化が可能な方式を取り扱うことができる. また, RCCA 安全性は認証や鍵交換といった多くの応用において十分であることが示されている. そのため, 暗号技術の現実世界での使用を考える際には RCCA 安全性は重要な安全性である.

RCCA 安全性を提案した Canetti らは, 三つの安全性 IND-RCCA, NM-RCCA, UC-RCCA を定式化した. そして, 平文空間のサイズが十分大きい場合にこの三つが等価であることを証明した. しかし, 彼らの定式化した NM-RCCA は, 既存の NM-CCA の自然な拡張にはなっておらず, その妥当性が不明である.

そこで本研究では, RCCA 環境下におけるより自然なシミュレーションベースの頑強性及び, 識別不可能性ベースの頑強性の定式化を行い, その等価性を明らかにする. さらに, Canetti らが提案している既存の IND-RCCA と本稿で提案する二つの頑強性の等価性を明らかにする.

目次

Chapter 1　序論

1.1　暗号技術と安全性

現代のネットワーク技術の進歩に伴い, 社会の電子化のための一つの重要な要素として, 情報セキュリティへの関心は以前にも増して高まっている. 公開鍵暗号 (Public-Key Encryption, PKE) は, 通信を行う二者間で事前に秘密情報の共有が必要であった共通鍵暗号の欠点を克服した暗号技術である. 共通鍵暗号では, 暗号化と復号に用いる鍵が同じ鍵であったのに対し, 公開鍵暗号では, 暗号化と復号に用いる鍵を分けることにより, 暗号化に用いる鍵を広く公開することができる. この暗号化鍵を用いて平文を暗号化し通信を行うことで, 当事者間での事前の鍵共有なしで安全な通信が可能となる. この公開鍵暗号の技術は, SSL/TLS のようにインターネット上の通信の秘匿性を保つ役割を果たしており, プロトコルの根幹を担っている.

公開鍵暗号は Diffie と Hellman による提唱 [23] 以降, 構成や安全性に関する研究が現在に至るまで盛んに研究されている. 暗号技術の安全性は, 安全性の達成度と攻撃者の攻撃法のモデルの二つの強度を考えることによって捉えることができる. 例えば, 公開鍵暗号の安全性の達成度の一つに秘匿性と呼ばれる安全性がある. 秘匿性は, 暗号文から平文の情報が漏れていないことを保証する. また, 秘匿性の他には頑強性 (Non-Malleability, NM) と呼ばれる安全性がある. 頑強性は, 暗号文に対し悪意のある改変をすることができないという事を保証する安全性である. 攻撃者のモデルの例としては, 選択平文攻撃 (Chosen Plaintext Attack, CPA) や, 適応的選択暗号文攻撃 (Adaptive Chosen Ciphertext Attack, CCA2) などが挙げられる. このように, 公開鍵暗号の概念が提案されてから現在に至るまで, 様々な安全性の達成度と攻撃者のモデルが提案されている.

1.2　証明可能安全性

あらゆる暗号技術は, 現在知られている困難な問題に基づくなどして, 証明可能安全性を持つことが望ましい. 証明可能安全性とは, 暗号の安全性を形式的に定義し, 数学的に解くことが困難とされている問題について言及し, その問題を解くことができないという仮定を利用して定義の範囲内の安全の有無を判断できるようにするものである. ある暗号技術の安全性の証明がないことが必ずしも安全ではないということを直接意味するわけではない. しかし, 経験則による安全性の議論を排除し, 客観的な安全性の議論を行うために, 現在では安全性の証明をつけることがほぼ必須となっている. 安全性証明を行うためには, 示したい安全性の達成度のモデル, 攻撃者の攻撃法のモデル, 根拠とする困難な問題の形式的な定義を行う必要がある. 根拠となる問題は, 素因数分解問題や離散対数問題などといった, 長くにわたって困難であると信じられている数

学的問題を使うことが多い. 安全性を証明したければ, “現実に知られている難しい問題の困難性の仮定が成り立つならば、安全性を無視できない確率で破るアルゴリズムが存在しない”, ということを示せばよい. また, 証明の際にはその対偶を示す. すなわち, “安全性証明をしたい暗号方式の安全性を無視できない確率で破る確率的多項式時間アルゴリズムが存在するならば, そのアルゴリズムを利用して現実に知られている困難な問題を解くことができる” という事を示すことにより, 問題の困難性の仮定を破ることから背理法により安全性を破る攻撃者は存在しない, という手法を利用する. 確率的多項式時間アルゴリズムは現実に存在するアルゴリズムの能力を表しており, この場合は方式の安全性を決定するセキュリティパラメータに対して多項式時間である.

1.3　本研究の目的と貢献

目的　公開鍵暗号技術の安全性に関する研究は, 情報セキュリティへの関心とその重要度が高まっているため, 非常に重要な研究の一つであるといえる. 本研究では, 公開鍵暗号における安全性の内, 平文保持型暗号文変換可能な CCA (RCCA) と呼ばれる攻撃者のモデルに注目する. この RCCA 環境における攻撃者の下で様々な安全性の達成度のモデルが提案されている. しかし, 現在使用されている RCCA 環境下での頑強性の定式化は, 従来の頑強性の直感を捉えた定式化になっていないという問題がある. 定式化の妥当性が明らかでない頑強性を用いて暗号方式の安全性証明を行った場合, その暗号方式が本当に悪意のある改変に耐性があるのかどうかを判断できない. そのため, 定義の妥当性が明らかでないような安全性モデルの使用は危険である. そこで本研究では, RCCA 環境下におけるより自然で頑強性の直感を捉えた定式化を行い, 上記の問題を解決することを目的とする.

貢献　現在使用されている RCCA 環境下での頑強性の定式化を見直し, より頑強性の直感を捉えた自然な RCCA 環境下での頑強性の定式化を行った. なお, 従来の頑強性の定式化と同様に, シミュレーションベースの定式化及び, 識別不可能性ベースの定式化を行った. また, Canetti らが提案している既存の IND-RCCA と本稿で提案する二つの頑強性の等価性を明らかにした. さらに, RCCA 環境下でのシミュレーションベースの頑強性の定式化を応用し, RCCA 環境下での意味論的安全性を定式化した. RCCA 環境下での意味論的安全性の定式化はこれまでされていなかったため, この定式化を行ったことも貢献の一つといえる. これに加えて, RCCA 環境下での意味論的安全性についても IND-RCCA との等価性を明らかにした.

本研究によって明らかになった安全性概念間の関係性を以下の図 1.1 に示す.

1.4　本稿の構成

以下 2 章では, 3 章以降で必要になる暗号要素技術や安全性定義を概要と共に説明する. 3 章では, 公開鍵暗号における安全性の達成度のモデルと攻撃者の攻撃法のモデルについて, そして RCCA 安全な方式構成に関する関連研究を紹介する. 4 章では, 本稿

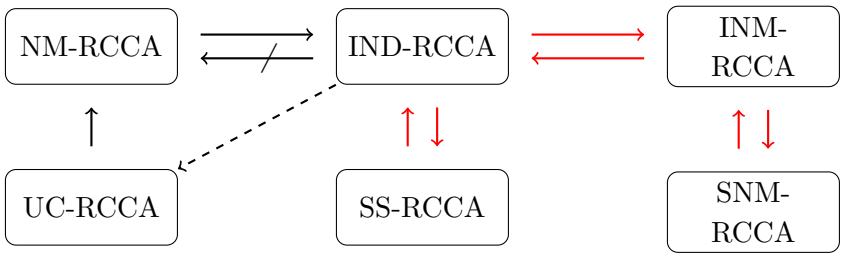

図 1.1: RCCA 環境における安全性概念間に関する本研究の結果と過去の結果の概要. SNM-RCCA と INM-RCCA は, それぞれ本稿で提案するシミュレーションベースと識別不可能ベースの頑強性である. SS-RCCA は本稿で提案する意味論的安全性である. 実線の矢印は含意を表す. 赤い矢印は本研究によって得られた結果を表している. 破線の矢印は, 平文空間が多項式より大きい PKE 方式に対する含意を表している. IND-RCCA から NM-RCCA への矢印は, IND-RCCA 安全であるが NM-RCCA 安全ではない PKE 方式が存在し, その平文空間のサイズが多項式であることを表している.

で提案する頑強性の定式化を示し, その安全性モデルに関するいくつかの証明を示す. 5 章では, 本稿で提案する意味論的安全性の定式化を示し, その安全性モデルに関する二つの証明を示す. 6 章は本稿のまとめである.

なお, 4 章及び 5 章の内容は, 査読なし国内会議 SCIS2019(発表文献 iii) において発表した.

Chapter 2　準備

本章では, 公開鍵暗号と代表的な安全性について, その概要と定義を述べる. また, 本研究にて取り扱う RCCA 安全性についても, 同様にしてその概要と定義を与える.

本稿で使用する記号の定義　本稿では確率的多項式時間アルゴリズムを PPTA と表記する. アルゴリズム A に対し, A が入力として a を与えられ b を出力する手続きを $b \leftarrow A(a)$ と表記する. また, 集合 $\mathcal{S}$ に対し, $\mathcal{S}$ に含まれる要素数を $\|\mathcal{S}\|$ と表記する.

差異補題　A, B 及び E を事象とする. $\Pr[A \wedge \neg E] = \Pr[B \wedge \neg E]$ ならば, $|\Pr[A] - \Pr[B]| \leq \Pr[E]$ が成立する.

無視可能関数　関数 $f : \mathbb{N} \to \mathbb{R}$ に関して, $f(k) < \epsilon(k)$ とは, 任意の定数 $c > 0$ に対して, $n \in \mathbb{N}$ が存在し, 任意の $k > n$ に対して $f(k) < k^{-c}$ が成立することをいう. このことを, 関数 $f(k)$ が k に関して無視できるという.

2.1　公開鍵暗号

公開鍵暗号の概念は Diffie ら [23] によって提唱された. 公開鍵暗号の提唱以前の共通鍵暗号では, 通信を行う二者が事前に同じ秘密鍵を共有しておく必要があった. これに対し, 公開鍵暗号では事前の鍵共有が必要ないという特徴がある.

以下に公開鍵暗号のシンタックスを記す.

公開鍵暗号方式 Π は以下の三つ組みの多項式時間アルゴリズム $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ によって構成される. 以下では Π の平文空間を $\{0,1\}^\ell$ とする, ただし ℓ はセキュリティパラメータの多項式である.

$\mathsf{Gen}(1^\lambda) \to (pk, sk)$: 鍵生成アルゴリズム Gen はセキュリティパラメータ 1^λ を入力として受け取り, 公開鍵 pk と秘密鍵 sk を出力する.

$\mathsf{Enc}(pk, m) \to c$: 暗号化アルゴリズム Enc は公開鍵 pk と平文 $m \in \{0,1\}^\ell$ を入力として受け取り, 暗号文 c を出力する.

$\mathsf{Dec}(sk, c) \to m/\perp$: 復号アルゴリズム Dec は秘密鍵 sk と暗号文 c を入力として受け取り, 平文 $m \in \{0,1\}^\ell$ 又は復号不可を表す特別な記号 $\perp$ を出力する.

正当性　公開鍵暗号方式 Π に対し, 以下を要求する. 任意の $\lambda \in \mathbb{N}$, $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$, 任意の平文 $m \in \{0,1\}^\ell$ に対し $\mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) = m$ が常に成立する.

公開鍵暗号の概念を提唱した Diffe らであったが, 当時具体的な公開鍵暗号の構成法は知られていなかった. その後, Rivest らによる RSA 暗号 [46] と呼ばれる公開鍵暗号の具体的構成法が提案されてから, Rabin 暗号 [44] や Elgamal [27] のように様々な構成法が提案されている. しかし, 上記の RSA 暗号のような初期に提案された公開鍵暗号は, IND-CPA 安全性という比較的弱い安全性すら満たさない. そのため, より強い安全性を満たすような公開鍵暗号の構成法が研究されている. 現在では, 非常に強い安全性である IND-CCA2 安全性を満たすような構成法が提案されている. 具体的には, RSA 暗号の安全性をより高めた RSA OAEP [38],[25] や, Cramer らによる Cramer-Shoup 暗号 [20] と呼ばれる暗号が例として挙げられる.

2.2　公開鍵暗号における攻撃者のモデル

公開鍵暗号における代表的な攻撃の種類は以下のように分類される.

選択平文攻撃 (Chosen Plaintext Attack, CPA): ターゲットとなる暗号文 c を受け取る前後に, 攻撃者は自分で選んだ平文に対する暗号文を得ることができる.

選択暗号文攻撃 (Non-Adaptive Chosen Ciphertext Attack, CCA1): 選択平文攻撃で行うことができる攻撃に加え, ターゲットとする暗号文 c を受け取る前に, 攻撃者は自分で選んだ暗号文を送ることで, その復号結果を返してくれる復号オラクルを利用することができる.

適応的選択暗号文攻撃 (Adaptive Chosen Ciphertext Attack, CCA2): 選択平文攻撃で行うことができる攻撃に加え, ターゲットとする暗号文 c を受け取る前後に, 攻撃者は自分で選んだ暗号文を送ることで, その復号結果を返してくれる復号オラクルを利用することができる.

2.3　公開鍵暗号における安全性

公開鍵暗号の安全性を定義する場合, 次の二つのアプローチがある.

ゲームベースの定義　ある暗号方式の安全性を攻撃者と挑戦者の間のゲームとして表現し, そのゲームで攻撃者が勝つ確率に基づいて定められた優位性が無視できるとき, その暗号方式は安全であると定義する. ゲームベースの定式化は安全性証明が容易にできるように作られた定式化である. そのため, 通常はある公開鍵暗号方式の安全性証明を行う際には, ゲームベースの定義に基づいて行われる.

シミュレーションベースの定義　ある暗号方式が使用される自然な状況 (現実世界) と, それに対応する理想的に安全な状況 (理想世界) で現実世界をシミュレーションしたものが, PPTA によって識別できなければ, その暗号方式は安全であると定義する. シミュレーションベースの定義は, その定義が持つ意味を理想世界の記述により明確に

示すことを目指している. しかし, シミュレーションベースの定義の下での安全性証明は, ゲームベースの定義の下での安全性証明と比べると難しいことが知られている.

ゲーム変換による証明　計算量的な安全性を持つ暗号方式の安全性をある計算量的仮定に帰着して証明するための手法として, ゲーム変換による証明手法がある. ゲーム変換による証明は以下のようにして行われる. まず, 証明したい安全性をゲームベースの定義により定められた安全性ゲームを ゲーム 0 とする. このゲームにおける攻撃者の優位性を $\mathrm{Adv}_0(k)$ と書く. 次に, ゲーム 0 を変化させたゲーム 1 を考え, このゲームにおける攻撃者の優位性を $\mathrm{Adv}_1(k)$ と書く. 同様にして, ゲーム i (i=0,1...) を変化させたゲーム $i+1$ を考え, このゲームにおける攻撃者の優位性を $\mathrm{Adv}_{i+1}(k)$ と書く.

このように順次ゲーム変換を繰り返して最終的にゲーム n に変換する. この最終ゲームは, その優位性を $\mathrm{Adv}_n(k)$ が 0 であることを容易に示すことができるようなものになっているものとする.

このゲーム変換手法を用いた安全性証明の概諦は, 全ての $i = 0, 1, \ldots, n-1$ において $|\mathrm{Adv}_i(k) - \mathrm{Adv}_{i+1}(k)| < \epsilon(k)$ であることを証明することである. これらがすべて示されれば, $|\mathrm{Adv}_0(k) - \mathrm{Adv}_n(k)| \leq \sum_{i=0}^{n-1} |\mathrm{Adv}_i(k) - \mathrm{Adv}_{i+1}(k)|$ が成立し, $|\mathrm{Adv}_0(k) - \mathrm{Adv}_n(k)| < \epsilon(k)$ となる. つまり, この暗号方式が安全であることが示せる.

以下の節に記す意味論的安全性及び, シミュレーションベースの頑強性は, シミュレーションベースの定義を用いて定式化されている. これに対し, 識別不可能性及び, 識別不可能性ベースの頑強性は, ゲームベースの定義を用いて定式化されている.

2.3.1　秘匿性

秘匿性は公開鍵暗号における安全性要件の一つである. この秘匿性は, 暗号文から平文に関する情報が漏れていないことを保証する安全性である. 秘匿性の達成度は次のように分類されている. 暗号文 c から平文 m 全体が得られないことを保証する一方向性や, 暗号文 c から平文 m のいかなる部分情報も求められないことを保証する強秘匿性によって定式化されている. また, 強秘匿性には意味論的安全性 (Semantic Security, SS) と識別不可能性 (Indistinguishability, IND) の二つの定式化が存在する.

本研究で主として取り扱う安全性は強秘匿性であるため, 以下では一方向性の定義は説明せず, 意味論的安全性と識別不可能性の定義を記す.

意味論的安全性

意味論的安全性 (Semantic Security, SS) では, 攻撃者は平文 m のある部分情報 v を求めることを要求される. このとき, 次の二つのタイプの攻撃者を考える. 一つ目の攻撃者 $\mathcal{A}$ は, m の暗号文を入力として受け取り, v を計算する. これに対し, 二つ目の攻撃者 $\mathcal{S}$ は暗号文を受け取らずに v を計算する. この二つの攻撃者の出力が PPTA によって識別できないならば, $\mathcal{A}$ と $\mathcal{S}$ が行うことのできる計算にほとんど差はないといえる. ここで, $\mathcal{A}$ と $\mathcal{S}$ の違いは, 暗号文を受け取っているかどうかであった. よって,

暗号文を受け取っているにもかかわらず, 暗号文を受け取っていない $\mathcal{S}$ と同程度の計算しかできていないという事は, 暗号文から情報が漏れていないということになる. 意味論的安全性では, 上記の考えを厳密に定式化することで, 暗号文から平文の情報が 1 ビットも漏れていないという事をモデル化している.

以下に意味論的安全性の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA とする. また, h, f を多項式時間関数とする. 以下の二つの実験 SS-ATK-0 と SS-ATK-1 を考える:

$\underline{\mathrm{Exp}^{\text{SS-ATK-0}}_{\Pi,\mathcal{A},h,f}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(\mathcal{M}, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$m \leftarrow \mathcal{M}$;
$c^* \leftarrow \mathsf{Enc}(pk, m)$;
$v \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m), st_1)$;
If $v = f(m)$, then $\beta := 1$
Else $\beta := 0$
output $(\mathcal{M}, \beta)$

$\underline{\mathrm{Exp}^{\text{SS-ATK-1}}_{\Pi,\mathcal{S},h,f}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(\mathcal{M}, st_1) \leftarrow \mathcal{S}_1(pk)$;
$m \leftarrow \mathcal{M}$;
$v \leftarrow \mathcal{S}_2(h(m), st_1)$;
If $v = f(m)$, then $\beta := 1$
Else $\beta := 0$
output $(\mathcal{M}, \beta)$

ただし, 攻撃の種類によって, 攻撃者は

- ATK=CPA: $\mathcal{O}_1(c) = \phi, \mathcal{O}_2(c) = \phi$
- ATK=CCA1: $\mathcal{O}_1(c) = \mathsf{Dec}(sk, c), \mathcal{O}_2(c) = \phi$
- ATK=CCA2: $\mathcal{O}_1(c) = \mathsf{Dec}(sk, c), \mathcal{O}_2(c) = \mathsf{Dec}(sk, c)$

のように復号オラクルを利用することができる (ϕ の場合は復号オラクルを利用することができない). また, 復号オラクル $\mathcal{O}_2$ にチャレンジ暗号文そのものをクエリすることは禁止されているものとする.

