修士論文

Rényi Divergence を用いた格子暗号の分散復号方式

沼畑 祥平

主指導教員 藤崎英一郎

北陸先端科学技術大学院大学
先端科学技術専攻
（情報科学）

令和 7 年 3 月

Abstract

This thesis has constructed a threshold public key encryption (ThPKE) scheme based on Regev's lattice cryptosystem[Reg05] utilizing the technique of Boudgoust and Scholl[BS23].

Many quantum algorithms threaten the security and privacy of current (classical) encryption system[Sho94],[Gro96]. Therefore, we must develop alternative schemes with quantum resilience. The lattice cryptosystem is attracting attention as a prominent candidate for post-quantum cryptography due to its hardness and its applicatons.In fact, The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) released draft standards for three lattice-based cryptographic schemes for post-quantum cryptography in 2024[NIS24b]. The Regev cryptosystem discussed in this thesis serves as a prototype for one of them.

The conscept of threshold secret sharing was independently proposed by Shamir[Sha79] and Blakley[Bla99]. In threshold schemes, the secret key is distributed among multiple parties using a secret sharing method. Even if some of these parties (up to a predefined threshod) are corrupted, the secrecy of the key is maintained, even during partial decryption that rely on it. This approach not only enhances security by distributing trust but also elliminates the critical problem of "single point of failure" in public key encryption (PKE) systems. NIST is advancing a project to develop future recommendations and guidelines for threshold cryptosystems[NIS24a].

In ThPKE, the technique of "noise flooding" is typically used to prevent the leakage of information about the secret key during partial decryption. In the early stages, the security provided by noise flooding was measured using statistical distance[BD10],[BGG$^+$18], which resulted in overhead in ciphertext and noise sizes, leading to a deteroration of the LWE parameters and reduced efficiency. In contrast, Boudgoust and Scholl's technique improves the parameters by using the Rényi Divergence. However, Rényi Divergence does not align decisional security notions such as IND-CPA. Therefore, we realize IND-CPA by transfomating from OW-CPA. In this transformation, we use the random oracle model. However, Random oracle model makes a strong assumption about the existence of ideal hash funtion. As future concern, we aim to cunstruct a transfomation in the standard model.

By combining Regev's cryptosystem with a threshold cryptosystem, our scheme achives quantum resitance while enabling trust distribution with improved efficiency. Lastly, We campare various (t, N) linear secret sharing schemes, highlighting potential parameter optimizations and their impact on overall performance.

目 次

図 目 次

第1章　はじめに

本研究では，Regev[Reg05] によって提案された公開鍵暗号方式を，Boudgoust, Scholl[BS23] によって提案された技法によって閾値型暗号方式を構成する．[BS23] では，完全準同型暗号に対して Rényi Divergence を導入し，ノイズ評価を改善したが，その方式を通常の公開鍵暗号に適用した．

格子問題　量子計算機の台頭により，素因数分解や離散対数問題の解読困難性に安全性の根拠をおく従来の暗号やプロトコルが安全ではなくなる [Sho94],[Gro96]．一方，格子問題を解く効率的量子アルゴリズムが見つかっていないことから，耐量子計算機安全な暗号として格子暗号が候補として注目されている．また，Rivest らが提案し [RD78], Gentry によって実現された [Gen09]，完全準同型暗号（暗号化した状態で加算・乗算が可能）などの高機能暗合への応用も数多く考案されている．実際，米国商務省標準化技術研究所（NIST）が耐量子暗号の標準化としてあげた [NIS24b],[NIS22]ML-KEM(旧 CRYSTALS-KYBER)，ML-DAS(旧 CRYSTALS-Dilithium)，FN-DAS(旧 FALCON) といった方式は，格子問題を基に構成されている．中でも，CRYSTAL-KYBER は，本研究で扱う Regev 暗合 [?] がプロトタイプとなっており，閾値型公開鍵暗号方式に同様の手法で拡張可能である．