上記の二つの実験において, $\mathcal{M}$ は暗号方式における平文空間上の分布であるものとする. また,

$$\mathsf{Adv}^{\text{SS-ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda) := \left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-ATK-0}}_{\Pi,\mathcal{A},h,f}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-ATK-1}}_{\Pi,\mathcal{S},h,f}(\lambda)\right) \to 1\right]\right|$$

と定義する.

定義 2.3.1. 任意の多項式時間関数 h, f, 任意の *PPTA* $\mathcal{A}$ に対し, ある *PPTA* $\mathcal{S}$ が存在し, 任意の *PPTA* $\mathcal{D}$ に対して, $\mathsf{Adv}^{\textit{SS-ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda)$ が無視できるならば Π は *SS-ATK* 安全であるという.

識別不可能性

識別不可能性 (Indistinguishability, IND) では, 意味論的安全性と異なり, 定式化に必要な攻撃者は一つである. 攻撃者はまず二つの平文 m_0, m_1 を出力することを要求さ

れる. その後, 攻撃者は m_b の暗号文を受け取る, ただしビット b はランダムに選択される. そして, 攻撃者は受け取った暗号文からビット b を推測するというゲームによって定式化される. また, 暗号方式が識別不可能性を満たすかどうかは, このビット b の推測に成功する確率によって評価される.

識別不可能性は意味論的安全性と比べるとその定義の妥当性がわかりにくい. しかし, 意味論的安全性の定式化では $\mathcal{A}$, $\mathcal{S}$ 及び $\mathcal{D}$ という三つの PPTA が必要であったのに対し, 識別不可能性では $\mathcal{A}$ のみを用いて安全性を定式化することができる. そのため, 識別不可能性の定式化は意味論的安全性の定式化と比べると, 簡潔な定式化である. 2.3.3 節で述べるが, 識別不可能性は意味論的安全性と等価であることが知られているため, 実際の安全性証明には識別不可能性の定式化が用いられることが多い.

以下に識別不可能性の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. 以下の二つの実験 IND-ATK-0 と IND-ATK-1 を考える:

$\underline{\mathrm{Exp}^{\text{IND-ATK-0}}_{\Pi,\mathcal{A}}(\lambda)}$	$\underline{\mathrm{Exp}^{\text{IND-ATK-1}}_{\Pi,\mathcal{A}}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
output b'	output b'

ただし, $\mathcal{O}_1$ 及び, $\mathcal{O}_2$ は ATK $\in$ {CPA,CCA1,CCA2} に応じて, 意味論的安全性で定義したオラクルと同様にして定義される. なお, IND-ATK においても, 意味論的安全性の場合と同様に, 復号オラクル $\mathcal{O}_2$ にチャレンジ暗号文そのものをクエリすることは禁止されているものとする.

また,

$$\mathsf{Adv}^{\text{IND-ATK}}_{\Pi,\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Exp}^{\text{IND-ATK-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-ATK-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right|$$

と定義する.

定義 2.3.2. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}^{\mathit{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できるならば, Π は *IND-ATK* 安全であるという.

2.3.2　頑強性

頑強性は公開鍵暗号における安全性要件の一つである. 頑強性は, 暗号文に対し悪意のある改変をすることができないことを保証する安全性である. 頑強性の概念は Dolve ら [24] によって提唱され, 現在はシミュレーションベース及び, 識別不可能性ベースの定式化がされている.

シミュレーションベースの頑強性

シミュレーションベースの頑強性 (Simulation-based Non-Malleability , SNM) では, 暗号文を受け取った上で, 暗号文の改変を行う攻撃者 $\mathcal{A}$ と, 暗号文を受け取らずに暗号文の改変を行う攻撃者 $\mathcal{S}$ を考える. 意味論的安全性の場合と同様に, $\mathcal{A}$ と $\mathcal{S}$ の出力が PPTA によって識別できないならば, $\mathcal{A}$ が受け取った暗号文は改変を行う上で攻撃者の役に立っていないといえる. シミュレーションベースの頑強性は上記の考え厳密に定式化することで, 暗号文に対し改変を行うことができないという事をモデル化している.

以下にシミュレーションベースの頑強性の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. また, h を多項式時間関数とする. 以下の二つの実験 SNM-ATK-0 と SNM-ATK-1 を考える:

$\mathrm{Exp}^{\text{SNM-ATK-0}}_{\Pi,\mathcal{A},h}(\lambda)$	$\mathrm{Exp}^{\text{SNM-ATK-1}}_{\Pi,\mathcal{S},h}(\lambda)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(\mathcal{M}, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(\mathcal{M}, st_1) \leftarrow \mathcal{S}_1(pk)$;
$m \leftarrow \mathcal{M}$;	$m \leftarrow \mathcal{M}$;
$c^* \leftarrow \mathsf{Enc}(pk, m)$;	
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m), st_1)$;	$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{S}_2(h(m), st_1)$;
For $i = 1$ to n	For $i = 1$ to n
$d_i := \mathsf{Dec}(sk, c_i)$	$d_i := \mathsf{Dec}(sk, c_i)$
output $(\mathcal{M}, m, d_1, \ldots, d_n, st_2)$	output $(\mathcal{M}, m, d_1, \ldots, d_n, st_2)$

ただし, $\mathcal{O}_1$ 及び, $\mathcal{O}_2$ は ATK $\in$ {CPA,CCA1,CCA2} に応じて, 2.3.1 節におけるオラクルと同様にして定義される. なお, SNM-ATK において, 復号オラクル $\mathcal{O}_2$ にチャレンジ暗号文そのものをクエリすることは禁止されているものとする. さらに, 上記の条件に加えて攻撃者 $\mathcal{A}$ が出力する暗号文に以下の二つの条件が課される.

非重複性: $c_i = c^*$ となる暗号文を出力しないこと.

正当性: 最終的に出力する暗号文 $(c_1, \ldots, c_n)$ は全て暗号化関数の出力値からなる空間に含まれていること. つまり, 全ての c_i に対し, $c_i = \mathsf{Enc}(pk, m_i)$ を満たす平文が存在すること.

上記の二つの実験において, $\mathcal{M}$ は暗号方式における平文空間上の分布であるものとする. また,

$$\mathsf{Adv}^{\text{SNM-ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda) := \left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-ATK-0}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-ATK-1}}_{\Pi,\mathcal{S},h}(\lambda)\right) \to 1\right]\right|$$

と定義する.

定義 2.3.3. 任意の多項式時間関数 h, 任意の *PPTA* $\mathcal{A}$ に対し, ある *PPTA* $\mathcal{S}$ が存在し, 任意の *PPTA* $\mathcal{D}$ に対して $\mathsf{Adv}^{SNM\text{-}ATK}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda)$ が無視できるならば, Π は *SNM-ATK* 安全であるという.

識別不可能性ベースの頑強性

識別不可能性ベースの頑強性 (Indistinguishability-based Non-Malleability, INM) では, 識別不可能性と同様にして, 攻撃者はまず二つの平文 m_0, m_1 を出力することが要求される. その後, 攻撃者は m_b の暗号文を受け取る, ただしビット b はランダムに選択される. そして, 攻撃者は受け取った暗号文の改変を試み, 暗号文の列を出力する. 最後に, 攻撃者が出力した暗号文の列が復号され, その復号結果を利用して攻撃者はビット b を推測する. 暗号方式が識別不可能性ベースの頑強性を満たすかどうかは, このビット b の推測に成功する確率によって評価される.

識別不可能性と同様にして, 識別不可能性ベースの頑強性はその定義の妥当性がわかりにくい. しかし, 識別不可能性ベースの頑強性の定式化は, シミュレーションベースの頑強性の定式化よりも簡潔な定式化になっている. 2.3.3 節で述べるが, 識別不可能性ベースの頑強性とシミュレーションベースの頑強性は等価であることが知られているため, 実際の安全性証明には識別不可能性ベースの頑強性の定式化が用いられることが多い. (また, この等価性から二つの頑強性を区別せず, 単に NM という表記をする場合がある.)

以下に識別不可能性ベースの頑強性の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ を PPTA の三つ組とする. 以下の二つの実験 INM-ATK-0 と INM-ATK-1 を考える:

$\mathrm{Exp}^{\text{INM-ATK-0}}_{\Pi,\mathcal{A}}(\lambda)$	$\mathrm{Exp}^{\text{INM-ATK-1}}_{\Pi,\mathcal{A}}(\lambda)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;	$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
For $i = 1$ to n	For $i = 1$ to n
$\quad d_i := \mathsf{Dec}(sk, c_i)$	$\quad d_i := \mathsf{Dec}(sk, c_i)$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$;	$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$;
output b'	output b'

ただし, $\mathcal{O}_1$ 及び, $\mathcal{O}_2$ は ATK $\in$ {CPA,CCA1,CCA2} に応じて, 2.3.1 節におけるオラクルと同様にして定義される. なお, INM-ATK において, 復号オラクル $\mathcal{O}_2$ にチャレンジ暗号文そのものをクエリすることは禁止されているものとする. さらに, SNM の場合と同様にして, INM においても攻撃者は正当性と非重複性が満たされている出力をするという制約が設けられているものとする.

また,

$$\mathsf{Adv}^{\text{INM-ATK}}_{\Pi,\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Exp}^{\text{INM-ATK-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{INM-ATK-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right|$$

と定義する.

定義 2.3.4. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}^{\textit{INM-ATK}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できるならば, Π は *INM-ATK* 安全であるという.

2.3.3　安全性概念間の関係

秘匿性及び頑強性は, それぞれ二つの定式化がされている. 意味論的安全性と識別不可能性間の関係性や, シミュレーションベースの頑強性と識別不可能性ベースの頑強性の関係性は既存研究によって明らかになっている. Goldwasser ら [29] によって, CPA 環境下における意味論的安全性と識別不可能性間が等価性が証明されている. また, CCA1 及び, CCA2 環境下での意味論的安全性と識別不可能性間が等価性は, Watanabe ら [48] によって証明されている. よって, 意味論的安全性と識別不可能性は, CPA, CCA1, CCA2 のいずれの場合においても等価であることが証明されている. 意味論的安全性は識別不可能性と比べると, 安全性証明をすることが難しい定式化になっているが, この等価性により, 現在は識別不可能性での安全性証明が主流となっている. 頑強性に関しては, Bellare ら [5] によってシミュレーションベースの頑強性と識別不可能性ベースの頑強性が CPA, CCA1, CCA2 のいずれの場合においても等価であることが証明されている.

また, 秘匿性と頑強性間の関係性についても既存研究によって明らかになっている. Bellare ら [3] によって, 秘匿性と頑強性が CCA2 の場合において等価であることが証明されている. そのため, ある暗号方式が IND-CCA2 安全であれば, その方式は自動的に INM-CCA2 安全であることが保証される. つまり, 秘匿性に関して安全性証明を行えば, 頑強性も同時に証明できたことになる. このように安全性概念間の等価性が明らかになれば, 複数の安全性の取り扱いを容易になる.

2.4　RCCA 安全性

RCCA 安全性は Canetti ら [15] によって提案された安全性であり, CCA 安全性を緩めた安全性として知られている. RCCA 安全性は多くの応用 (認証や鍵交換) において十分であることが示されている [15]. RCCA 安全性の定式化では, m_0, m_1 がチャレンジメッセージであるとき, 復号オラクルが m_0 または m_1 の暗号文がクエリされた場合に “Test” というシンボルを返すという定式化がされている. このような定式化を行うことによって, 暗号文のリプレイを許容する定式化になっている. 例えば, 暗号文の再ランダム化ができる暗号方式を考える. このとき, 攻撃者はチャレンジ暗号文に対し再ランダム化を行うことで, 平文の内容を保持した違う形の暗号文を生成することができる. 通常の CCA 環境では, このようにして生成された暗号文を復号オラクルにクエリすることは禁止されていない. よって, チャレンジ暗号文の復号結果が間接的に漏れてしまい, 暗号文の再ランダム化が行える暗号方式は CCA 安全性を満たさない. しかし, RCCA 環境においては, チャレンジ暗号文を再ランダム化した暗号文を復号オラクルにクエリすると, “Test” というシンボルがオラクルから返ってくる. そのため, CCA 環境での状況と異なり, 攻撃者はチャレンジ暗号文の復号結果をオラクルから得ることはできない. このように RCCA 安全性では, 上記の暗号文の再ランダム化が行える方式のように, ある暗号文から平文の内容を保持した別の形の暗号文へ変換する能力は, 暗号方式攻撃の役に立たない. つまり, 同じ平文に復号されるような暗号文を繰り

返し送るようなリプレイが許容されている.

Canetti らは RCCA 環境下における頑強性 NM-RCCA を定義している. また, この NM-RCCA の他に, 識別不可能性 IND-RCCA と 汎用的結合可能性 UC-RCCA の定式化を行い, 平文空間のサイズが大きい場合にこれら三つの安全性が等価であることを証明した. 識別不可能性と頑強性については既に定義を述べていたが, 汎用的結合可能性 (Universal Composability, UC) については述べていなかったので, 以下に概要を説明する.

汎用的結合可能性は, Canetti [13] によって提唱された安全性である. この汎用的結合可能性は, 暗号プロトコルを並列に結合したときの安全性を保証する安全性である. Canetti による汎用的結合可能性の提唱以前の安全性では, 各種暗号プロトコルを単体で使用した場合における安全性が定式化がされており, 並列利用は考慮されていなかった. そのため, プロトコルの並列利用によって安全性が損なわれてしまう場合がある. このような問題を解決するための安全性モデルが汎用的結合可能性である. また, 汎用的結合可能性を満たすことが証明されたプロトコルは, 他のどんなプロトコルと組み合わせて使用されても, その安全性が保証されることが知られている. 以上が汎用的結合可能性の概要であるが, 本研究で主として取り扱う安全性は強秘匿性と頑強性である. そのため, 以下では汎用的結合可能性の詳細な定義は説明せず, RCCA 環境下における識別不可能性である IND-RCCA と頑強性 NM-RCCA の定義を紹介する.

2.4.1 IND-RCCA

IND-RCCA 安全性は, IND-CCA2 安全性を緩めた定式化である. IND-CCA2 安全性において, 攻撃者は復号オラクル $\mathcal{O}_2$ に自身が選択した暗号文を自由にクエリして, その復号結果を得ることができていた. しかし, Canetti ら [15] の定義した IND-RCCA 安全性においては状況が少し異なる. 彼らは, 復号オラクル $\mathcal{O}_2$ が攻撃者が選択したチャレンジメッセージ m_0 又は m_1 の暗号文をクエリされた際に “Test” というシンボルを返すという定式化をしている. 復号オラクル $\mathcal{O}_2$ が “Test” という応答をすることによって, チャレンジ暗号文の再ランダム化を行った暗号文などから平文の情報がオラクルクエリによって漏れず, CCA 安全性を緩めた定式化になっている.

以下に Canetti らが提案した IND-RCCA の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. 以下の二つの実験 IND-RCCA-0 と IND-RCCA-1 を考える:

$\mathrm{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda)$	$\mathrm{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
output b'	output b'

ただし,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c) & (\text{otherwise}) \end{cases}$$

である.

また,

$$\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right|$$

と定義する.

定義 2.4.1. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}^{IND\text{-}RCCA}_{\Pi,\mathcal{A}}(\lambda)$ が無視できるならば, Π は *IND-RCCA* 安全であるという.

2.4.2 NM-RCCA

NM-RCCA では, IND-RCCA の定式化と同様にして, 復号オラクル $\mathcal{O}_2$ が攻撃者が選択したチャレンジメッセージ m_0 又は m_1 の暗号文をクエリされた際に "Test" というシンボルを返すという定式化がされている.

以下に Canetti らが提案した NM-RCCA の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. 以下の二つの実験 NM-RCCA-0 と NM-RCCA-1 を考える:

$\mathrm{Exp}^{\text{NM-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda)$	$\mathrm{Exp}^{\text{NM-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$c' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;	$c' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
$m' \leftarrow \mathsf{Dec}(sk, c')$	$m' \leftarrow \mathsf{Dec}(sk, c')$
If $m' = m_0$, then output 0	If $m' = m_1$, then output 1
Otherwise, then output 1	Otherwise, then output 0

ただし,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c) & (\text{otherwise}) \end{cases}$$

である.

また,

$$\mathsf{Adv}^{\text{NM-RCCA}}_{\Pi,\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Exp}^{\text{NM-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{NM-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right|$$

と定義する.

定義 2.4.2. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}^{NM\text{-}RCCA}_{\Pi,\mathcal{A}}(\lambda)$ が無視できるならば, Π は *NM-RCCA* 安全であるという.

上記の NM-RCCA では, 攻撃者は最後に m_{1-b} の暗号文を出力した場合に成功とみなされている, ただし b はチャレンジビットである. Canetti らのこの NM-RCCA の定式化と IND-RCCA の定式化は, 最後に攻撃者にチャレンジビット b を推測させるか, m_{1-b} の暗号文を出力させるかという部分のみ異なる. それ以外の部分は IND-RCCA と NM-RCCA の定式化は全く同じであり, この二つの定式化は非常に似たものとなっている. さらに, Canetti らの NM-RCCA の定式化は, 2.3.2 節で述べた従来のシミュレーションベースの頑強性や識別不可能性ベースの頑強性のどちらとも大きく異なる定式化がされている. これに加え, 彼らは平文空間のサイズが十分大きい場合の UC-RCCA, IND-RCCA 及び NM-RCCA の等価性から NM-RCCA の定義の妥当性を主張しているが, 平文空間のサイズが多項式の場合, IND-RCCA 安全性を満たすが, NM-RCCA 安全性を満たさないような暗号方式が存在する. そのため, 彼らの NM-RCCA の定式化が本当に頑強性の直感を捉えた定式化なのかは, その妥当性が不明である.

2.5　高機能暗号

通常の公開鍵暗号では, 平文の暗号化, 暗号文の復号という機能しか持たない. 公開鍵暗号に暗号化, 復号以外の機能を持たせた暗号のことを高機能暗号と呼び, 現在盛んに研究が行われている. 高機能暗号の例として, 任意の文字列を公開鍵として使用可能な ID ベース暗号 [47],[11], 柔軟なアクセス制御が可能な属性ベース暗号 [30],[7] が挙げられる. ID ベース暗号を用いると, 公開鍵証明書が不要になるといった恩恵が受けられ, 属性ベース暗号は動画配信サービスにおけるアクセス制御などの応用が考えられている. ID ベース暗号や属性ベース暗号の他にも, 代理人と呼ばれる第三者が再暗号化作業によって宛先を変えることができる代理人再暗号化 [8],[32] や, 暗号文の復号を行わずにキーワード検索が可能な検索可能暗号 [10],[1] などが挙げられる. 代理人再暗号化を用いることで, クラウドでの安全なアクセス制御を行うことができる. また, 検索可能暗号を用いると, クラウドに暗号化したデータをアウトソースしつつ, 必要に応じて検索を実行できるため, クラウドの安全性を高めることができる. このように, 公開鍵暗号に機能が付け加えられた高機能暗号は, 様々な現実的なニーズを解決するような応用先がある.

高機能暗号の研究においても, 安全性概念間の関係性に関する研究や RCCA 安全性に関する研究が行われている. 例えば, ID ベース暗号における意味論的安全性の定式化と, 識別不可能性の等価性が Attrapadung ら [2] 及び, Galindo ら [26] によって明らかになっている. ID の匿名性に関しては, シミュレーションベースの定式化が小松ら [49] によって行われ, CPA 環境での識別不可能性ベースの匿名性との等価性が証明されている. この他にも, ID ベース暗号における匿名性の新たな安全性モデルの定式化を行い, 既存の安全性との関係性を明らかにした研究として 大友ら [50],[51] の研究が挙げられる.

高機能暗号における RCCA 安全性に関する研究も, 通常の公開鍵暗号と同様にして行われている. 例えば, 代理人再暗号化における CCA 安全性の定式化を行う際に, RCCA 安全性の定式化の考えが用いられている [36]. これに加え, 代理人再暗号化の方式構成に関する研究では, RCCA 安全な方式構成の研究も行われている [37],[34].

以上のように, 公開鍵暗号を発展させた高機能暗号においても, 盛んに安全性概念間の関係性に関する研究や, RCCA 安全性に関連した研究が行われており, 重要な研究の一つとして位置づけられている.

Chapter 3　関連研究

3.1　攻撃者のモデルに関する研究

公開鍵暗号における代表的な攻撃者のモデルとして, 2.2 節で紹介したように 選択平文攻撃 (Chosen Plaintext Attack, CPA), 選択暗号文攻撃 (Chosen Ciphertext Attack, CCA1) や, 適応的選択暗号文攻撃 (Adaptive Chosen Ciphertext Attack, CCA2) が挙げられる. まず, IND-CPA の概念は, Goldwasser ら [28] によって提唱された. その後, CCA1 の概念が Naor ら [39] によって提唱され, Rackoff ら [45] によって CCA2 の概念が提唱された.

上記の代表的な攻撃者モデル以外には, 本稿で取り扱う RCCA の他に, ECCA (Enhanced Chosen Ciphertext Attack), RECCA (Replayable Enhanced Chosen Ciphertext Attack), CCVA (Chosen Ciphertext Verification Attack) といったモデルが考えられている. ECCA は CCA2 よりも強い攻撃を考えた攻撃モデルであり, Dachman-Soled ら [21] によって提案された. CCA2 環境では, 攻撃者が復号オラクルに暗号文をクエリした場合, 攻撃者はその復号結果のみを得ることができる. 一方, ECCA 環境では, 攻撃者が復号オラクルに暗号文をクエリした場合, 攻撃者は復号結果に加えて, 暗号化の際に使用された乱数の値も同時に得ることができる. RECCA は, ECCA 環境において暗号文のリプレイを許した定式化になっており, Dai ら [22] によって提案されている. RCCA が CCA2 を緩めた定式化になっていることと同様に, RECCA は ECCA を緩めた定式化になっている.

CCVA は, RCCA と同様に CCA2 を緩めた定式化になっている [40]. 具体的には, CCVA 環境では, 攻撃者は復号オラクルの代わりに, 検証オラクルと呼ばれるオラクルにアクセスすることができる. 検証オラクルには, 復号オラクルの場合と同様に, 攻撃者が自分で選んだ暗号文をクエリすることができる. ここで, 検証オラクルはその暗号文が正当に作られた暗号文ならば 1 を攻撃者に返し, そうでなければ 0 を返す. 検証オラクルは復号オラクルと異なり, 暗号文の復号結果は返さない.

初期の SSL では, システムが復号結果が正しくないフォーマットとなっている場合に, その旨を返答するプロトコルになっていた. Bleichenbach [9] はこのプロトコルからの返答を利用して暗号文の復号を行う攻撃法を発見した. CCVA は Bleichenbach の攻撃のような, 現実に起こりうる攻撃を定式化している.

RCCA と関連が深い攻撃者モデルとして, WRCCA (weak RCCA) と呼ばれる攻撃者モデルが Groth [31] によって提案されている. WRCCA は RCCA とは異なり, 復号オラクル $\mathcal{O}_2$ にチャレンジメッセージ m_0 又は m_1 に復号されるような暗号文をクエリすると, $\perp$ が返ってくるという定式化がされている. RCCA 環境における攻撃者は, オラクルから “Test” という返答が返ってくことで, クエリした暗号文が m_0 又は m_1 に復号されるという情報を得ることができた. 一方, WRCCA 環境での攻撃者は, オラ

クルからの $\perp$ という返答から, 自分がクエリした暗号文が m_0 又は m_1 に復号されるような暗号文だったのか, それとも復号不可な暗号文だったのかが判断できない場合がある. そのため, 復号オラクルが “Test” を返すか $\perp$ を返すかによって, 攻撃者が得られる情報量は異なる. このように, 些細な定式化の違いでも攻撃者の攻撃能力に差が生まれる場合がある.

3.2　RCCA 安全な方式の構成に関する研究

RCCA 安全な暗号方式の構成に関する研究は Canetti らによって RCCA 安全性が提案されてから複数行われている. 例えば, 2.4 節で述べたように, RCCA 安全性は暗号文の再ランダム化が行える方式を取り扱うことができる. そのため, RCCA 安全性を満たす方式は, 暗号文の再ランダム化が行える方式構成と共に行われている場合が多い. 以下に暗号文の再ランダム化が行える方式構成に関する研究を紹介する.

まず, Groth [31] によって RCCA 安全性を弱めた weak RCCA 安全性を満たす再ランダム化可能な方式の具体的な構成が提案された. その後, Prabhakaran ら [42] によって, 再ランダム化可能かつ RCCA 安全な方式の non-standard cryptographic groups を使った構成が与えられている. なお, この Prabhakaran らの構成は, 暗号構成の際に広く使用されている標準的な仮定からではなく, 非標準的な仮定の下で構成されている. Prabhakaran らによる方式提案の後, Chase ら [16] による再ランダム化可能で RCCA 安全な方式の標準的な仮定からの提案や, Libert ら [35] によるその効率化等が後続の研究として挙げられる. また, この他にも RCCA 安全性を満たす再ランダム化可能な方式構成に関する研究として, Kawamoto ら [33] よる研究が挙げられる.

上記においては暗号文の再ランダム化が行える方式に着目していたが, RCCA 安全な方式構成の研究は, この他にも存在している. 例えば, Chen ら [19] による公開鍵暗号方式は, 暗号文の再ランダム化が行えない. しかし, 彼らの方式は CCA2 安全な方式をベースにして構成されており, CCA2 安全性よりも安全性が落ちるものの, 効率的な構成になっている. また, 通常の公開鍵暗号の構成以外には, 共通鍵暗号と公開鍵暗号技術を組み合わせたハイブリッド暗号の構成 [17],[18] に関する研究が行われている.

3.3　公開鍵暗号における安全性概念間の関係性に関する研究

2.3.3 節で述べたように, 安全性概念間の関係性に関する研究は広く行われている. 意味論的安全性と識別不可能性が CPA, CCA1, CCA2 いずれの場合においても等価であることや, シミュレーションベースの頑強性と識別不可能性ベースの頑強性もまた CPA, CCA1, CCA2 いずれの場合においても等価であることを述べた. さらに, CCA2 環境において秘匿性と頑強性が等価であること, つまり IND-CCA2 と INM-CCA2 が等価であることについても触れた. このように異なる安全性概念間であっても等価性が示されているものも存在する.

しかし, 安全性概念間の関係性に関する研究においては, 必ずしも等価性が言えるというわけではない. 例えば, CCVA を提案した Pandey ら [40] は, IND-CCVA 安全だが, IND-CCA2 安全でない暗号方式や, IND-CCA1 安全だが IND-CCVA 安全でない暗号方式が存在することを証明した.

Pandey らの研究以外には, Pass ら [41] による研究が挙げられる. 彼らの研究では, 従来の頑強性よりも強い頑強性が定式化された. 従来の頑強性の定式化においては, 攻撃者にはチャレンジ暗号文をそのまま出力しないという非重複性と, 出力する暗号文は全て暗号化関数の出力値からなる空間に含まれているという正当性が制約として設けられていた. Pass らはこれら非重複性と正当性を満たさないような攻撃者を捉えた頑強性の定式化を行い, 安全性概念間の関係性を明らかにした. 結果として, 彼らの想定した非重複性と正当性を満たさないような攻撃者の下では, シミュレーションベースの頑強性と識別不可能性ベースの頑強性は CCA2 環境で等価でないことが明らかになった. 具体的には, $\perp$ に復号されるような暗号文がオラクルの力を借りることなく効率的にサンプルすることができない暗号方式が, 識別不可能性ベースの頑強性を満たしていたとしても, その方式がシミュレーションベースの頑強性を満たさない場合があるという事が示された.

Pass らの研究は, 安全性概念間の関係性を明らかにする研究であると同時に, 本研究の基礎となるので, 4.1 節にて詳しく説明を行う.

Chapter 4　RCCA 環境下における頑強性の定式化

本章では, 本研究の基礎となる既存結果について述べた後, RCCA 環境下での頑強性の定式化を行う. また, 本稿で定式化した二つの頑強性間の等価性を証明する. さらに, 既存の RCCA 環境下での安全性概念との関係性についても同様に証明を与える.

4.1　提案モデルの基礎となる研究

2.3.2 節の頑強性の定式化では, 攻撃者が $\perp$ に出力されるような暗号文を出力することや, チャレンジ暗号文をそのまま出力することは禁止されている. Pass ら [41] はそのような制約がない場合の頑強性の定式化を行い, 従来の頑強性との関係性を明らかにした. 本研究でのシミュレーションベースの頑強性を行う際に, 彼らのシミュレータに特殊なシンボルを出力することを許すという定式化を参考にした.

以下に Pass らの頑強性の定式化について記す.

4.1.1　より強いシミュレーションベースの頑強性 (SIM-NME′)

まず, Pass らのシミュレーションベースの頑強性 SIM-NME′ についての定義を以下に記す.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. また, M を分布から $\ell(k)$ 個の平文をサンプルするチューリング機械とする.

以下の二つの実験 SIM-NME′ と $\overline{\text{SIM-NME}'}$ を考える:

$\underline{\text{SIM-NME}'(\Pi, \mathcal{A}, k, t, r)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^k)$;
$(M, s) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$(m_1, \ldots, m_t) \leftarrow M(1^k)$;
$\boldsymbol{y} \leftarrow \mathsf{Enc}(pk, \boldsymbol{m})$;
$(c_1, \ldots, c_r, \sigma) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(\boldsymbol{y}, h(\boldsymbol{m}), s)$;
For $i = 1$ to r
$d_i := \begin{cases} \mathsf{Copy} & (c_i \in \boldsymbol{y}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m, d_1, \ldots, d_r, \sigma)$

$\underline{\overline{\text{SIM-NME}'}(\Pi, \mathcal{S}, k, t, r)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^k)$;
$(M, s) \leftarrow \mathcal{S}_1(pk)$;
$(m_1, \ldots, m_t) \leftarrow M(1^k)$;
$(c_1, \ldots, c_r, \sigma) \leftarrow \mathcal{S}_2(h(\boldsymbol{m}), s)$;
For $i = 1$ to r
$d_i := \begin{cases} \mathsf{Copy} & (c_i = \mathsf{Copy}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m, d_1, \ldots, d_r, \sigma)$

ただし,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \mathsf{Dec}(sk, c)$$

である. また, M が以下の二つの条件を満たすとき, M を (p,t)-valid message sampler と呼ぶ.

- $M(1^k)$ の実行時間は高々 $p(k)$ である.
- $M(1^k)$ が任意の $1 \leq i \leq t(k)$ に対し, $|m_i| = l_i(1^k)$ を満たすような平文の列 $(m_1, \ldots, m_{t(k)})$ を出力するような多項式 $l_1, \ldots, l_t$ が存在する.

定義 4.1.1. 任意の多項式 $t(k), r(k), p(k)$, 任意の多項式時間関数 h, 任意の実行時間が高々 $p(k)$ であり, 常に (p,t)-*valid message sampler* を出力する *PPTA* $\mathcal{A}$ に対し, 以下の二つの分布が計算量的に識別不可能となるような, ある実行時間が高々 $p(k)$ であり, 常に (p,t)-*valid message sampler* を出力する *PPTA* $\mathcal{S}$ が存在するとき, Π は *SIM-NME′* 安全であるという.

$$\left\{\text{SIM-NME}'\left(\Pi, \mathcal{A}, k, t(k), r(k)\right)\right\}_k \overset{c}{\approx} \left\{\overline{\text{SIM-NME}'}(\Pi, \mathcal{S}, k, t(k), r(k))\right\}_k$$

上記の SIM-NME′ では 2.3.2 節の非重複性と正当性という二つの制約を攻撃者に対して設けていない. 従来のシミュレーションベースの頑強性の定式化において, 攻撃者が非重複性を満たさない場合, 任意の暗号方式はシミュレーションベースの頑強性を満たせない. なぜなら, 攻撃者 $\mathcal{A}$ は $c_i = c^*$ $(i = 1, \ldots, n)$ を出力することができる, ただし c^* はチャレンジ暗号文である. これに対し, シミュレータ $\mathcal{S}$ はチャレンジ暗号文を受け取らないので, $\mathcal{A}$ のこの振る舞いを模倣することができない. そのため, $\mathcal{A}$ と $\mathcal{S}$ の出力する分布を多項式時間で識別可能な $\mathcal{D}$ が存在してしまう.

Pass らの SIM-NME′ の定式化では, 上記の問題を取り払うため, シミュレータが "Copy" というシンボルを出力することを許している. このような定式化を行うことで, シミュレータはチャレンジ暗号文を受け取らずに, $\mathcal{A}$ がチャレンジ暗号文をそのまま出力するという行動を模倣することができる.

RCCA 環境下でのシミュレーションベースの頑強性の定式化を行う上で, シミュレータが特殊なシンボルを出力するというアイデアを用いた. 従来のシミュレーションベースの頑強性の単純な拡張によって RCCA 環境下でのシミュレーションベースの頑強性が定式化できない理由を以下に記す. 2.4 節で述べたように, RCCA 環境で取り扱うことのできる暗号方式には, 暗号文の再ランダム化ができる方式があった. よって, RCCA 環境下での頑強性を考える上でも, このような再ランダム化ができる方式を取り扱うことができる定式化が必要となる. 暗号文の再ランダム化が行える方式において, 攻撃者が再ランダム化されたチャレンジ暗号文を出力した場合を考える. このとき, シミュレータはチャレンジ暗号文を受け取らないため, チャレンジ暗号文の再ランダム化をすることができない. そのため, シミュレータは攻撃者の振る舞いを模倣できない. このような理由から, 従来のシミュレーションベースの頑強性の単純な拡張に

よって RCCA 環境下でのシミュレーションベースの頑強性の定式化は行えない. しかし, Pass らの SNM-NME′ の定式化の考えを利用することによってこの問題が解決される. なぜなら, シミュレータが特殊なシンボル “Test” という出力を許す定式化にすると, チャレンジ暗号文を受け取っていない場合でも攻撃者のチャレンジ暗号文を再ランダム化して出力するという行動を模倣できるからである.

4.1.2　より強い識別不可能性ベースの頑強性 (IND-NME′)

以下に Pass らによる識別不可能性ベースの頑強性 (IND-NME′) の定義を述べる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ を PPTA の三つ組とする.

以下の二つの実験 IND-NME′-b (b=0,1) を考える:

$$
\begin{array}{l}
\underline{\text{IND-NME}'^{\,}_b(\Pi, \mathcal{A}, k, t, r)} \\
(pk, sk) \leftarrow \mathsf{Gen}(1^k); \\
((m_{0,1}, \ldots, m_{0,t}), (m_{1,1}, \ldots, m_{1,t}), s) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk) \text{ s.t. } |m_{0,i}| = |m_{1,i}|; \\
y_i \leftarrow \mathsf{Enc}(pk, m_{b,i}) \text{ for } i = 1 \text{ to } t; \\
(c_1, \ldots, c_r) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(\boldsymbol{y}, s); \\
\text{For } i = 1 \text{ to } r \\
\quad d_i := \begin{cases} \mathsf{Copy} & (c_i \in \boldsymbol{y}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases} \\
\text{output } \ (d_1, \ldots, d_r)
\end{array}
$$

ただし,

$$
\begin{aligned}
\mathcal{O}_1(c) &= \mathsf{Dec}(sk, c), \\
\mathcal{O}_2(c) &= \mathsf{Dec}(sk, c)
\end{aligned}
$$

である.

定義 4.1.2. 任意の *PPTA* $\mathcal{A}$, 任意の多項式 $t(k), r(k)$ に対し, 以下の二つの分布が計算量的に識別不可能であれば, Π は *IND-NME′* 安全であるという.

$$
\{\textit{IND-NME}'_0(\Pi, \mathcal{A}, k, t(k), r(k))\}_k \overset{c}{\approx} \{\textit{IND-NME}'_1(\Pi, \mathcal{A}, k, t(k), r(k))\}_k
$$

IND-NME′ においても SIM-NME′ の場合と同様に, 攻撃者には非重複性と正当性という制約が設けられていない. 従来の識別不可能性ベースの頑強性において, 攻撃者が非重複性を満たさない場合, 以下のような振る舞いをする攻撃者が考えられる. 攻撃者 $\mathcal{A}$ は $c_i = c^*$ $(i = 1, \ldots, n)$ を出力する, ただし c^* はチャレンジ暗号文である. 従来の識別不可能性ベースの頑強性では最後に攻撃者の出力した暗号文の列が復号される. その結果, チャレンジビットの情報が自明に漏れてしまう.

IND-NME′ の定式化では, 最後に暗号文の列を復号する際に, チャレンジ暗号文がそのまま出力されていた場合には “Copy” というシンボルを復号結果の代わりとして

いる. このようにしてチャレンジビットの情報が漏れない定式化となっている. RCCA 環境下での識別不可能性ベースの頑強性を考える上で, 復号結果に特別なシンボルを用いるという考えを用いた. Pass らの定式化ように, 復号結果に特別なシンボルを用いることによって, チャレンジ暗号文を再ランダム化した暗号文からは情報が漏れない定式化を行うことができる.

4.2　SNM-RCCA の定義

以下に本稿で提案する RCCA 環境下でのシミュレーションベースの頑強性 (SNM-RCCA) の定義を与える. SNM-RCCA を定義する上で, Pass らのシミュレータが特別なシンボルを出力することを許すという定式化を参考にした他, 述語を用いて定式化を行った.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. また, h を多項式時間関数とする.

以下の二つの実験 SNM-RCCA-0 と SNM-RCCA-1 を考える:

$\underline{\mathrm{Exp}^{\text{SNM-RCCA-0}}_{\Pi,\mathcal{A},h}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$m \leftarrow \mathcal{M}$;
$c^* \leftarrow \mathsf{Enc}(pk, m)$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m), st_1)$;
For $i = 1$ to n
$$d_i := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m, \mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$$
output $(\mathcal{M}, m, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st_2)$

$\underline{\mathrm{Exp}^{\text{SNM-RCCA-1}}_{\Pi,\mathcal{S},h}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{S}_1(pk)$;
$m \leftarrow \mathcal{M}$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{S}_2^{\boldsymbol{P}(m,\cdot)}(h(m), st_1)$;
For $i = 1$ to n
$$d_i := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m, \mathsf{Dec}(sk, c_i)) = 1 \\ & \quad \vee\, c_i = \mathsf{Test}) \\ \perp & (c_i = \perp) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$$
output $(\mathcal{M}, m, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st_2)$

ただし, 述語 $\boldsymbol{P}$ は $\mathcal{M}$ のサポートに含まれる任意の m に対し, $\boldsymbol{P}(m, m) = 1$ を満たすものとする. また,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m, \mathsf{Dec}(sk, c)) = 1) \\ \mathsf{Dec}(sk, c) & (\text{otherwise}) \end{cases}$$

である. 上記の二つの実験において, $\mathcal{M}$ は暗号方式における平文空間上の分布であるものとする. また,

$$\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda) := \left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-0}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-1}}_{\Pi,\mathcal{S},h}(\lambda)\right) \to 1\right]\right|$$

と定義する.