Regev 暗合は，格子問題と同程度の困難性を持つ，LWE 問題の計算量困難性に安全性の理由を置く公開鍵暗号方式（PKE）である．

閾値公開鍵暗号　(t, N) 閾値値秘密分散方式は, Shamir[Sha79] および Blakley[Bla99] によって独立に提案された．この方式では，秘密 x を保持するディーラーが，N 人の参加者にシェアと呼ばれる秘密を分割したものを分配し，$t+1$ 人以上の参加者が集まれば秘密を復元できる（閾値型アクセス構造）．一方，t 人以下では秘密について何も知ることができない．つまり，閾値以下の参加者が不正・破損した場合でも，秘密が漏れることはない．Ito, Saito, Hishizeki[ISN89] らによって提案された複製秘密分散方式では，(t, N) 秘密分散方式のシェアを各参加者に複数個分配することで，より一般的なアクセス構造の実現が可能である．これらの方式は，情報理論的安全性を満たす．つまり，攻撃者が無限の計算能力を持っていようとも，条件（アクセス構造）を満たさない部分情報からは，秘密が漏れることはない．

秘密分散方式では，攻撃者の振る舞いに関し，二分することができる．一つ目が，受動的攻撃者で，プロトコルから逸脱しない範囲で，他の参加者の情報を盗み見ようとする．二つ目が，能動的攻撃者で，プロトコルから逸脱し，他の参加者の情報を盗む，データの改ざんといったことをする．本研究では，受動的攻撃者を仮定する．

本研究では，[BS23] で提案された閾値秘密分散方式の構成方法を，格子問題に安全性の根拠をおく公開鍵暗号方式（PKE）である Regev 暗合と，(t, N) 閾値秘密分散に適用し，いくつかの秘密分散方式によってそれらを評価する．Regev 暗合を拡張した Peikert, Vaikuntanathan, Waters らの暗号方式 [?] に対して，この変換を利用することも可能だが，本論では簡潔さを優先して Regev 暗合を使用する．

公開鍵暗号方式（PKE）では，秘密鍵を一人の参加者が管理する．従って，その参加者が何らかの理由で復号の失敗した場合や，不正した場合，システム全体が危険にさらされる可能性がある．このような単一障害点 (single point of failure) を避けるため，閾値公開鍵暗号（ThPKE）では，秘密鍵を秘密分散し，複数の参加者で管理する．参加者は各自で部分復号を計算し，復号者に送信する．復号者は閾値（閾値アクセス構造を満たす）を超える参加者のシェアを受け取ることで，秘密鍵を復元することなく，元のメッセージを復元できる．このような方式を閾値公開鍵暗号方式（Threshold Public Key Encryption, ThPKE）という．

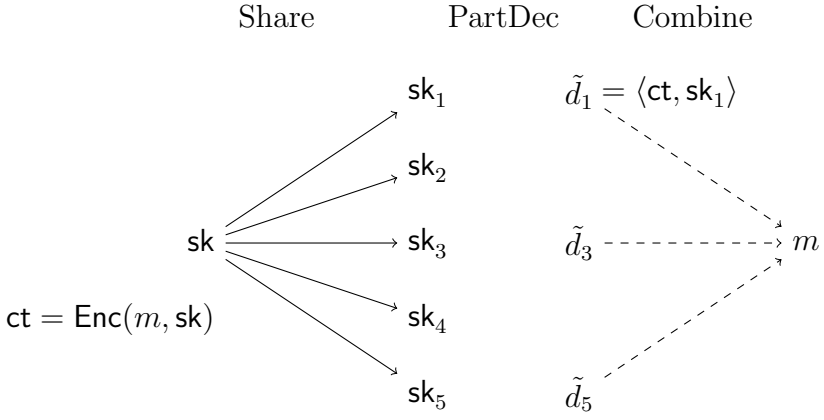


図 1.1: $(2, 5)$ThPKE の例 (Noise less PartDec)

Noise Flooding　Noise flooding は，秘密分散で部分復号を計算した際，秘密鍵に関する情報を漏らさないようにする技術である．Noise flooding を使わない場合，復号は，

$$\mathsf{Rec}(\{\mathbf{d}_i\}_{i\in S}) = \mathsf{Rec}(\{\langle \mathsf{ct}, \mathsf{sk}_i \rangle\}_i) = \langle \mathsf{ct}, \mathsf{sk} \rangle = \lfloor q/p \rceil \cdot m + e_{\mathsf{ct}}$$

のように行われ, 暗号文と秘密鍵に依存した復号ノイズ e_{ct} を漏らしてしまう．Noise flooding では, この漏洩を防ぐため, 各参加者は自身の部分復号に新たなノイズ e_{flood} を追加する．すなわち，$\mathbf{d}_i = \langle \mathsf{ct}, \mathsf{sk}_i \rangle + e_{\mathsf{flood}}$ となるので，復号は

$$\begin{aligned}\mathsf{Rec}(\{\mathbf{d}_i\}_{i\in S}) &= \mathsf{Rec}(\{\langle \mathsf{ct}, \mathsf{sk}_i \rangle\}_i + e_{\mathsf{flood},i}) \\ &= \langle \mathsf{ct}, \mathsf{sk} \rangle + \mathsf{Rec}(\{e_{\mathsf{flood},i}\}_i) \\ &= \lfloor q/p \rceil \cdot m + e_{\mathsf{ct}} + \mathsf{Rec}(\{e_{\mathsf{flood},i}\}_i)\end{aligned}$$

となる．ゲーム変換による安全性証明では，$e_{\mathsf{ct}} + e_{\mathsf{flood}}$ をシミュレートしたノイズ e_{sim} に置き換える．従来の閾値分散方式 [BD10][BGG+18] では，実際のノイズ

とシミュレートしたノイズの近さを統計距離で測っていたが，[BS23] では，Rényi Divergence を用いることで，セキュリティパラメータの改善をした．

Rényi Divergence　統計距離では，確率分布 P, Q ，事象 E に対し，確率保存則によって，

$$P(E) \leq \Delta(P, Q) + Q(E)$$

が成り立つ．したがって，$Q(E)$ が無視でき (2.1)，かつ $\Delta(P, Q)$ が無視できるならば，$P(E)$ は無視できる．一方，RD では ，

$$P(E)^{\frac{a}{a-1}} \leq \mathsf{RD}(P\|Q) \cdot Q(E)$$

が成り立つ．したがって，$Q(E)$ が無視でき，かつ $\mathsf{RD}(P\|Q)$ が定数ならば，$P(E)$ は無視できる．つまり，先程のノイズ評価において，統計距離を使った場合，

$$\Delta(e_{\mathsf{flood}} + e_{\mathsf{ct}}, e_{\mathsf{sim}}) \leq \mathsf{negl}(\lambda) \tag{1.1}$$

RD を使った場合，

$$\mathsf{RD}(e_{\mathsf{flood}} + e_{\mathsf{ct}}\|e_{\mathsf{sim}}) \leq \mathsf{constant} \tag{1.2}$$

となれば，ゲーム間の優位性が攻撃者に識別できない，つまり，安全性が証明されたことになる．[BLRL+15] では，それぞれの場合に必要なセキュリティパラメータに関する評価を行っている．

式 (1.1) を実現するためには，flooding noise e_{flood} を，復号ノイズ e_{ct} よりも十分に大きくとる必要がある．具体的には，サイズ比 $\frac{\|e_{\mathsf{flood}}\|}{\|e_{\mathsf{ct}}\|}$ がセキュリティパラメータに対し，超多項式 (2.2) であることが要求される．しかし，LWE 問題に基づく暗号では，復号を正しく行うためには，ノイズが一定の範囲に収まる必要がある（法 q の数分の一程度に設定する）．しかし，法を大きくすると，格子基底削減アルゴリズム（BKZ）[SE94],[敦剛 19] などの，LWE 問題を効率的に解くアルゴリズムが存在するため，安全性を損なう．一方，式 (1.2) では，RD が定数で抑えられればよく，サイズ比 $\frac{\|e_{\mathsf{flood}}\|}{\|e_{\mathsf{ct}}\|}$ が，多項式 (2.2) であればよい．したがって，法を抑えることができる．さらに，[Reg05, Theorem 1.1] より，法対ノイズ比が，超多項式の場合より，多項式の場合，LWE 問題が困難である．