定義 4.2.1. 任意の多項式時間関数 h, 任意の *PPTA* $\mathcal{A}$ に対し, ある *PPTA* $\mathcal{S}$ が存在し, 任意の *PPTA* $\mathcal{D}$ に対して $\mathsf{Adv}^{\mathit{SNM\text{-}RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda)$ が無視できるならば, Π は *SNM-RCCA* 安全であるという.

上記の SNM-RCCA の定式化において, 我々は述語を用いた定式化をしている. これは, シミュレーションベースの定式化を行う際に, 攻撃者にどのような復号オラクルにアクセスさせるかが非自明であるからである. 例えば, $m \leftarrow \mathcal{M}$ としてサンプルされた平文に復号される暗号文に対し, 復号オラクルが "Test" を返す単純な定式化を行ったとする. この定式化では, 復号オラクルは平文空間のサイズが多項式の場合, 平文 m の情報を攻撃者に漏らし, 意味のない定式化になってしまう. なぜなら, 平文空間のサイズが多項式の場合, 攻撃者は平文空間内の全ての平文の暗号文を生成し, 復号オラクルにクエリすることができる. そして, 復号オラクルはこの内の一つのクエリに対して "Test" を返し, 攻撃者はこの "Test" というオラクルからの返答によって m を特定することができる. このように, シミュレーションベースの定式化を行う場合, RCCA 環境下での復号オラクルは平文に関する情報を漏らしてしまう. そのため, RCCA 環境下でのシミュレーションベースの定式化を行う際には, 復号オラクルから得られる情報を除き, いかなる平文の情報も漏れないという直感を捉えた定式化を行う必要がある.

そこで, 攻撃者に対し "攻撃成功とみなさない条件" を記述する述語を出力させる定式化を行った. これに加え, シミュレータにはオラクルから漏れる情報を与えるため, 述語オラクルにアクセスさせる. このような定式化を行うことにより, 上記の直感を捉えた定式化を行うことができる.

また, シミュレーションベースの定式化だけでなく, 従来の IND-RCCA についても述語を用いた定式化 IND-RCC′ を考えることができる. この IND-RCCA′ と IND-RCCA は等価であることを示すことができ, この等価性は RCCA 環境が述語を用いて定式化できるという一つの裏付けとなる. 述語を用いた IND-RCCA の定式化や等価性に関する定理については, 4.6 節を参照されたい.

4.3　INM-RCCA の定義

以下に本稿で提案する RCCA 環境下における二つの識別不可能性ベースの頑強性 (INM-RCCA) の定義を与える. INM-RCCA の定式化には, 攻撃者が最後に出力する暗号文の復号を行う際, 特定の暗号文が含まれていた場合, その復号結果を特別なシンボルで置き換えるという Pass らの定式化を参考にした. また, INM-RCCA ではシミュレータを考える必要がないため, SNM-RCCA の定式化と異なり, 述語を用いずに定式化することができる.

以下に本稿で提案する, 識別不可能性ベースの頑強性 (INM-RCCA) の定義を与える.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ を PPTA の三つ組とする. 以下の二つの実験 INM-RCCA-0 と INM-RCCA-1 を考える:

$\underline{\mathrm{Exp}^{\text{INM-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
For $i = 1$ to n
$d_i := \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c_i) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$;
output b'

$\underline{\mathrm{Exp}^{\text{INM-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
For $i = 1$ to n
$d_i := \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c_i) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$;
output b'

ただし,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c) & (\text{otherwise}) \end{cases}$$

である. また,

$$\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Exp}^{\text{INM-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{INM-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right|$$

と定義する.

定義 4.3.1. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}^{\textit{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できるならば, Π は *INM-RCCA* 安全であるという.

上記の INM-RCCA では, 述語を用いない定式化がされている. しかし, INM-RCCA の実験において, 攻撃者に述語を出力させる定式化 (INM-RCCA′) を行うことも可能である. さらに, INM-RCCA′ と INM-RCCA は等価であることが示せる. そのため, RCCA 環境において, 復号オラクル $\mathcal{O}_2$ が "Test" を返すような暗号文は, 必ずしも m_0, m_1 の暗号文である必要はないことがわかる. また, この等価性から述語が RCCA 環境を捉える上で有用であることもうかがえる. INM-RCCA′ の定式化や INM-RCCA との等価性については, 4.6.4 節を参照されたい.

4.4　提案した二つの頑強性間の関係

本稿で提案した INM-RCCA と SNM-RCCA は等価であることが示せる. まず初めに, INM-RCCA が SNM-RCCA を含意することを証明し, その後 SNM-RCCA が INM-RCCA を含意することを証明する.

4.4.1　INM-RCCA⇒SNM-RCCA

INM-RCCA 安全性を満足する方式が SNM-RCCA 安全性を満足することを場合分けを用いて証明する. 具体的には, 暗号方式 Π がサポートする平文空間のサイズによって場合分けを行う. まずはじめに平文空間のサイズが多項式の場合についての証明を与え, その後サイズが多項式より大きい場合についての証明を与える.

定理 4.4.1. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *INM-RCCA* 安全であり, 平文空間のサイズが多項式であると仮定する. このとき, Π は *SNM-RCCA* 安全である.

(証明) 任意の INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の SNM-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, 任意の多項式時間関数 h に対し, ある PPTA $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し, 任意の PPTA $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 から Game 3) を使用する. また, $\mathcal{S}$ の構成は図 4.1 の通りである.

Game 0 から Game 3 を以下のように定義する:

Game 0: Game 0 は SNM-RCCA-0 である.

Game 1: Game 0 との違いは, 公開鍵/秘密鍵の生成 $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ を新たに行い, 公開鍵 pk' の下でゲームを行うものとする. $\mathcal{A}_1$ への入力は pk' に変更され, チャレンジ暗号文は pk' を用いて生成される. また, $\mathcal{A}_2$ が出力する暗号文 c_i $(i = 0, \ldots, n)$ の復号を行う際に使用される秘密鍵が sk' に変更される. さらに, $\mathcal{A}$ が使用するオラクル $\mathcal{O}_1$ と $\mathcal{O}_2$ は sk' の下でのオラクルに変更される.

Game 2: Game 1 との違いは, $m_0 \leftarrow \mathcal{M}$ が $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \mathcal{P}_{m_0}$ に変更される, ただし $\mathcal{P}_{m_0}$ は $\boldsymbol{P}(m_0, m') = 1$ を満たす平文 m' 全体の集合上の一様分布とする. また, チャレンジ暗号文 $c^* \leftarrow \mathsf{Enc}(pk', m_0)$ が $c^* \leftarrow \mathsf{Enc}(pk', m_1)$ へと変更される.

Game 3: Game 3 は PPTA $\mathcal{S}$ と pk の下での SNM-RCCA-1 である.

Game 2 及び $\mathcal{S}_2$ で分布 $\mathcal{P}_{m_0}$ を用いているが, このような分布からのサンプリングは効率的に可能である. これは, 仮定より平文空間のサイズが多項式であるため, 述語 $\boldsymbol{P}(m_0, \cdot)$ が一度定まると, 平文空間に含まれる全ての平文を $\boldsymbol{P}(m_0, \cdot)$ に入力することによって $\boldsymbol{P}(m_0, m') = 1$ を満たすような m' を全て特定可能なためである.

T_i を Game i で 1 が出力される事象とする.

補題 4.4.1. $\Pr[T_1] = \Pr[T_0]$ が成立する.

(証明) Game 1 は, (pk', sk') の下で SNM-RCCA-0 の実験に $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ が追加されているだけであり, $\mathcal{A}$ には $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ は一切入力されていない. そのため, $\mathcal{A}$ からみて Game 0 と Game 1 は同一のゲームである. よって $\Pr[T_1] = \Pr[T_0]$ が成り立つ. □

$\mathcal{S}_1(pk)$ $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1'}(pk')$ $st_1 := (pk, pk', sk', st_1')$ output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1')$	$\mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(h(m_0), st_1)$ $m_1 \leftarrow \mathcal{P}_{m_0}$ $c^* \leftarrow \mathsf{Enc}(pk', m_1)$ $(c_1', \ldots, c_n', st_2') \leftarrow \mathcal{A}_2^{\mathcal{O}_2'}(c^*, h(m_0), st_1')$ $st_2 := st_2'$ For $i = 1$ to n $d_i' := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c_i')) = 1) \\ \mathsf{Dec}(sk', c_i') & (\text{otherwise}) \end{cases}$ $c_i := \begin{cases} \mathsf{Test} & (d_i' = \mathsf{Test}) \\ \perp & (d_i' = \perp) \\ \mathsf{Enc}(pk, d_i') & (\text{otherwise}) \end{cases}$ output $(c_1, \ldots, c_n, st_2)$

図 4.1: 定理 4.4.1 内で使用される $\mathcal{S}$ の構成

Game 0 (SNM-RCCA-0) $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$ $m_0 \leftarrow \mathcal{M}$ $c^* \leftarrow \mathsf{Enc}(pk, m_0)$ $(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), st_1)$ For $i = 1$ to n $d_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$ output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n)$	Game 1 $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1'}(pk')$ $m_0 \leftarrow \mathcal{M}$ $c^* \leftarrow \mathsf{Enc}(pk', m_0)$ $(c_1', \ldots, c_n', st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2'}(c^*, h(m_0), st_1)$ For $i = 1$ to n $d_i' = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c_i')) = 1) \\ \mathsf{Dec}(sk', c_i') & (\text{otherwise}) \end{cases}$ output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1', \ldots, d_n')$
Game 2 $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1'}(pk)$ $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \mathcal{P}_{m_0}$ $c^* \leftarrow \mathsf{Enc}(pk', m_1)$ $(c_1', \ldots, c_n', st_2) \leftarrow A_2^{\mathcal{O}_2'}(c^*, h(m_0), st_1)$ For $i = 1$ to n $d_i' = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c_i')) = 1) \\ \mathsf{Dec}(sk', c) & (\text{otherwise}) \end{cases}$ output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1', \ldots, d_n')$	Game 3 (SNM-RCCA-1) $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{S}_1(pk)$ $m_0 \leftarrow \mathcal{M}$ $(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(c^*, h(m_0), st_1)$ For $i = 1$ to n $d_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk, c_i)) = 1 \vee c_i = \mathsf{Test}) \\ \perp & (c_i = \perp) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$ output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n)$

図 4.2: 定理 4.4.1 で使用されるゲーム列

$\underline{\mathcal{B}_1^{\mathcal{O}'_1}(pk')}$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$ $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \mathcal{P}_{m_0}$ $st_1 := (m_0, m_1, \mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1)$ output (m_0, m_1, st_1)	$\underline{\mathcal{B}_2^{\mathcal{O}'_2}(c^*, st_1)}$ $(c'_1, \ldots, c'_n, st'_2) \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, st'_1)$ $st_2 := (m_0, m_1, \mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_2)$ output $(c'_1, \ldots, c'_n, st_2)$
$\underline{\mathcal{B}_3(d_1, \ldots, d_n, st_2)}$ By using m_0 and $\boldsymbol{P}(\cdot,\cdot)$, check the value of $\boldsymbol{P}(m_0, d_i)$ for each d_i. d_i that satisfies $\boldsymbol{P}(m_0, d_i) = 1$ is set as $d_i :=$"Test" by the above procedure $b' \leftarrow \mathcal{D}(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st'_2)$ output b'	

図 4.3: 補題 4.4.2 内で使用される $\mathcal{B}$ の構成

補題 4.4.2. $|\Pr[T_2] - \Pr[T_1]| = \mathsf{Adv}_{\Pi,\mathcal{B}}^{INM\text{-}RCCA}(\lambda)$ となるような $\mathcal{B}$ が存在する.

(証明) $\mathcal{A}$ と $\mathcal{D}$ を内部で図 4.3 のように使用する, (pk', sk') の下での INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ を考える. また, $\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は "Test" を受け取る. その後, $\boldsymbol{P}(m_0, m) = 1$ もしくは $\mathcal{B}_2$ が "Test" を受け取った場合, $\mathcal{B}_2$ は $\mathcal{A}_2$ に "Test" を送る. そうでなければ, $\mathcal{B}_2$ は $\mathcal{A}_2$ に m を送る. $\mathcal{B}_1$ の内部で生成されている m_1 は $\boldsymbol{P}(m_0, m_1) = 1$ を満たすような平文が選択されているので, $\mathcal{B}_2$ がこのように $\mathcal{A}_2$ からの復号クエリに返答することによって $\mathcal{O}_2$ のシミュレーションを正しく行うことができる. また, 同様にして $\mathcal{B}_3$ が $\mathcal{D}$ へ入力する d_i のシミュレーションについても正しく行うことができる.

INM-RCCA-0 において $\mathcal{B}_3$ が 1 を出力するのは, 内部で利用している $\mathcal{A}_2$ が m_0 の暗号文を受け取っている状況で暗号文の列を出力し, $\mathcal{D}$ が 1 を出力している場合である. これは Game 1 において $\mathcal{D}$ が 1 を出力する場合と等価である. よって, $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-0}}(\lambda) \rightarrow 1] = \Pr[T_1]$ が成立する. また, 同様にして $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-1}}(\lambda) \rightarrow 1] = \Pr[T_2]$ が成立する.

従って,

$$\begin{aligned} |\Pr[T_2] - \Pr[T_1]| &= \left| \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-1}}(\lambda) \rightarrow 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-0}}(\lambda) \rightarrow 1\right] \right| \\ &= \mathsf{Adv}_{\Pi,\mathcal{B}}^{\text{INM-RCCA}}(\lambda). \end{aligned}$$

□

補題 4.4.3. $\Pr[T_3] = \Pr[T_2]$ が成立する.

(証明) Game 3 において, シミュレータ $\mathcal{S}$ は図 4.1 のように $\mathcal{A}$ を内部で使用する. ここで, Game 3 は SNM-RCCA-1 であるので, $\mathcal{S}$ には復号オラクルは与えられていない.

しかし, $\mathcal{S}$ は内部で (pk', sk') を生成し, 述語オラクル $\boldsymbol{P}(m_0, \cdot)$ にアクセスすることができる. また, $\mathcal{A}$ には Game 2 のように pk' を入力するため, $\mathcal{A}$ からの復号クエリに対して sk' と $\boldsymbol{P}(m_0, \cdot)$ を用いて正しく返答することができる.

$\mathcal{S}_2$ は内部で生成した m_1 の暗号文を $\mathcal{A}_2$ に入力し, $\mathcal{A}_2$ は暗号文の列を出力する. $\mathcal{S}_2$ は $\mathcal{A}_2$ が出力した全ての暗号文を sk' を用いて復号する. その後, 各 d_i は $\mathcal{S}$ によって pk を用いて暗号化され, 最終的な $\mathcal{S}$ の出力はこの暗号文の列となる. $\mathcal{S}_2$ が暗号文の列を出力した後, 全ての暗号文は復号され, $\mathcal{D}$ に入力される. ここで, $\mathcal{D}$ への入力の分布は Game 2 と Game 3 で同一である. 従って, $\Pr[T_3] = \Pr[T_2]$ が成立する.　□

補題 4.4.1 から補題 4.4.3 の結果より,

$$\begin{aligned}
\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda) &= \left| \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-0}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-1}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right] \right| \\
&= |\Pr[T_0] - \Pr[T_3]| \\
&= |\Pr[T_1] - \Pr[T_2]| \\
&= \mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda).
\end{aligned}$$

が成り立つ. よって, 任意の $\mathcal{A}$ に対し図 4.1 に示される $\mathcal{S}$ が存在し, 任意の $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda)$ は無視できる.　□

定理 4.4.2. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *INM-RCCA* 安全であり, 平文空間のサイズが多項式よりも大きいと仮定する. このとき, Π は *SNM-RCCA* 安全である.

(証明) 任意の INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の SNM-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, 任意の多項式時間関数 h に対し, ある PPTA $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し, 任意の PPTA $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 から Game 5) を使用する. また, $\mathcal{S}$ の構成は図 4.4 の通りである.

Game 0 から Game 5 を以下のように定義する:

Game 0: Game 0 は SNM-RCCA-0 である.

Game 1: Game 0 との違いは, 公開鍵/秘密鍵の生成 $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ を新たに行い, 公開鍵 pk' の下でゲームを行うものとする. $\mathcal{A}_1$ への入力は pk' に変更され, チャレンジ暗号文は pk' を用いて生成される. また, $\mathcal{A}_2$ が出力する暗号文 c_i $(i = 0, \ldots, n)$ の復号を行う際に使用される秘密鍵が sk' に変更される. さらに, $\mathcal{A}$ が使用するオラクル $\mathcal{O}_1$ と $\mathcal{O}_2$ は sk' の下でのオラクルに変更される.

Game 2: Game 1 との違いは, $m_0 \leftarrow \mathcal{M}$ が $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$ に変更される. さらに, 暗号文の列 c'_i の復号を行う際に, $m'_i \leftarrow \mathsf{Dec}(sk', c'_i), \boldsymbol{P}(m_0, m'_i) = 1 \vee m'_i = m_1$ であれば, d_i を "Test" とする.

$\mathcal{S}_1(pk)$	$\mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(h(m_0), st_1)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$	$m_1 \leftarrow \{0,1\}^\ell$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1'}(pk')$	$c^* \leftarrow \mathsf{Enc}(pk', m_1)$
$st_1 := (pk, pk', sk', st_1')$	$(c_1', \ldots, c_n', st_2') \leftarrow \mathcal{A}_2^{\mathcal{O}_2'}(c^*, h(m_0), st_1')$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1)$	$st_2 := st_2'$
	For $i = 1$ to n
	$d_i' := \begin{cases} \mathsf{Test} & (m_i' \leftarrow \mathsf{Dec}(sk', c_i'), \boldsymbol{P}(m_0, m_i') = 1 \\ & \vee m_i' = m_1) \\ \mathsf{Dec}(sk', c_i') & (\text{otherwise}) \end{cases}$
	$c_i := \begin{cases} \mathsf{Test} & (d_i' = \mathsf{Test}) \\ \perp & (d_i' = \perp) \\ \mathsf{Enc}(pk, d_i') & (\text{otherwise}) \end{cases}$
	output $(c_1, \ldots, c_n, st_2)$

図 4.4: 定理 4.4.2 内で使用される $\mathcal{S}$ の構成

Game 3: Game 2 との違いは, $\mathcal{O}_2$ が m_1 の暗号文もしくは $\boldsymbol{P}(m_0, m) = 1$ を満たすような平文 m の暗号文をクエリされた場合に "Test" を返すように変更される.

Game 4: Game 3 との違いは, チャレンジ暗号文 $c^* \leftarrow \mathsf{Enc}(pk', m_0)$ が $c^* \leftarrow \mathsf{Enc}(pk', m_1)$ に変更される.

Game 5: Game 5 は PPTA $\mathcal{S}$ と pk の下での SNM-RCCA-1 である.

T_i を Game i で 1 が出力される事象とする.

補題 4.4.4. $\Pr[T_1] = \Pr[T_0]$ が成立する.

(証明) Game 1 は, (pk', sk') の下で SNM-RCCA-0 の実験に $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ が追加されているだけであり, $\mathcal{A}$ には $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ は一切入力されていない. そのため, $\mathcal{A}$ からみて Game 0 と Game 1 は同一のゲームである. よって $\Pr[T_1] = \Pr[T_0]$ が成り立つ. □

補題 4.4.5. $|\Pr[T_2] - \Pr[T_1]| < \frac{poly(\lambda)}{2^\ell}$ が成り立つ.

(証明) Game 1 と Game 2 は $\mathcal{A}_2$ が m_1 の暗号文を出力しない場合等価である. また, m_1 は $\{0,1\}^\ell$ から一様ランダムに選択されている. $\mathcal{A}_2$ が出力する暗号文の数は $poly(\lambda)$ であるので, 差異補題及び Union Bound より $|\Pr[T_2] - \Pr[T_1]| < \frac{poly(\lambda)}{2^\ell}$ が成立する. □

<table>
<tr>
<td>Game 0 (SNM-RCCA-0)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$

$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$m_0 \leftarrow \mathcal{M}$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), st_1)$
For $i = 1$ to n
$d_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st_2)$</td>
<td>Game 1
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$
$m_0 \leftarrow \mathcal{M}$
$c^* \leftarrow \mathsf{Enc}(pk', m_0)$
$(c'_1, \ldots, c'_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
For $i = 1$ to n
$d'_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c'_i)) = 1) \\ \mathsf{Dec}(sk', c'_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d'_1, \ldots, d'_n, st'_2)$</td>
</tr>
<tr>
<td>Game 2
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$
$c^* \leftarrow \mathsf{Enc}(pk', m_0)$
$(c'_1, \ldots, c'_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
For $i = 1$ to n
$d'_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c'_i)) = 1 \\ & \vee \mathsf{Dec}(sk', c'_i) = m_1) \\ \mathsf{Dec}(sk', c'_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d'_1, \ldots, d'_n, st'_2)$</td>
<td>Game 3
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$
$c^* \leftarrow \mathsf{Enc}(pk', m_0)$
$(c'_1, \ldots, c'_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
where
$\mathcal{O}'_2 = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c'_i)) = 1 \\ & \vee \mathsf{Dec}(sk', c'_i) = m_1) \\ \mathsf{Dec}(sk', c'_i) & (\text{otherwise}) \end{cases}$
For $i = 1$ to n
$d'_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c'_i)) = 1 \\ & \vee \mathsf{Dec}(sk', c'_i) = m_1) \\ \mathsf{Dec}(sk', c'_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d'_1, \ldots, d'_n, st'_2)$</td>
</tr>
<tr>
<td>Game 4
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk)$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$
$c^* \leftarrow \mathsf{Enc}(pk', m_1)$
$(c'_1, \ldots, c'_n, st_2) \leftarrow A_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
where
$\mathcal{O}'_2 = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c'_i)) = 1 \\ & \vee \mathsf{Dec}(sk', c'_i) = m_1) \\ \mathsf{Dec}(sk', c) & (\text{otherwise}) \end{cases}$
For $i = 1$ to n
$d'_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c'_i)) = 1 \\ & \vee \mathsf{Dec}(sk', c'_i) = m_1) \\ \mathsf{Dec}(sk', c) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d'_1, \ldots, d'_n)$</td>
<td>Game 5 (SNM-RCCA-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{S}_1(pk)$
$m_0 \leftarrow \mathcal{M}$
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(c^*, h(m_0), st_1)$
For $i = 1$ to n
$d_i = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk, c_i)) = 1 \\ & \vee c_i = \mathsf{Test}) \\ \perp & (c_i = \perp) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
output $(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st_2)$</td>
</tr>
</table>

図 4.5: 定理 4.4.2 で使用されるゲーム列

$\underline{\mathcal{B}_1^{\mathcal{O}'_1}(pk')}$ $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$ $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$ $st_1 := (m_0, m_1, \mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1)$ output (m_0, m_1, st_1)	$\underline{\mathcal{B}_2^{\mathcal{O}'_2}(c^*, st_1)}$ $(c'_1, \ldots, c'_n, st'_2) \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, st'_1)$ $st_2 := (m_0, m_1, \mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_2)$ output $(c'_1, \ldots, c'_n, st_2)$
$\underline{\mathcal{B}_3(d_1, \ldots, d_n, st_2)}$ By using m_0 and $\boldsymbol{P}(\cdot,\cdot)$, check the value of $\boldsymbol{P}(m_0, d_i)$ for each d_i. d_i that satisfies $\boldsymbol{P}(m_0, d_i) = 1 \vee d_1 = m_1$ is set as $d_i :=$"Test" by the above procedure $b' \leftarrow \mathcal{D}(\mathcal{M}, m_0, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st'_2)$ output b'	

図 4.6: 補題 4.4.7 内で使用される $\mathcal{B}$ の構成

補題 4.4.6. $|\Pr[T_3] - \Pr[T_2]| < \frac{poly(\lambda)}{2^\ell}$ が成り立つ.

(証明) Game 2 と Game 3 は $\mathcal{A}_2$ によって m_1 の暗号文が復号オラクルにクエリされなければ等価である. また, m_1 は $\{0,1\}^\ell$ から一様ランダムに選択されている. $\mathcal{A}_2$ がクエリできる暗号文の個数は $poly(\lambda)$ なので, 差異補題及び Union Bound より $|\Pr[T_3] - \Pr[T_2]| < \frac{poly(\lambda)}{2^\ell}$ が成立する. □

補題 4.4.7. $|\Pr[T_4] - \Pr[T_3]| = \mathsf{Adv}_{\Pi,\mathcal{B}}^{INM\text{-}RCCA}(\lambda)$ が成り立つような $\mathcal{B}$ が存在する.

(証明) 図 4.6 のように内部で $\mathcal{A}$ と $\mathcal{D}$ を使用する (pk', sk') の下での INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ を考える. また, $\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は "Test" を受け取る. その後, $\boldsymbol{P}(m_0, m) = 1 \vee m = m_1$ もしくは $\mathcal{B}_2$ が "Test" を受け取った場合, $\mathcal{B}_2$ は $\mathcal{A}_2$ に "Test" を送る. そうでなければ, $\mathcal{B}_2$ は $\mathcal{A}_2$ に m を送る.

INM-RCCA-0 において $\mathcal{B}_3$ が 1 を出力するのは, 内部で利用している $\mathcal{A}_2$ が m_0 の暗号文を受け取っている状況で暗号文の列を出力し, $\mathcal{D}$ が 1 を出力している場合である. これは Game 3 において $\mathcal{D}$ が 1 を出力する場合と等価である. よって, $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-0}}(\lambda) \rightarrow 1] = \Pr[T_3]$ が成立する. また, 同様にして $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-1}}(\lambda) \rightarrow 1] = \Pr[T_4]$ が成立する.

従って,

$$\begin{aligned} |\Pr[T_4] - \Pr[T_3]| &= \left| \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-1}}(\lambda) \rightarrow 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{INM-RCCA-0}}(\lambda) \rightarrow 1\right] \right| \\ &= \mathsf{Adv}_{\Pi,\mathcal{B}}^{\text{INM-RCCA}}(\lambda). \end{aligned}$$

が成立する.

□

補題 4.4.8. $\Pr[T_5] = \Pr[T_4]$ が成立する.

(証明) Game 5 において, シミュレータ $\mathcal{S}$ は内部で図 4.4 のように $\mathcal{A}$ を使用している. ここで, Game 5 は SNM-RCCA-1 であるので, $\mathcal{S}$ には復号オラクルは与えられていない. しかし, $\mathcal{S}$ は内部で (pk', sk') を生成し, 述語オラクル $\boldsymbol{P}(m_0, \cdot)$ にアクセスすることができる. また, $\mathcal{A}$ には Game 4 のように pk' を入力するため, $\mathcal{A}$ からの復号クエリに対して sk' と $\boldsymbol{P}(m_0, \cdot)$ を用いて正しく返答することができる.

$\mathcal{S}_2$ は内部で生成した m_1 の暗号文を $\mathcal{A}_2$ に入力し, $\mathcal{A}_2$ は暗号文の列を出力する. $\mathcal{S}_2$ は $\mathcal{A}_2$ が出力した全ての暗号文を sk' を用いて復号する. その後, 各 d_i は $\mathcal{S}$ によって pk を用いて暗号化され, 最終的な $\mathcal{S}$ の出力はこの暗号文の列となる. $\mathcal{S}_2$ が暗号文の列を出力した後, 全ての暗号文は復号され, $\mathcal{D}$ に入力される. ここで, $\mathcal{D}$ への入力の分布は Game 4 と Game 5 で同一である. 従って, $\Pr[T_5] = \Pr[T_4]$ が成立する. □

補題 4.4.4 から補題 4.4.8 の結果より,

$$
\begin{aligned}
\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda) &= \left| \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-0}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-1}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right] \right| \\
&= |\Pr[T_0] - \Pr[T_5]| \\
&= |\Pr[T_1] - \Pr[T_4]| \\
&= |\Pr[T_1] - \Pr[T_2] + \Pr[T_2] - \Pr[T_3] + \Pr[T_3] - \Pr[T_4]| \\
&\leq |\Pr[T_1] - \Pr[T_2]| + |\Pr[T_2] - \Pr[T_3]| + |\Pr[T_3] - \Pr[T_4]| \\
&\leq \frac{poly(\lambda)}{2^\ell} + \frac{poly(\lambda)}{2^\ell} + \mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)
\end{aligned}
$$

が成り立つ. ここで, 平文空間のサイズが多項式よりも大きいことと, Π が INM-RCCA 安全であることを仮定していたので, 任意の $\mathcal{A}$ に対し図 4.4 に示される $\mathcal{S}$ が存在し, 任意の $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h}(\lambda)$ は無視できる. □

定理 4.4.1, 4.4.2 より以下の定理が成り立つ.

定理 4.4.3. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *INM-RCCA* 安全ならば, Π は *SNM-RCCA* 安全である.

4.4.2　SNM-RCCA⇒ INM-RCCA

本節では SNM-RCCA 安全性が INM-RCCA 安全性を含意することを示す.

定理 4.4.4. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *SNM-RCCA* 安全であるならば, Π は *INM-RCCA* 安全である.

(証明) $\mathsf{Exp}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}$ を実験がチャレンジビット b をランダムに選択することを表すとする. このとき, 一般性を失うことなく任意の INM-RCCA 攻撃者 $\mathcal{A}$ に対し,

Game 0 (INM-RCCA′-0)	Game 1 (INM-RCCA′-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$	$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$
For $i = 1$ to n	For $i = 1$ to n
$d_i := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(\mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$	$d_i := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(\mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$	$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$

図 4.7: 定理 4.4.4 で使用されるゲーム列

$\Pr[\mathsf{Exp}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b] \geq 1/2$ とすることができる. なぜなら, $\Pr[\mathsf{Exp}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b] < 1/2$ ならば, $\mathcal{A}$ の出力を反転させて出力する攻撃者 $\mathcal{A}'$ を考えることができる. すると, $\mathcal{A}'$ と $\mathcal{A}$ の優位性は同じであるが, $\Pr[\mathsf{Exp}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}'}(\lambda) \to b] \geq 1/2$ となる. 従って, $\mathcal{A}'$ の優位性を抑えることができれば, それは同時に $\mathcal{A}$ の優位性を抑えることになる.

任意の SNM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ と任意の多項式時間関数 h に対し, ある PPTA $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し, 任意の $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SNM-RCCA}}_{\Pi,\mathcal{B},\mathcal{D},h}(\lambda)$ が無視できると仮定する. このとき, 任意の INM-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 と Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は INM-RCCA-0 である.

Game 1: Game 1 は INM-RCCA-1 である.

T_i を INM-RCCA-i $(i = 0, 1)$ で 1 が出力される事象とする.

$h : m \mapsto \epsilon$ における SNM-RCCA-0 を考える, ただし ϵ は空文字列である. また, このとき 図 4.8 のように内部で $\mathcal{A}$ を使用する SNM-RCCA 攻撃者 $\mathcal{B}$ と $\mathcal{D}$ を構成する. $\mathcal{A}_2$ が $\mathcal{B}_2$ に復号クエリ c を送ってきた場合, $\mathcal{B}_2$ は自身がアクセスできる復号オラクルに c を送る. その後, $\mathcal{B}_2$ は復号オラクルからの返答をそのまま $\mathcal{A}_2$ に送る.

上記の $\mathcal{B}, \mathcal{D}$ の構成より, $\mathcal{D}$ が 1 を出力するのは, $\mathcal{B}$ 及び $\mathcal{D}$ の内部の $\mathcal{A}$ が試行によって選択される b を正しく推測した場合である. 従って,

$$\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-0}}_{\Pi,\mathcal{B},h}(\lambda)\right) \to 1\right] = \Pr\left[\mathsf{Exp}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b\right]$$

が成り立つ.

SNM-RCCA-1 において, $\mathcal{S}$ が $\|\mathcal{M}\| = 2$ かつ, $\boldsymbol{P}(m, m_0) = 1 \wedge \boldsymbol{P}(m, m_1) = 1$ を満たすような $\mathcal{M}, \boldsymbol{P}$ を出力する事象を E とし, その確率を p とする. ただし, $[\{m_0, m_1\}, \Pr(m_0) = \Pr(m_1) = 1/2] = \mathcal{M}$ である. SNM-RCCA-1 において $\mathcal{S}$ はチャ

$\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$	$\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)}$
$(m_0, m_1, st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$\mathcal{M} := [\{m_0, m_1\}, \Pr(m_0) = \Pr(m_1) = 1/2]$	$(c_1, \ldots, c_n, st_2') \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1')$
$\boldsymbol{P}(m, m') := \begin{cases} 1 & (m' \in \{m_0, m_1\}) \\ 0 & (\text{otherwise}) \end{cases}$	$st_2 := (m_0, m_1, \boldsymbol{P}(\cdot,\cdot), st_2')$
$st_1 := (m_0, m_1, \boldsymbol{P}(\cdot,\cdot), st_1')$	output $(c_1, \ldots, c_n, st_2)$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1)$	

$\underline{\mathcal{D}(\mathcal{M}, m, \boldsymbol{P}(\cdot,\cdot), d_1, \ldots, d_n, st_2)}$
if $\|\mathcal{M}\| \neq 2$, then output 0
else if $\boldsymbol{P}'(m, m_0) = 0 \vee \boldsymbol{P}'(m, m_1) = 0$, then output 0,
　where $[\{m_0, m_1\}, \Pr(m_0) = \Pr(m_1) = 1/2] = \mathcal{M}$
else if $b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2') \wedge m = m_{b'}$, then output 1
else then output 0

図 4.8: 定理 4.4.4 内で使用される $\mathcal{B}$ と $\mathcal{D}$ の構成

レンジ暗号文を受け取らず, 述語オラクルへのアクセスによって m_0, m_1 の選択に関するいかなる情報も得られない. また, $\|\mathcal{M}\| = 2$ であるので,

$$\begin{aligned} \Pr\left[\mathcal{D}\left(\mathsf{Exp}_{\Pi,\mathcal{S},h}^{\text{SNM-RCCA-1}}(\lambda)\right) \to 1\right] &= \Pr\left[\mathcal{D}\left(\mathsf{Exp}_{\Pi,\mathcal{S},h}^{\text{SNM-RCCA-1}}(\lambda)\right) \to 1 \middle| E\right] \cdot \Pr[E] \\ &= \frac{p}{2} \\ &\leq \frac{1}{2} \end{aligned} \tag{4.1}$$

となる.

ここで, $\mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda)$ は

$$\begin{aligned} \mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda) &= \left|\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA-0}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA-1}}(\lambda) \to 1\right]\right| \\ &= \left|2 \cdot \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda) \to b\right] - 1\right| \end{aligned}$$

と書き直すことができる. このとき,

$$\begin{aligned} \mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda) &= \left|2 \cdot \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda) \to b\right] - 1\right| \\ &= \left|2 \cdot \Pr\left[\mathcal{D}\left(\mathsf{Exp}_{\Pi,\mathcal{B},h}^{\text{SNM-RCCA-0}}(\lambda)\right) \to 1\right] - 1\right| \\ &\leq \left|2 \cdot \Pr\left[\mathcal{D}\left(\mathsf{Exp}_{\Pi,\mathcal{B},h}^{\text{SNM-RCCA-0}}(\lambda)\right) \to 1\right] - 2 \cdot p/2\right| \\ &= 2\left(\left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}_{\Pi,\mathcal{B},h}^{\text{SNM-RCCA-0}}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}_{\Pi,\mathcal{S},h}^{\text{SNM-RCCA-1}}(\lambda)\right) \to 1\right]\right)\right. \\ &= 2 \cdot \mathsf{Adv}_{\Pi,\mathcal{B},\mathcal{D},h}^{\text{SNM-RCCA}}(\lambda) \end{aligned}$$

となる, なお式変形には不等式 (4.1) を用いた. よって, 任意の PPTA $\mathcal{A}$ に対して $\mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda)$ は無視できる. □

Game 0 (IND-RCCA-0)	Game 1 (IND-RCCA-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$

図 4.9: 定理 4.5.1 で使用されるゲーム列

4.5　既存の RCCA 環境下における安全性概念との関係

4.4 節にて, 本稿で提案した SNM-RCCA と INM-RCCA が等価であることを証明した. 本節では, SNM-RCCA 及び, INM-RCCA が Canetti らが提案した IND-RCCA と等価であることを証明する.

具体的には以下の定理 4.5.1 と定理 4.5.2 が成り立つ.

定理 4.5.1. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *INM-RCCA* 安全ならば, Π は *IND-RCCA* 安全である.

(証明) 任意の INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の IND-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す.

証明を与える上で, 以下のゲーム列 (Game 0 and Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は IND-RCCA-0 である.

Game 1: Game 1 は IND-RCCA-1 である.

T_i を Game i で 1 が出力される事象とする. このとき, $\Pr[T_0] = \Pr[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1], \Pr[T_1] = \Pr[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1]$ が成立する.

補題 4.5.1. $|\Pr[T_1] - \Pr[T_0]| = \mathsf{Adv}^{\textit{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ を満たすような $\mathcal{B}$ が存在する.

(証明) 図 4.10 のように $\mathcal{A}$ を内部で使用する (pk, sk) の下での INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ を構成する. 図 4.10 の $\mathcal{B}$ の構成より, $\mathcal{B}_3$ は, m_0 の暗号文を $\mathcal{B}_2$ から $\mathcal{A}_2$ が受け取った状況で, $\mathcal{A}_2$ が 1 を出力するときに限り 1 を出力する. これは IND-RCCA-0 で 1 が出力される確率と等価であるため, $\Pr[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_0]$ が成立する. また, 同様にして, $\Pr[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_1]$ が成立する.

従って,

$$\begin{aligned} |\Pr[T_1] - \Pr[T_0]| &= \left|\Pr\left[\mathsf{Exp}^{\text{INM-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{INM-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda) \end{aligned}$$

$\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ $(m_0, m_1, st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$ $st_1 := (m_0, m_1, st_1')$ output (m_0, m_1, st_1)	$\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)}$ $b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1')$ c : empty string $st_2 := b'$ output (c, st_2)
$\underline{\mathcal{B}_3(d, st_2)}$ output b'	

図 4.10: 補題 4.5.1 で使用される $\mathcal{B}$ の構成

が成立する. □

補題 4.5.1 の結果より, Π が INM-RCCA 安全であることを仮定していたので,

$$\begin{aligned}\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) &= \left|\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)\end{aligned}$$

は無視できる. □

定理 4.5.2. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *IND-RCCA* 安全ならば, Π は *INM-RCCA* 安全である.

(証明) 任意の IND-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の INM-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す.

証明を与える上で, 以下のゲーム列 (Game 0 and Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は INM-RCCA-0 である.

Game 1: Game 1 は INM-RCCA-1 である.

T_i を Game i で 1 が出力される事象とする. このとき, $\Pr[T_0] = \Pr[\mathsf{Exp}^{\text{INM-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1], \Pr[T_1] = \Pr[\mathsf{Exp}^{\text{INM-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1]$ が成立する.

補題 4.5.2. $|\Pr[T_1] - \Pr[T_0]| = \mathsf{Adv}^{\textit{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ を満たすような $\mathcal{B}$ が存在する.