安全性の定式化　Rényi Divergence は，OW-CPA などの，探索問題には適しているが，IND-CPA などの，決定問題には適していない．なぜなら，IND-CPA では，攻撃者が勝利する確率は 1/2 と高確率であるため，確率保存則によって十分に制限することができない．したがって，OW-CPA を構成してから，IND-CPA へランダムオラクルを使った変換をする手法をとる．

1.1 関連研究

RSA 暗号や ElGamal 暗号等の古典暗号に対する閾値分散方式は多くの研究がある [Des87],[DF89]．Bendlin, Damgård は，格子暗号ベースの ThPKE を初めて構成した [BD10]．彼らは，ゼロ知識証明を組み込むことによって，安全性を重視した．一方，Boudgoust, Scholl は，Bendlin らの方式における，統計距離に基づく noise flooding 評価を Rényi Divergence に置き換えることで，効率を改善した [BS23]．

格子暗号ベースの PKE として，本研究では Regev 暗合 [Reg05] を用いたが，Peikert, Vaikuntanathan, Waters による Regev 暗合の改良版 [PVW08] によって，より平文空間を大きくとることができる．また, CRYSTALS-KYBER[NIS22] によって，より効率，安全性を向上させることができる．

第2章　記法

[BS23] の記法に従う.

2.1　基本的な記法

任意の整数 q に対し，$\mathbb{Z}_q$ で q を法とする整数を表す．任意の整数 N に対し，$[N]$ で集合 $\{1,\ldots,N\}$ を表す．ベクトルを小文字の太文字，行列を大文字の太文字で表す．任意の集合 X に対し，2^X で X の冪集合を表す.

多項式時間　関数 $f\colon \mathbb{N}\to\mathbb{R}^+$ が多項式時間であるとは,

$$\exists c>0, \exists n_0\in\mathbb{R}^+, \forall n\geq n_0 \Rightarrow f(n)\leq n^c \tag{2.1}$$

が成り立つことを言う．これを，$f(n)=\mathcal{O}(\mathrm{poly}(n))$ と表す.

超多項式時間　関数 $f\colon \mathbb{N}\to\mathbb{R}^+$ が超多項式時間であるとは,

$$\forall c>0, \exists n_0\in\mathbb{R}^+, \forall n\geq n_0 \Rightarrow \forall k\in\mathbb{R}^+, 0\leq cn^k<f(n) \tag{2.2}$$

が成り立つことを言う．これを，$f(n)=\omega(n^k)$ と表す.

PPT で確率的多項式時間を表す．PPT 攻撃者 $\mathcal{A}$ が複数のアルゴリズム $(\mathcal{A}_i)_i$ から成るとき，$\mathcal{A}_i$ の出力は，$\mathcal{A}_{i+1}$ に渡されるとする.

無視できる関数　関数 $\epsilon\colon \mathbb{N}\to\mathbb{R}^+$ が無視できるとは，ϵ がいかなる多項式の逆数より早く 0 に収束することを言う:

$$\forall c>0, \exists n_0\in\mathbb{N}, n\geq n_0 \Rightarrow \epsilon(n)\leq n^{-c}$$

言い換えると，$\mathsf{negl}(\lambda)=\lambda^{-\omega(1)}$ [1]が成り立つとき，$\epsilon(n)$ は無視できるという.