(証明)

図 4.12 のように $\mathcal{A}$ を内部で使用する (pk, sk) の下での IND-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ を構成する. 図 4.12 の $\mathcal{B}$ の構成より, $\mathcal{B}_2$ は, m_0 の暗号文を $\mathcal{B}_2$ から $\mathcal{A}_2$ が受け取った状況で, $\mathcal{A}_2$ からの出力された暗号文の列の復号結果を入力として受け取った $\mathcal{A}_3$ が 1 を出力するときに限り 1 を出力する. これは INM-RCCA-0 で 1 が出力され

Game 0 (INM-RCCA-0)	Game 1 (INM-RCCA-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$	$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$
For $i = 1$ to n	For $i = 1$ to n
$d_i := \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c_i) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$	$d_i := \begin{cases} \mathsf{Test} & (\mathsf{Dec}(sk, c_i) \in \{m_0, m_1\}) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(d_1, \ldots, d_n, st_2)$	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(d_1, \ldots, d_n, st_2)$

図 4.11: 定理 4.5.2 で使用されるゲーム列

$\mathcal{B}_1^{\mathcal{O}_1}(pk)$	$\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)$
$(m_0, m_1, st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(c_1, \ldots, c_n, st_2') \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1')$
$st_1 := st_1'$	For $i = 1$ to n
output (m_0, m_1, st_1)	$d_i := \mathcal{O}_2(c_i)$
	$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2')$

図 4.12: 補題 4.5.2 で使用される $\mathcal{B}$ の構成

る確率と等価であるため, $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-0}}(\lambda) \to 1] = \Pr[T_0]$ が成立する. また, 同様にして, $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-1}}(\lambda) \to 1] = \Pr[T_1]$ が成立する.

従って,

$$\begin{aligned} |\Pr[T_1] - \Pr[T_0]| &= \left|\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-0}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-1}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}_{\Pi,\mathcal{B}}^{\text{IND-RCCA}}(\lambda) \end{aligned}$$

が成立する. □

補題 4.5.2 の結果より, Π が IND-RCCA 安全であることを仮定していたので,

$$\begin{aligned} \mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{INM-RCCA}}(\lambda) &= \left|\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA-0}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA-1}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}_{\Pi,\mathcal{B}}^{\text{IND-RCCA}}(\lambda) \end{aligned}$$

は無視できる. □

4.6　述語を用いた IND-RCCA と INM-RCCA の定式化

SNM-RCCA の定式化のように, IND-RCCA 及び INM-RCCA の実験中において攻撃者に述語を出力させる定式化を行うことができる. また, 述語を用いた定式化は述語を用いない定式化と等価であることが示せる. この等価性は, 述語が RCCA 環境を捉えることに有用であるという直感を示すことができる.

4.6.1　IND-RCCA′の定義

以下に IND-RCCA と等価である, 述語を用いた識別不可能性 IND-RCCA′ について記す.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA の二つ組とする. 以下の二つの実験 IND-RCCA′-0 と IND-RCCA′-1 を考える:

$\mathrm{Exp}^{\text{IND-RCCA′-0}}_{\Pi,\mathcal{A}}(\lambda)$	$\mathrm{Exp}^{\text{IND-RCCA′-1}}_{\Pi,\mathcal{A}}(\lambda)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
output b'	output b'

ただし, 述語 $\boldsymbol{P}$ は $\boldsymbol{P}(m_0) = \boldsymbol{P}(m_1) = 1$ を満たすものとする. また,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(\mathsf{Dec}(sk, c)) = 1) \\ \mathsf{Dec}(sk, c) & (\text{otherwise}) \end{cases}$$

である. また,

$$\mathsf{Adv}^{\text{IND-RCCA′}}_{\Pi,\mathcal{A}}(\lambda) := \left| \Pr\left[\mathsf{Exp}^{\text{IND-RCCA′-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA′-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] \right|$$

と定義する.

定義 4.6.1. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}^{\textit{IND-RCCA′}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できるならば, Π は *IND-RCCA′* 安全であるという.

4.6.2　IND-RCCA⇒IND-RCCA′

定理 4.6.1. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *IND-RCCA* 安全ならば, Π は *IND-RCCA′* 安全である.

(証明) 任意の IND-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の IND-RCCA′ 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA′}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 と Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は IND-RCCA′-0 である.

Game 0 (IND-RCCA′-0)	Game 1 (IND-RCCA′-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$b' \leftarrow \mathcal{A}_2(c^*, st_1)$	$b' \leftarrow \mathcal{A}_2(c^*, st_1)$

図 4.13: 定理 4.6.1 で使用されるゲーム列

$\mathcal{B}_1^{\mathcal{O}_1}(pk)$	$\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)$
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$
$st_1 := (m_0, m_1, \boldsymbol{P}(\cdot), st_1')$	output b'
output (m_0, m_1, st_1)	

図 4.14: 定理 4.6.1 で使用される $\mathcal{B}$ の構成

Game 1: Game 1 は IND-RCCA′-1 である.

T_i を Game i で 1 が出力される事象とする.

図 4.14 のように $\mathcal{A}$ を内部で使用する IND-RCCA′ 攻撃者 $\mathcal{B}$ を構成する. $\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は “Test” を受け取る. その後, $\boldsymbol{P}(m) = 1$ である, 又は $\mathcal{B}$ が “Test” をオラクルから受け取っていた場合, $\mathcal{B}_2$ は $\mathcal{A}_2$ に “Test” を返す. そうでなければ, $\mathcal{B}_2$ は $\mathcal{A}_2$ に m を返す.

図 4.14 の $\mathcal{B}$ の構成より, $\mathcal{B}$ は, m_0 の暗号文を $\mathcal{B}_2$ から受け取った $\mathcal{A}_2$ が 1 を出力するときに限り 1 を出力するため, $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-0}}(\lambda) \to 1] = \Pr[T_0]$ が成り立つ. また, 同様にして, $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-1}}(\lambda) \to 1] = \Pr[T_1]$ が成り立つ.

従って,

$$\begin{aligned}
\mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{IND-RCCA}'}(\lambda) &= |\Pr[T_1] - \Pr[T_0]| \\
&= \left|\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-0}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\text{IND-RCCA-1}}(\lambda) \to 1\right]\right| \\
&= \mathsf{Adv}_{\Pi,\mathcal{B}}^{\text{IND-RCCA}}(\lambda)
\end{aligned}$$

が成り立つ.

□

4.6.3 IND-RCCA′⇒IND-RCCA

定理 4.6.2. 公開鍵暗号式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *IND-RCCA′* 安全ならば, Π は *IND-RCCA* 安全である.

(証明) 任意の IND-RCCA′ 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対し, $\mathsf{Adv}_{\Pi,\mathcal{B}}^{\text{IND-RCCA}'}(\lambda)$ が無視

Game 0 (IND-RCCA-0)	Game 1 (IND-RCCA-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$b' \leftarrow \mathcal{A}_2(c^*, st_1)$	$b' \leftarrow \mathcal{A}_2(c^*, st_1)$

図 4.15: 定理 4.6.2 で使用されるゲーム列

できると仮定する．このとき, 任意の IND-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 と Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は IND-RCCA-0 である.

Game 1: Game 1 は IND-RCCA-1 である.

T_i を Game i で 1 が出力される事象とする.

図 4.16 のように $\mathcal{A}$ を内部で使用する IND-RCCA 攻撃者 $\mathcal{B}$ を構成する, ただし

$$\boldsymbol{P}_{m_0,m_1}(m) = \begin{cases} 1 & (m \in \{m_0, m_1\}) \\ 0 & (\text{otherwise}). \end{cases}$$

である. $\mathcal{A}_2$ が復号クエリとして c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は "Test" を受け取る. その後, $\mathcal{B}_2$ はオラクルからの出力を $\mathcal{A}_2$ に送る. $\boldsymbol{P}_{m_0,m_1}$ は入力が m_0 もしくは m_1 のときのみ 1 を出力するので, $\mathcal{A}_2$ からのクエリに対し, $\mathcal{B}_2$ は常に正しく返答できる.

図 4.16 の $\mathcal{B}$ の構成より, $\mathcal{B}$ は, m_0 の暗号文を $\mathcal{B}_2$ から受け取った $\mathcal{A}_2$ が 1 を出力するときに限り 1 を出力するため, $\Pr[\mathsf{Exp}^{\text{IND-RCCA}'\text{-}0}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_0]$ が成り立つ. また, 同様にして $\Pr[\mathsf{Exp}^{\text{IND-RCCA}'\text{-}1}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_1]$ が成り立つ.

従って,

$$\begin{aligned} \mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) &= |\Pr[T_1] - \Pr[T_0]| \\ &= \left|\Pr\left[\mathsf{Exp}^{\text{IND-RCCA}'\text{-}0}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA}'\text{-}1}_{\Pi,\mathcal{B}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}^{\text{IND-RCCA}'}_{\Pi,\mathcal{B}}(\lambda) \end{aligned}$$

が成り立つ.

□

4.6.4　INM-RCCA′ の定義

以下に INM-RCCA と等価である, 述語を用いた識別不可能性ベースの頑強性 INM-RCCA′ について記す.

$\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$	$\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)}$
$(m_0, m_1, st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$
$st_1 := (m_0, m_1, \boldsymbol{P}_{m_0,m_1}(\cdot), st_1')$	output b'
output $(m_0, m_1, \boldsymbol{P}_{m_0,m_1}(\cdot), st_1)$	

図 4.16: 定理 4.6.2 で使用される $\mathcal{B}$ の構成

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ を PPTA の三つ組とする. 以下の二つの実験 INM-RCCA′-0 と INM-RCCA′-1 を考える:

$\underline{\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA′-0}}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
For $i = 1$ to n
$d_i := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(\mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2;)$
output b'

$\underline{\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA′-1}}(\lambda)}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \leftarrow \mathsf{Enc}(pk, m_1)$;
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$;
For $i = 1$ to n
$d_i := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(\mathsf{Dec}(sk, c_i)) = 1) \\ \mathsf{Dec}(sk, c_i) & (\text{otherwise}) \end{cases}$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$;
output b'

ただし, 述語 $\boldsymbol{P}$ は $\boldsymbol{P}(m_0) = \boldsymbol{P}(m_1) = 1$ を満たすものとする. また,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$
$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(\mathsf{Dec}(sk, c)) = 1) \\ \mathsf{Dec}(sk, c) & (\text{otherwise}) \end{cases}$$

である. また,

$$\mathsf{Adv}_{\Pi,\mathcal{A}}^{\text{INM-RCCA′}}(\lambda) := \left| \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA′-0}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\text{INM-RCCA′-1}}(\lambda) \to 1\right] \right|$$

と定義する.

定義 4.6.2. 任意の *PPTA* $\mathcal{A}$ に対し, $\mathsf{Adv}_{\Pi,\mathcal{A}}^{INM\text{-}RCCA'}(\lambda)$ が無視できるならば, Π は *INM-RCCA′* 安全であるという.

4.6.5　INM-RCCA⇒INM-RCCA′

定理 4.6.3. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *INM-RCCA* 安全ならば, Π は *INM-RCCA′* 安全である.

Game 0 (INM-RCCA′-0)	Game 1 (INM-RCCA′-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, \boldsymbol{P}(\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$	$(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1)$
$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$	$b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$

図 4.17: 定理 4.6.3 で使用されるゲーム列

(証明) 任意の INM-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の INM-RCCA′ 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}'}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す.

証明を与える上で, 以下のゲーム列 (Game 0 と Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は INM-RCCA′-0 である.
Game 1: Game 1 は INM-RCCA′-1 である.

T_i を Game i で 1 が出力される事象とする.

図 4.18 のように $\mathcal{A}$ を内部で使用する INM-RCCA 攻撃者 $\mathcal{B}$ を構成する. $\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は "Test" を受け取る. その後, $\boldsymbol{P}(m) = 1$ もしくは $\mathcal{B}_2$ が "Test" を受け取った場合, $\mathcal{B}_2$ は $\mathcal{A}_2$ に "Test" を送る. そうでなければ, $\mathcal{B}_2$ は $\mathcal{A}_2$ に m を送る.

図 4.18 の $\mathcal{B}$ の構成より, $\mathcal{B}$ は, m_0 の暗号文を $\mathcal{B}_2$ から受け取った $\mathcal{A}_2$ が出力した暗号文の列を復号した結果の列を受け取った $\mathcal{A}_3$ が 1 を出力するときに限り 1 を出力するため, $\Pr[\mathsf{Exp}^{\text{INM-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_0]$ が成り立つ. また, 同様にして $\Pr[\mathsf{Exp}^{\text{INM-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_1]$ が成り立つ.

従って,

$$\begin{aligned} |\Pr[T_1] - \Pr[T_0]| &= \left| \Pr\left[\mathsf{Exp}^{\text{INM-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{INM-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] \right| \\ &= \mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{B}}(\lambda) \end{aligned}$$

が成立する. □

4.6.6　INM-RCCA′⇒INM-RCCA

定理 4.6.4. 公開鍵暗号式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *INM-RCCA′* 安全ならば, Π は *INM-RCCA* 安全である.

$\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ $(m_0, m_1, \boldsymbol{P}(\cdot), st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$ $st_1 := (m_0, m_1, \boldsymbol{P}(\cdot), st_1')$ output (m_0, m_1, st_1)	$\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)}$ $(c_1', \ldots, c_n', st_2') \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1')$ For $i = 1$ to n $d_i := \begin{cases} m_0 & (\mathcal{O}_2(c_i') = \mathsf{Test} \\ & \vee m_i' \leftarrow \mathcal{O}_2(c_i'), \boldsymbol{P}(m_i') = 1) \\ \mathcal{O}_2(c_i') & (\text{otherwise}) \end{cases}$ For $i = 1$ to n $c_i := \mathsf{Enc}(pk, m_i)$ $st_2 := st_2'$ output $(c_1, \ldots, c_n, st_2)$
$\underline{\mathcal{B}_3(d_1, \ldots, d_n, st_2)}$ $b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$ output b'	

図 4.18: 定理 4.6.3 内で使用される $\mathcal{B}$ の構成

$\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ $(m_0, m_1, st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$ $st_1 := (m_0, m_1, \boldsymbol{P}_{m_0,m_1}(\cdot), st_1')$ output $(m_0, m_1, \boldsymbol{P}_{m_0,m_1}(\cdot), st_1)$	$\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)}$ $(c_1, \ldots, c_n, st_2) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1')$ output $(c_1, \ldots, c_n, st_2)$
$\underline{\mathcal{B}_3(d_1, \ldots, d_n, st_2)}$ $b' \leftarrow \mathcal{A}_3(d_1, \ldots, d_n, st_2)$ output b'	

図 4.19: 定理 4.6.4 内で使用される $\mathcal{B}$ の構成

(証明) 任意の INM-RCCA′ 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}'}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の INM-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ に対し, $\mathsf{Adv}^{\text{INM-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す. T_i を INM-RCCA-i $(i = 0, 1)$ で 1 が出力される事象とする.

図 4.19 のように $\mathcal{A}$ を内部で使用する INM-RCCA′ 攻撃者 $\mathcal{B}$ を構成する, ただし

$$\boldsymbol{P}_{m_0,m_1}(m) = \begin{cases} 1 & (m \in \{m_0, m_1\}) \\ 0 & (\text{otherwise}) \end{cases}$$

である.

$\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は “Test” を受け取る. その後, $\mathcal{B}_2$ はオラクルからの出力を $\mathcal{A}_2$ に送る. $\boldsymbol{P}_{m_0,m_1}$ は入力が m_0 もしくは m_1 のときのみ 1 を出力するので, $\mathcal{A}_2$ からのクエリに対し, $\mathcal{B}_2$ は常に正しく返答できる.

図 4.19 の $\mathcal{B}$ の構成より, $\mathcal{B}$ は, m_0 の暗号文を $\mathcal{B}_2$ から受け取った $\mathcal{A}_2$ が出力した暗号文の列を復号した結果の列を受け取った $\mathcal{A}_3$ が 1 を出力するときに限り 1 を出力するため, $\Pr[\mathsf{Exp}^{\text{INM-RCCA}'\text{-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_0]$ が成り立つ. また, 同様にして $\Pr[\mathsf{Exp}^{\text{INM-RCCA}'\text{-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1] = \Pr[T_1]$ が成り立つ.

従って,

$$\begin{aligned}|\Pr[T_1] - \Pr[T_0]| &= \left|\Pr\left[\mathsf{Exp}^{\text{INM-RCCA}'\text{-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{INM-RCCA}'\text{-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}^{\text{INM-RCCA}'}_{\Pi,\mathcal{B}}(\lambda)\end{aligned}$$

が成り立つ. □

Chapter 5　RCCA 環境下における意味論的安全性の定式化

5.1　SS-RCCA の定義

以下に本稿で提案する RCCA 環境下での強秘匿性 (SS-RCCA) の定義を述べる. SS-RCCA の定式化は SNM-RCCA の定式化と同様にして, 述語を用いて定式化することができる.

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を PPTA とする. また, h, f を多項式時間関数とする. 以下の二つの実験 SS-RCCA-0 と SS-RCCA-1 を考える:

$\mathrm{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{A},h,f}(\lambda)$	$\mathrm{Exp}^{\text{SS-RCCA-1}}_{\Pi,\mathcal{S},h,f}(\lambda)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$;
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;	$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{S}_1(pk)$;
$m \leftarrow \mathcal{M}$;	$m \leftarrow \mathcal{M}$;
$c^* \leftarrow \mathsf{Enc}(pk, m)$;	$c^* \leftarrow \mathsf{Enc}(pk, m)$;
$v \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m), st_1)$;	$v \leftarrow \mathcal{S}_2^{\boldsymbol{P}(m,\cdot)}(h(m), st_1)$;
If $v = f(m)$, then $\beta := 1$	If $v = f(m)$, then $\beta := 1$
Else $\beta := 0$	Else $\beta := 0$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$

ただし, 述語 $\boldsymbol{P}$ は $\mathcal{M}$ のサポートに含まれる任意の m に対し, $\boldsymbol{P}(m, m) = 1$ を満たすものとする. また,

$$\mathcal{O}_1(c) = \mathsf{Dec}(sk, c),$$

$$\mathcal{O}_2(c) = \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m, \mathsf{Dec}(sk, c)) = 1) \\ \mathsf{Dec}(sk, \cdot) & (\text{otherwise}) \end{cases}$$

である. 上記の二つの実験において, $\mathcal{M}$ は暗号方式における平文空間上の分布であるものとする. また,

$$\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda) := \left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{A},h,f}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-1}}_{\Pi,\mathcal{S},h,f}(\lambda)\right) \to 1\right]\right|$$

と定義する.

定義 5.1.1. 任意の多項式時間関数 h, f, 任意の *PPTA* $\mathcal{A}$ に対し, ある *PPTA* $\mathcal{S}$ が存在し, 任意の *PPTA* $\mathcal{D}$ に対して, $\mathsf{Adv}^{\textit{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda)$ が無視できるならば Π は *SS-RCCA* 安全であるという.

5.2　IND-RCCA との関係

本稿で提案した SS-RCCA は IND-RCCA と等価であることが示せる.

5.2.1　IND-RCCA⇒SS-RCCA

以下に IND-RCCA 安全性を満足する方式が SS-RCCA 安全性を満足することを示す. 定理 4.4.1, 4.4.2 と同様にして暗号方式がサポートする平文空間のサイズによって場合分けを行い証明する.

定理 5.2.1. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *IND-RCCA* 安全であり, 平文空間のサイズが多項式であると仮定する. このとき, Π は *SS-RCCA* 安全である.

(証明) 任意の IND-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の SS-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, 任意の多項式時間関数 h, f に対し, ある PPTA $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し, 任意の PPTA $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 から Game 3) を使用する.

Game 0 から Game 3 を以下のように定義する:

Game 0: Game 0 は SS-RCCA-0 である.

Game 1: Game 0 との違いは, 公開鍵/秘密鍵の生成 $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ を新たに行い, 公開鍵 pk' の下でゲームを行うものとする. $\mathcal{A}_1$ への入力は pk' に変更され, チャレンジ暗号文は pk' を用いて生成される. さらに, $\mathcal{A}$ が使用するオラクル $\mathcal{O}_1$ と $\mathcal{O}_2$ は sk' の下でのオラクルに変更される.

Game 2: Game 1 との違いは, $m_0 \leftarrow \mathcal{M}$ が $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \mathcal{P}_{m_0}$ に変更される, ただし $\mathcal{P}_{m_0}$ は $\boldsymbol{P}(m_0, m') = 1$ を満たす平文 m' 全体の集合である. また, チャレンジ暗号文 $c^* \leftarrow \mathsf{Enc}(pk', m_0)$ が $c^* \leftarrow \mathsf{Enc}(pk', m_1)$ へと変更される.

Game 3: Game 2 は PPTA $\mathcal{S}$ と pk の下での SS-RCCA-1 であり, $\mathcal{S}$ は内部で $\mathcal{A}$ を図 5.2 のように使用しているものとする.

Game 2 及び $\mathcal{S}_2$ で分布 $\mathcal{P}_{m_0}$ を用いているが, 定理 4.4.1 の証明と同様にして, このような分布からのサンプリングは効率的に可能である.

T_i を Game i で 1 が出力される事象とする.

補題 5.2.1. $\Pr[T_1] = \Pr[T_0]$ が成立する.

(証明) Game 1 は, (pk', sk') の下で SS-RCCA-0 の実験に $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ が追加されているだけであり, $\mathcal{A}$ には $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ は一切入力されていない. そのた

Game 0 (SS-RCCA-0)	Game 1
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
	$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$
$m_0 \leftarrow \mathcal{M}$	$m_0 \leftarrow \mathcal{M}$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk', m_0)$
$v \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), st_1)$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
If $v = f(m_0)$, then $\beta := 1$	If $v = f(m)$, then $\beta := 1$
Else $\beta := 0$	Else $\beta := 0$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$
Game 2	**Game 3 (SS-RCCA-1)**
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$	$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{S}_1(pk)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$	$m_0 \leftarrow \mathcal{M}$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \mathcal{P}_{m_0}$	$c^* \leftarrow \mathsf{Enc}(pk, m_0)$
$c^* \leftarrow \mathsf{Enc}(pk', m_1)$	$v \leftarrow \mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(c^*, h(m_0), st_1)$
$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$	If $v = f(m)$, then $\beta := 1$
If $v = f(m)$, then $\beta := 1$	Else $\beta := 0$
Else $\beta := 0$	output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	

図 5.1: 定理 5.2.1 で使用されるゲーム列

$\mathcal{S}_1(pk)$	$\mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(h(m_0), st_1)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$	$m_1 \leftarrow \mathcal{P}_{m_0}$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$	$c^* \leftarrow \mathsf{Enc}(pk', m_1)$
$st_1 := (pk, pk', sk', st'_1)$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st'_1)$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1)$	output v

図 5.2: 定理 5.2.1 で使用される $\mathcal{S}$ の構成

$\underline{\mathcal{B}_1^{\mathcal{O}'_1}(pk')}$	$\underline{\mathcal{B}_2^{\mathcal{O}'_2}(c^*, st_1)}$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, st'_1)$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \mathcal{P}_{m_0}$	If $v = f(m_0)$, then $\beta := 1$
$st_1 := (m_0, m_1, \boldsymbol{P}(\cdot,\cdot), \mathcal{M}, st'_1)$	Else $\beta := 0$
output (m_0, m_1, st_1)	$b' \leftarrow \mathcal{D}(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$
	output b

図 5.3: 補題 5.2.2 で使用される $\mathcal{B}$ の構成

め, $\mathcal{A}$ からみて Game 0 と Game 1 は同一のゲームである. よって $\Pr[T_1] = \Pr[T_0]$ が成り立つ. □

補題 5.2.2. $|\Pr[T_2] - \Pr[T_1]| = \mathsf{Adv}^{\mathit{IND\text{-}RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ となるような $\mathcal{B}$ が存在する.

(証明) $\mathcal{A}$ と $\mathcal{D}$ を内部で図 5.3 のように使用する, (pk', sk') の下での IND-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ を考える. $\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は "Test" を受け取る. その後, $\boldsymbol{P}(m_0, m) = 1$ もしくは $\mathcal{B}_2$ が "Test" を受け取った場合, $\mathcal{B}_2$ は $\mathcal{A}_2$ に "Test" を送る. そうでなければ, $\mathcal{B}_2$ は $\mathcal{A}_2$ に m を送る. IND-RCCA-0 において B_2 が 1 を出力するのは, 内部で利用している $\mathcal{A}_2$ が m_0 の暗号文を $\mathcal{B}_2$ から受け取った状況で, $\mathcal{B}_2$ から β を受け取った $\mathcal{D}$ が 1 を出力している場合である. これは Game 1 において $\mathcal{D}$ が 1 を出力する場合と等価である. よって, $\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] = \Pr[T_1]$ が成立する. また, 同様にして $\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] = \Pr[T_2]$ が成立する.

従って,

$$\begin{aligned}|\Pr[T_2] - \Pr[T_1]| &= \left|\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)\end{aligned}$$

が成立する.

□

補題 5.2.3. $\Pr[T_3] = \Pr[T_2]$ が成立する.

(証明) Game 3 において, シミュレータ $\mathcal{S}$ は図 5.2 のように $\mathcal{A}$ を内部で使用する. ここで, Game 3 は SS-RCCA-1 であるので, $\mathcal{S}$ には復号オラクルは与えられていない. しかし, $\mathcal{S}$ は内部で (pk', sk') を生成し, 述語オラクル $\boldsymbol{P}(m_0, \cdot)$ にアクセスすることができる. また, $\mathcal{A}$ には Game 2 のように pk' を入力するため, $\mathcal{A}$ からの復号クエリに対して sk' と $\boldsymbol{P}(m_0, \cdot)$ を用いて正しく返答することができる.

$\mathcal{S}_2$ は内部で生成した m_1 の暗号文を $\mathcal{A}_2$ に入力し, $\mathcal{A}_2$ は v を出力する. $\mathcal{S}_2$ はこの v を出力し, $\mathcal{D}$ に入力される. ここで, $\mathcal{D}$ への入力の分布は Game 2 と Game 3 で同一である. 従って, $\Pr[T_3] = \Pr[T_2]$ が成立する. □

補題 5.2.1 から補題 5.2.3 の結果より,

$$\begin{aligned}\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda) &= \left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{A},h,f}(\lambda)\right)\to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-1}}_{\Pi,\mathcal{A},h,f}(\lambda)\right)\to 1\right]\right| \\ &= |\Pr[T_0] - \Pr[T_3]| \\ &= |\Pr[T_1] - \Pr[T_2]| \\ &= \mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda).\end{aligned}$$

が成立する. よって, 任意の $\mathcal{A}$ に対し図 5.2 に示される $\mathcal{S}$ が存在し, 任意の $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda)$ は無視できる. □

定理 5.2.2. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *IND-RCCA* 安全であり, 平文空間のサイズが多項式よりも大きいと仮定する. このとき, Π は *SS-RCCA* 安全である.

(証明) 任意の IND-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)$ が無視できると仮定する. このとき, 任意の SS-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, 任意の多項式時間関数 h, f に対し, ある PPTA $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し, 任意の PPTA $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda)$ が無視できることを示す. 証明を与える上で, 以下のゲーム列 (Game 0 から Game 4) を使用する.

Game 0 から Game 4 を以下のように定義する:

Game 0: Game 0 は SS-RCCA-0 である.

Game 1: Game 0 との違いは, 公開鍵/秘密鍵の生成 $(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$ を新たに行い, 公開鍵 pk' の下でゲームを行うものとする. $\mathcal{A}_1$ への入力は pk' に変更され, チャレンジ暗号文は pk' を用いて生成される. さらに, $\mathcal{A}$ が使用するオラクル $\mathcal{O}_1$ と $\mathcal{O}_2$ は sk' の下でのオラクルに変更される.

Game 2: Game 1 との違いは, $m_0 \leftarrow \mathcal{M}$ が $m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$ に変更される. また, $\mathcal{O}_2$ が m_1 の暗号文もしくは $\boldsymbol{P}(m_0, m) = 1$ を満たすような暗号文をクエリされた場合に "Test" を返すように変更される.

Game 3: Game 2 との違いは, チャレンジ暗号文 $c^* \leftarrow \mathsf{Enc}(pk', m_0)$ が $c^* \leftarrow \mathsf{Enc}(pk', m_1)$ へと変更される.

Game 4: Game 4 は PPTA $\mathcal{S}$ と pk の下での SS-RCCA-1 であり, $\mathcal{S}$ は内部で $\mathcal{A}$ を図 5.5 のように使用しているものとする.

T_i を Game i で 1 が出力される事象とする.

補題 5.2.4. $\Pr[T_1] = \Pr[T_0]$ が成立する.

Game 0 (SS-RCCA-0)	Game 1
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
	$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$
$m_0 \leftarrow \mathcal{M}$	$m_0 \leftarrow \mathcal{M}$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk', m_0)$
$v \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), st_1)$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
$\mathcal{O}_2 := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk, c)) = 1) \\ \mathsf{Dec}(sk, \cdot) & (\text{otherwise}) \end{cases}$	$\mathcal{O}'_2 := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c)) = 1) \\ \mathsf{Dec}(sk, \cdot) & (\text{otherwise}) \end{cases}$
If $v = f(m_0)$, then $\beta := 1$	If $v = f(m)$, then $\beta := 1$
Else $\beta := 0$	Else $\beta := 0$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$
Game 2	Game 3
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$	$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$	$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$
$c^* \leftarrow \mathsf{Enc}(pk', m_0)$	$c^* \leftarrow \mathsf{Enc}(pk', m_1)$
$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st_1)$
$\mathcal{O}'_2 := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c)) = 1 \\ & \vee \mathsf{Dec}(sk', c) = m_1) \\ \mathsf{Dec}(sk, \cdot) & (\text{otherwise}) \end{cases}$	$\mathcal{O}'_2 := \begin{cases} \mathsf{Test} & (\boldsymbol{P}(m_0, \mathsf{Dec}(sk', c)) = 1 \\ & \vee \mathsf{Dec}(sk', c) = m_1) \\ \mathsf{Dec}(sk, \cdot) & (\text{otherwise}) \end{cases}$
If $v = f(m)$, then $\beta := 1$	If $v = f(m)$, then $\beta := 1$
Else $\beta := 0$	Else $\beta := 0$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$
Game 4 (SS-RCCA-1)	
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st_1) \leftarrow \mathcal{S}_1(pk)$	
$m_0 \leftarrow \mathcal{M}$	
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	
$v \leftarrow \mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(c^*, h(m_0), st_1)$	
If $v = f(m)$, then $\beta := 1$	
Else $\beta := 0$	
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	

図 5.4: 定理 5.2.2 で使用されるゲーム列

$\mathcal{S}_1(pk)$	$\mathcal{S}_2^{\boldsymbol{P}(m_0,\cdot)}(h(m_0), st_1)$
$(pk', sk') \leftarrow \mathsf{Gen}(1^\lambda)$	$m_1 \leftarrow \{0,1\}^\ell$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$	$c^* \leftarrow \mathsf{Enc}(pk', m_1)$
$st_1 := (pk, pk', sk', st'_1)$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), st'_1)$
output $(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1)$	output v

図 5.5: 定理 5.2.2 で使用される $\mathcal{S}$ の構成

$\underline{\mathcal{B}_1^{\mathcal{O}'_1}(pk')}$	$\underline{\mathcal{B}_2^{\mathcal{O}'_2}(c^*, st_1)}$
$(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1) \leftarrow \mathcal{A}_1^{\mathcal{O}'_1}(pk')$	$v \leftarrow \mathcal{A}_2^{\mathcal{O}'_2}(c^*, st'_1)$
$m_0 \leftarrow \mathcal{M}, m_1 \leftarrow \{0,1\}^\ell$	If $v = f(m_0)$, then $\beta := 1$
$st_1 := (m_0, m_1, \mathcal{M}, \boldsymbol{P}(\cdot,\cdot), st'_1)$	Else $\beta := 0$
output (m_0, m_1, st_1)	$b' \leftarrow \mathcal{D}(\mathcal{M}, \beta)$
	output b'

図 5.6: 補題 5.2.6 で使用される $\mathcal{B}$ の構成

(証明) Game 1 は, (pk', sk') の下で SS-RCCA-0 の実験に $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ が追加されているだけであり, $\mathcal{A}$ には $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$ は一切入力されていない. そのため, $\mathcal{A}$ からみて Game 0 と Game 1 は同一のゲームである. よって $\Pr[T_1] = \Pr[T_0]$ が成り立つ. □

補題 5.2.5. $|\Pr[T_2] - \Pr[T_1]| < \frac{poly(\lambda)}{2^\ell}$ が成り立つ.

(証明) Game 2 と Game 3 は $\mathcal{A}_2$ によって m_1 の暗号文が復号オラクルにクエリされなければ等価である. また, m_1 は $\{0,1\}^\ell$ から一様ランダムに選択されている. よって, 差異補題及び Union Bound より $|\Pr[T_3] - \Pr[T_2]| < \frac{poly(\lambda)}{2^\ell}$ が成立する. □

補題 5.2.6. $|\Pr[T_3] - \Pr[T_2]| = \mathsf{Adv}^{IND\text{-}RCCA}_{\Pi,\mathcal{B}}(\lambda)$ を満たすような $\mathcal{B}$ が存在する.

(証明) $\mathcal{A}$ と $\mathcal{D}$ を内部で図 5.6 のように使用する (pk', sk') の下での IND-RCCA′ 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ を考える. $\mathcal{A}_2$ が $\mathcal{B}_2$ に c をクエリした場合, $\mathcal{B}_2$ は自身がアクセスできるオラクルに c を送る. すると, $\mathcal{B}_2$ はオラクルの出力 m 又は "Test" を受け取る. その後, $\boldsymbol{P}(m_0, m) = 1 \vee m = m_1$ もしくは $\mathcal{B}_2$ が "Test" を受け取った場合, $\mathcal{B}_2$ は $\mathcal{A}_2$ に "Test" を送る. そうでなければ, $\mathcal{B}_2$ は $\mathcal{A}_2$ に m を送る.

IND-RCCA-0 において $\mathcal{B}_2$ が 1 を出力するのは, 内部で利用している $\mathcal{A}_2$ が m_0 の暗号文を $\mathcal{B}_2$ から受け取った状況で, $\mathcal{B}_2$ から β を受け取った $\mathcal{D}$ が 1 を出力している場合である. これは Game 2 において $\mathcal{D}$ が 1 を出力する場合と等価である. よって, $\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] = \Pr[T_2]$ が成立する. また, 同様にして, $\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] = \Pr[T_3]$ が成立する.

従って

$$\begin{aligned}|\Pr[T_3] - \Pr[T_2]| &= \left|\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{B}}(\lambda) \to 1\right]\right| \\ &= \mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda)\end{aligned}$$

が成立する. □

補題 5.2.7. $\Pr[T_4] = \Pr[T_3]$ が成立する.

(証明) Game 4 において, シミュレータ $\mathcal{S}$ は図 5.5 のように $\mathcal{A}$ を内部で使用する. ここで, Game 4 は SS-RCCA-1 であるので, $\mathcal{S}$ には復号オラクルは与えられていない. しかし, $\mathcal{S}$ は内部で (pk', sk') を生成し, 述語オラクル $\boldsymbol{P}(m_0, \cdot)$ にアクセスすることができる. また, $\mathcal{A}$ には Game 3 のように pk' を入力するため, $\mathcal{A}$ からの復号クエリに対して sk' と $\boldsymbol{P}(m_0, \cdot)$ を用いて正しく返答することができる.

$\mathcal{S}_2$ は内部で生成した m_1 の暗号文を $\mathcal{A}_2$ に入力し, $\mathcal{A}_2$ は v を出力する. $\mathcal{S}_2$ はこの v を出力し, $\mathcal{D}$ に入力される. ここで, $\mathcal{D}$ への入力の分布は Game 3 と Game 4 で同一である. 従って, $\Pr[T_4] = \Pr[T_3]$ が成立する. □

補題 5.2.4 から補題 5.2.7 の結果より,

$$\begin{aligned}
\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda) &= \left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{A},h,f}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-1}}_{\Pi,\mathcal{A},h}(\lambda)\right) \to 1\right]\right| \\
&= |\Pr[T_0] - \Pr[T_4]| \\
&= |\Pr[T_1] - \Pr[T_3]| \\
&= |\Pr[T_1] - \Pr[T_2] + \Pr[T_2] - \Pr[T_3] \\
&\leq |\Pr[T_1] - \Pr[T_2]| + |\Pr[T_2] - \Pr[T_3]| \\
&\leq \frac{poly(\lambda)}{2^\ell} + \mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{B}}(\lambda).
\end{aligned}$$

が成立する. ここで, 平文空間のサイズが多項式よりも大きいことと, Π が IND-RCCA 安全であることを仮定していたので, 任意の $\mathcal{A}$ に対し図 5.5 に示される $\mathcal{S}$ が存在し, 任意の $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D},h,f}(\lambda)$ は無視できる. □

5.2.2 SS-RCCA⇒ IND-RCCA

定理 5.2.3. 公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が *SS-RCCA* 安全であれば, Π は *IND-RCCA* 安全である.

(証明) $\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}$ を実験がチャレンジビット b をランダムに選択することを表すとする. このとき, 一般性を失うことなく任意の IND-RCCA 攻撃者 $\mathcal{A}$ に対し, $\Pr[\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b] \geq 1/2$ とすることができる. なぜなら, $\Pr[\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b] < 1/2$ ならば, $\mathcal{A}$ の出力を反転させて出力する攻撃者 $\mathcal{A}'$ を考えることができる. すると, $\mathcal{A}'$ と $\mathcal{A}$ の優位性は同じであるが, $\Pr[\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}'}(\lambda) \to b] \geq 1/2$ となる. 従って, $\mathcal{A}'$ の優位性を抑えることができれば, それは同時に $\mathcal{A}$ の優位性を抑えることになる.

任意の SS-RCCA 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ と任意の多項式時間関数 h, f に対し, ある PPTA $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し, 任意の $\mathcal{D}$ に対して $\mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{D},h,f}(\lambda)$ が無視できると仮

Game 0 (IND-RCCA-0)	Game 1 (IND-RCCA-1)
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$	$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$(m_0, m_1, st_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_0)$	$c^* \leftarrow \mathsf{Enc}(pk, m_1)$
$b' \leftarrow \mathcal{A}_2(c^*, st_1)$	$b' \leftarrow \mathcal{A}_2(c^*, st_1)$

図 5.7: 定理 5.2.3 で使用されるゲーム列

$\mathcal{B}_1^{\mathcal{O}_1}(pk)$	$\mathcal{B}_2^{\mathcal{O}_2}(c^*, st_1)$
$(m_0, m_1, st_1') \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$	$b' \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(c^*, st_1')$
$\mathcal{M} := [\{m_0, m_1\}, \Pr(m_0) = \Pr(m_1) = 1/2]$	$v := m_{b'}$
$\boldsymbol{P}'(m, m') := \begin{cases} 1 & (\boldsymbol{P}(m') = 1) \\ 0 & (\text{otherwise}) \end{cases}$	output v
$st_1 := (m_0, m_1, \boldsymbol{P}(\cdot), \boldsymbol{P}'(\cdot,\cdot), st_1')$	
output $(\mathcal{M}, \boldsymbol{P}'(\cdot,\cdot), st_1)$	
$\mathcal{D}(\mathcal{M}, \boldsymbol{P}(\cdot,\cdot), \beta)$	
if $\|\mathcal{M}\| \neq 2$, then output 0	
else if $\boldsymbol{P}(m_1, m_0) = 0 \vee \boldsymbol{P}(m_0, m_1) = 0$, then output 0,	
where $[\{m_0, m_1\}, \Pr(m_0) = \Pr(m_1) = 1/2] = \mathcal{M}$	
else then output β	

図 5.8: 定理 5.2.3 で使用される $\mathcal{B}$ と $\mathcal{D}$ の構成

定する. このとき, 任意の IND-RCCA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ が無視できることを示す.

証明を与える上で, 以下のゲーム列 (Game 0 と Game 1) を使用する.

Game 0 と Game 1 を以下のように定義する:

Game 0: Game 0 は IND-RCCA-0 である.

Game 1: Game 1 は IND-RCCA-1 である.

T_i を Game i で 1 が出力される事象とする.

$h : m \mapsto \epsilon$ における SS-RCCA-0 を考える, ただし ϵ は空文字列である. また, このとき 図 5.8 のように内部で $\mathcal{A}$ を使用する SS-RCCA 攻撃者 $\mathcal{B}$ と $\mathcal{D}$ を構成する. $\mathcal{A}_2$ が $\mathcal{B}_2$ に復号クエリ c を送ってきた場合, $\mathcal{B}_2$ は自身がアクセスできる復号オラクルに c を送る. その後, $\mathcal{B}_2$ は復号オラクルの返答を $\mathcal{A}_2$ に送る.

上記の $\mathcal{B}, \mathcal{D}$ の構成より, $\mathcal{D}$ が 1 を出力するのは, $\mathcal{B}$ 及び $\mathcal{D}$ の内部の $\mathcal{A}$ が試行によって選択される b を正しく推測した場合である. 従って,

$$\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{B},h,f}(\lambda)\right) \to 1\right] = \Pr\left[\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b\right]$$

が成り立つ.

SS-RCCA-1 において, $\mathcal{S}$ が $\|\mathcal{M}\| = 2$ かつ, $\boldsymbol{P}(m, m_0) = 1 \wedge \boldsymbol{P}(m, m_1) = 1$ を満たすような $\mathcal{M}, \boldsymbol{P}$ を出力する事象を E とし, その確率を p とする. ただし,

$[\{m_0, m_1\}, \Pr(m_0) = \Pr(m_1) = 1/2] = \mathcal{M}$ である．SS-RCCA-1 において $\mathcal{S}$ はチャレンジ暗号文を受け取らず, 述語オラクルへのアクセスによって m_0, m_1 の選択に関するいかなる情報も得られない．また, $\|\mathcal{M}\| = 2$ であるので,

$$\begin{aligned}\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-1}}_{\Pi,\mathcal{S},h,f}(\lambda)\right) \to 1\right] &= \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-1}}_{\Pi,\mathcal{S},h,f}(\lambda)\right) \to 1 \middle| E\right] \cdot \Pr[E] \\ &= \frac{p}{2} \\ &\leq \frac{1}{2} \end{aligned} \tag{5.1}$$

となる．

ここで, $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ は

$$\begin{aligned}\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) &= \left|\Pr\left[\mathsf{Exp}^{\text{IND-RCCA-0}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{\text{IND-RCCA-1}}_{\Pi,\mathcal{A}}(\lambda) \to 1\right]\right| \\ &= \left|2 \cdot \Pr\left[\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b\right] - 1\right|\end{aligned}$$

と書き直すことができる．このとき,

$$\begin{aligned}\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) &= \left|2 \cdot \Pr\left[\mathsf{Exp}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda) \to b\right] - 1\right| \\ &= \left|2 \cdot \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{B},h,f}(\lambda)\right) \to 1\right] - 1\right| \\ &\leq \left|2 \cdot \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{B},h}(\lambda)\right) \to 1\right] - 2 \cdot p/2\right| \\ &= 2\left(\left|\Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SS-RCCA-0}}_{\Pi,\mathcal{B},h,f}(\lambda)\right) \to 1\right] - \Pr\left[\mathcal{D}\left(\mathsf{Exp}^{\text{SNM-RCCA-1}}_{\Pi,\mathcal{S},h,f}(\lambda)\right) \to 1\right]\right)\right. \\ &= 2 \cdot \mathsf{Adv}^{\text{SS-RCCA}}_{\Pi,\mathcal{B},\mathcal{D},h,f}(\lambda)\end{aligned}$$

となる, なお式変形には不等式 (5.1) を用いた．よって, 任意の PPTA $\mathcal{A}$ に対して $\mathsf{Adv}^{\text{IND-RCCA}}_{\Pi,\mathcal{A}}(\lambda)$ は無視できる．　□

Chapter 6　結論

本研究では, 公開鍵暗号の平文保持型暗号文変換可能な CCA 環境下 (RCCA) における安全性概念を取り扱った. RCCA 安全性は, 既存の CCA 安全性で取り扱うことができない暗号文の再ランダム化ができる方式を取り扱うことができる他, 認証や鍵交換といった応用を考える上で重要な安全性となっている. RCCA 安全性を提案した Canetti らは, IND-RCCA 安全性, NM-RCCA 安全性, UC-RCCA 安全性という三つの RCCA 環境下における安全性を提案していた. しかし, 彼らの NM-RCCA の定式化は既存の NM-CCA の自然な拡張になっておらず, その妥当性が不明であった. 定式化の妥当性が明らかでない定式化を用いて暗号方式の安全性証明を行った場合, その暗号方式が本当に安全かどうかを判断できない. そのため, 定義の妥当性が明らかでないような安全性モデルの使用は危険である.

そこで, 本研究では上記の問題を解決することを目的とした. RCCA 環境では, 暗号文のリプレイを許容する定式化を行う必要があるため, 単純な NM-CCA の拡張によって RCCA 環境下における頑強性を定式化することはできない. さらに, RCCA 環境下におけるシミュレーションベースの定式化を行う際に, 攻撃者にどのような復号オラクルにアクセスさせるかは非自明であった. そのため, 本稿による RCCA 環境下での頑強性は, Pass らの頑強性の定式化を参考にし, さらに述語を用いることによって定式化した. 具体的には, シミュレーションベースの頑強性及び, 識別不可能性ベースの頑強性の二つの定式化を行い, その等価性を明らかにした. さらに, Canetti らが提案している既存の IND-RCCA と本稿で提案する二つの頑強性の等価性を明らかにした. また, シミュレーションベースの頑強性の定式化を応用し, RCCA 環境下における意味論的安全性の定式化を行い, IND-RCCA との等価性を示した. 結果として, 本稿で定式化した二つの頑強性, 意味論的安全性と既存の IND-RCCA は全て平文空間のサイズに関わらず等価であるという事が明らかになった.

本研究による SNM-RCCA と INM-RCCA は, 従来のシミュレーションベースの頑強性及び, 識別不可能性ベースの頑強性を基にして定式化した. そのため, Canetti らの NM-RCCA よりもより自然な定式化となっている. より自然な定式化を行った SNM-RCCA 及び, INM-RCCA と IND-RCCA が等価であるという関係性から, 我々の定式化は少なくとも Canetti らの頑強性の定式化よりも妥当性が高いといえる. よって, 本研究によって Canetti らの NM-RCCA の定式化が妥当でないことの傍証を与えた.

謝辞

本研究を遂行するにあたり, 日頃から常にご指導を頂きました東京大学生産技術研究所の松浦幹太教授に感謝致します. 松浦先生には研究の進め方だけでなく, 研究に対する姿勢を含む基礎的な部分から教えて頂き, また学会参加, 外部機関との連携など多数の各種活動の機会を与えて頂いたことで, 修士 2 年間を非常に有意義に過ごすことができました.

また, 研究に関して大いに助言, 議論をしていただいた, 新明るい暗号勉強会メンバーである産業技術総合研究所の花岡悟一郎さん, 辛星漢さん, Nuttapong Attrapadung さん, Jacob C. N. Schuldt さん, 松田隆宏さん, 照屋唯紀さん, 村上隆夫さん, 山田翔太さん, 坂井祐介さん, 森田啓さん, 大畑幸矢さん, 石田愛さん, 藤田亮さん, 東京大学の縫田光司さん, 高安敦さん, 勝又秀一さん, 東京工業大学の王宇さん, 北川冬航さん, 品川和雅さん, 原啓祐さん, 東京電機大学の橋本侑知さん, 小松みさきさん, 岡田大弥さん, 大阪大学の矢内直人さん, 北井宏昌さん, 情報通信研究機構の江村恵太さん, 渡邉洋平さん, に深く感謝致します. 特に花岡さん, 坂井さんには研究の内容だけでなく、論文執筆や発表資料作成など細部に渡るまで助言を頂きました。

また, 産業技術総合研究所の高機能暗号研究グループの皆様及び, 事務スタッフの皆さまに感謝いたします. 皆様のおかげで修士課程の研究生活を楽しく過ごすことができました.

松浦研究室打ち合わせでの発表において様々な的確な助言をくださったり, 研究内容に関して議論していただいた Miodrag Mihaljevic さん, 警察庁の田村研輔さん, 角田大輔さんを始めとする, 今まで修士 2 年間の間にお世話になった松浦研究室打ち合わせの参加者の皆様に感謝致します.

そして, 私たちの研究活動が円滑に進むように日頃から尽力してくださっている教授室秘書の小倉華代子さん, 鶴山陽子さん, 仲野小絵さんにも改めて深く感謝致します.

また, 松浦研の技術職員である細井琢朗さん, 松浦研究室メンバーの石坂理人さん, 宮前剛さん, 碓井利宣さん, 長嶺隆寛さん, 黄珂さんにも, 研究室や松浦研究室の打ち合わせにおいて議論をしたり, 様々な助言をいただきました. 皆様のおかげで松浦研究室での 2 年間の生活は素晴らしいものとなりました.

最後に, 常日頃から私を支えてくれた家族に心から感謝します.

参考文献

[1] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. In *Proc. of CRYPTO2005*, LNCS3621, pages 205–222, 2005.

[2] Nuttapong Attrapadung, Yang Cui, David Galindo, Goichiro Hanaoka, Ichiro Hasuo, Hideki Imai, Kanta Matsuura, Peng Yang, and Rui Zhang. Relations Among Notions of Security for Identity Based Encryption Schemes. In *Proc. of LATIN2006*, LNCS3887, pages 130–141, 2006.

[3] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In *Proc. of CRYPTO1998*, LNCS1462, pages 26–45, 1998.

[4] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In *Cryptology ePrint Archive*, 1998/21, 1998. Full version of [3].

[5] Mihir Bellare and Amit Sahai. Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-based Characterization. In *Proc. of CRYPTO1999*, LNCS1666, pages 519–536, 1999.

[6] Mihir Bellare and Amit Sahai. Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-based Characterization. In *Cryptology ePrint Archive*, 2006/228, 2006. Full version of [5].

[7] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In *IEEE Symposium on Security and Privacy (SP '07)*, pages 321–334, 2007.

[8] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible Protocols and Atomic Proxy Cryptography. In *Proc. of EUROCRYPT1998*, LNCS1403, pages 127–144, 1998.

[9] Daniel Bleichenbacher. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1. In *Proc. of CRYPTO1998*, LNCS1462, pages 1–12, 1998.

[10] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public Key Encryption with Keyword Search. In *Proc. of EUROCRYPT2004*, LNCS3027, pages 506–522, 2004.

[11] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *Proc. of CRYPTO2001*, LNCS, pages 213–229, 2001.

[12] Ran Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *Cryptology ePrint Archive*, 2000/67, 2000. Full version of [13].

[13] Ran Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *Proc. of FOCS2001*, pages 136–145, 2001.

[14] Ran Canetti, Hugo Krawczyk, and Jesper Nielsen. Relaxing Chosen-Ciphertext Security. In *Cryptology ePrint Archive*, 2003/174, 2003. Full version of [15].

[15] Ran Canetti, Hugo Krawczyk, and Jesper Buus Nielsen. Relaxing Chosen-Ciphertext Security. In *Proc. of CRYPTO2003*, LNCS2729, pages 565–582, 2003.

[16] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Malleable Proof Systems and Applications. In *Proc. of EUROCRYPT2012*, LNCS7237, pages 281–300, 2012.

[17] Yuan Chen and Qingkuan Dong. RCCA Security for KEM+DEM Style Hybrid Encryptions. In *Proc. of Inscrypt2012*, LNCS7763, pages 102–121, 2012.

[18] Yuan Chen and Qingkuan Dong. RCCA security for KEM+DEM style hybrid encryptions and a general hybrid paradigm from RCCA-secure KEMs to CCA-secure encryptions. *Security and Communication Networks*, 7(8):1219–1231, 2014.

[19] Yuan Chen, Qingkuan Dong, and Qiqi Lai. Natural sd-RCCA Secure Public-Key Encryptions. In *Proc. of ProvSec2017*, LNCS10592, pages 236–250, 2017.

[20] Ronald Cramer and Victor Shoup. A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. In *Proc. of CRYPTO1998*, LNCS1462, pages 13–25, 1998.

[21] Dana Dachman-Soled, Georg Fuchsbauer, Payman Mohassel, and Adam O'Neill. Enhanced Chosen-Ciphertext Security and Applications. In *Proc. of PKC2014*, LNCS8383, pages 329–344, 2014.

[22] Honglong Dai, Jinying Chang, Zhenduo Hou, and Maozhi Xu. Relaxing Enhanced Chosen-Ciphertext Security. *IEICE Transactions*, 101-A(12):2454–2463, 2018.

[23] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[24] Danny Dolev, Cynthia Dwork, and Moni—Naor. Non-Malleable Cryptography (Extended Abstract). In *Proc. of STOC1991*, pages 542–552, 1991.

[25] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA-OAEP Is Secure under the RSA Assumption. In *Proc. of CRYPTO2001*, LNCS2139, pages 260–274, 2001.

[26] David Galindo and Ichiro Hasuo. Security Notions for Identity Based Encryption. In *Cryptology ePrint Archive*, 2005/253, 2005.

[27] Taher El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discret Logarithms. In *Proc. of CRYPTO1984*, LNCS196, pages 10–18, 1984.

[28] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In *Proc. of STOC1982*, pages 365–377, 1982.

[29] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[30] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of ACM CCS2006*, pages 89–98, 2006.

[31] Jens Groth. Rerandomizable and Replayable Adaptive Chosen Ciphertext Attack Secure Cryptosystems. In *Proc. of TCC2004*, LNCS2951, pages 152–170, 2004.

[32] Goichiro Hanaoka, Yutaka Kawai, Noboru Kunihiro, Takahiro Matsuda, Jian Weng, Rui Zhang, and Yunlei Zhao. Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption. In *Proc. of CT-RSA2012*, LNCS7178, pages 349–364, 2012.

[33] Yusuke Kawamoto, Hideki Sakurada, and Masami Hagiya. Computationally Sound Formalization of Rerandomizable RCCA Secure Encryption. In *Proc. of Formal to Practical Security2009*, LNCS5458, pages 158–180, 2009.

[34] Keying Li, Jianfeng Wang, Yinghui Zhang, and Hua Ma. Key Policy Attribute-based Proxy Re-encryption and RCCA Secure Scheme. *J. Internet Serv. Inf. Secur.*, 4(2):70–82, 2014.

[35] Benoît Libert, Thomas Peters, and Chen Qian. Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts. In *Proc. of Public Key Cryptography (1) 2017*, LNCS10174, pages 247–276, 2017.

[36] Benoît Libert and Damien Vergnaud. Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption. In *Proc. of PKC2008*, LNCS4939, pages 360–379, 2008.

[37] Rongxing Lu, Xiaodong Lin, Jun Shao, and Kaitai Liang. RCCA-Secure Multi-use Bidirectional Proxy Re-encryption with Master Secret Security. In *Proc. of ProvSec2014*, LNCS8782, pages 194–205, 2014.

[38] Phillip Rogaway Mihir Bellare. Optimal Asymmetric Encryption. In *Proc. of EUROCRYPT1994*, LNCS950, pages 92–111, 1994.

[39] Moni Naor and Moti Yung. Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. In *Proc. of STOC1990*, pages 427–437, 1990.

[40] Sumit Kumar Pandey, Santanu Sarkar, and Mahabir Prasad Jhanwar. Relaxing IND-CCA: Indistinguishability against Chosen Ciphertext Verification Attack. In *Security, Privacy, and Applied Cryptography Engineering*, pages 63–76, 2012.

[41] Rafael Pass, abhi shelat, and Vinod Vaikuntanathan. Relations Among Notions of Non-malleability for Encryption. In *Proc. of ASIACRYPT2007*, LNCS4833, pages 519–535, 2007.

[42] Manoj Prabhakaran and Mike Rosulek. Rerandomizable RCCA Encryption. In *Proc. of CRYPTO2007*, LNCS4622, pages 517–534, 2007.

[43] Manoj Prabhakaran and Mike Rosulek. Rerandomizable RCCA Encryption. In *Cryptology ePrint Archive*, 2007/119, 2007. Full version of [42].

[44] Michael O. Rabin. Digitalized Signatures and Public-key Functions as Intractable as Factorization. In *Massachusetts Institute of Technology*, 1979.

[45] Charles Rackoff and Daniel R. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In *Proc. of CRYPTO1991*, LNCS576, pages 433–444, 1991.

[46] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[47] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Proc. of CRYPTO1984*, LNCS196, pages 47–53, 1984.

[48] Yodai Watanabe, Junji Shikata, and Hideki Imai. Equivalence between Semantic Security and Indistinguishability against Chosen Ciphertext Attacks. In *Proc. of PKC2003*, LNCS2567, pages 71–84, 2003.

[49] 小松みさき, 山田翔太, 坂井祐介, 花岡悟一郎. ID ベース暗号の強秘匿匿名性について. In *2018* 年 コンピュータセキュリティシンポジウム *3A3-4*, 2018.

[50] 大友萌夢, 佐々木太良, 藤岡淳. ID ベース暗号における匿名性定義の関係性. In *2017* 年 暗号と情報セキュリティシンポジウム *2F2-3*, 2017.

[51] 大友萌夢, 佐々木太良, 藤岡淳. ID ベース暗号の匿名性定義の関係 〜CCA2 の場合〜. In *2018* 年 暗号と情報セキュリティシンポジウム *1A1-1*, 2018.

発表文献

国際会議

i Junichiro Hayata, Masahito Ishizaka, Yusuke Sakai, Goichiro Hanaoka, Kanta Matsuura. Generic Construction of Adaptively Secure Anonymous Key-Policy Attribute-Based Encryption from Public-Key Searchable Encryption, Proceeding of the 2018 International Symposium on Information Theory and its Applications (ISITA2018), pp.739-743, 2018.

国内会議

ii 林田淳一郎, 石坂理人, 坂井祐介, 花岡悟一郎, 松浦幹太. 公開鍵型検索可能暗号を用いた適応的安全な匿名鍵ポリシー型属性ベース暗号の一般的構成, Generic Construction of Adaptively Secure Anonymous Key-Policy Attribute-Based Encryption from Public-Key Searchable Encryption, 2018 年　暗号と情報セキュリティシンポジウム (SCIS2018）予稿集, 2018.

iii 林田淳一郎, 北川冬航, 坂井祐介, 花岡悟一郎, 松浦幹太. 公開鍵暗号の Replayable CCA 環境下での安全性概念間の等価性について, Relations among Notions of Security under Replayable CCA Environment for Public-Key Encryption, 2019 年　暗号と情報セキュリティシンポジウム (SCIS2019）予稿集, 2019.