ランダムオラクル　OW-CPA から IND-CPA の変換の際, ランダムオラクル（ROM）を使用する．このとき, 理想的ハッシュ関数の存在を仮定する．すなわち, ランダムオラクル $\mathsf{F}\colon \{0,1\}^n\to\{0,1\}^m$ に対し, $\Pr[\mathsf{F}(x)=y]=2^{-m}$ かつ $\Pr\left[\mathsf{F}(x)=\mathsf{F}(x')=y \mid x\neq x'\right]=\Pr[\mathsf{F}(x)=y]\cdot\Pr\left[\mathsf{F}(x')=y\right]=2^{-2m}$ を満たす．つまり，ランダムオラクルには衝突困難性がある.

[1] $f=\omega(n)$ iff $\lim_{n\to\infty}\frac{f(n)}{g(n)}=+\infty$

2.2 確率とエントロピー

集合 S に対し，濃度を $|S|$ で表す．S 上の一様分布を $U(S)$ で表す．確率分布 D から $x \in S$ をサンプルすることを，$x \leftarrow D$ で表す．

定義 1 (ガウス分布)**.** $\mathbb{R}$ 上の確率密度関数

$$\rho_{\sigma,c}(x) = \frac{1}{\sqrt{2\pi}\sigma} \cdot \exp\left(-\frac{(x-c)^2}{2\sigma^2}\right)$$

によって定義された分布を，平均 c，分散 σ^2 のガウス分布といい，$N(c, \sigma^2)$ で表す．$c = 0$ のとき，簡略化して，ρ_σ と表す．

定義 2 (離散ガウス分布)**.** 集合 $S \subseteq \mathbb{R}$ に対し，$\rho_{\sigma,c}(S) \coloneqq \sum_{x \in S} \rho_{\sigma,c}(x)$ とする．確率密度関数

$$\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(S)}$$

によって定義された分布を，S 上の平均 c，分散 σ^2 の離散ガウス分布と呼び，$D_{S,\sigma,c}$ で表す．

注釈 3. $s > 0, x \in \mathbb{R}$ ，$\rho_s(x) = \frac{1}{s}\exp\left(-\pi(\frac{x}{s})^2\right)$ とする．このとき，$x \in \mathbb{Z}$ に対し，確率密度関数

$$\tilde{\rho}_s(x) \coloneqq \rho_s(x)/\rho_s(\mathbb{Z})$$

によって定義された分布を $\mathbb{Z}$ 上の離散確率分布といい，$D_{\mathbb{Z},s}$ で表す．

また，$\rho_s(x)$ で作られる分布は，$s = \sqrt{2\pi}\sigma$ とすると，ガウス分布 $N(0, \frac{s^2}{2\pi})$ である．

定理 4 (Gaussian Tail Bound)**.** $s > 0, x \in \mathbb{R}$ とする．確率密度関数 $\rho_s(x)$ によって定義される分布に従う確立変数を X とすると，$t > 0$ のとき，

$$\Pr\left[|X| > t\right] \leq 2e^{-\pi(\frac{t}{s})^2}$$

が成り立つ．

定義 5 (δ-subgaussian)**.** $\delta \geq 0$ とする．$c = \mathbb{E}[X]$ のとき，任意の $\lambda > 0$ に対して，ある $s > 0$ が存在して

$$\mathbb{E}\left[e^{\lambda(X-c)}\right] \leq \exp(\delta) \cdot \exp\left(\frac{\lambda^2 s^2}{4\pi}\right)$$

を満たすとき，X の従う分布を *δ-subgaussian* という．

定理 6. X の従う分布が *δ-subgaussian* であれば，*δ-subgaussian Tail Bound*

$$\Pr\left[|X - c| \geq t\right] \leq 2\exp(\delta) \cdot \exp\left(-\pi t^2/s^2\right)$$

が得られる．

定理 7. 確率変数 $X_1, \ldots, X_m$ が独立で，$\mathbb{E}[X_1] = \cdots = \mathbb{E}[X_m] = 0$ かつ，従う分布が同じ s をもつ *δ-subgaussian* とする．そのとき，確率変数 $Z \coloneqq \sum X_i$ は，

$$\Pr\left[|Z| \geq t\sqrt{m}\right] \leq 2\exp(m \cdot \delta) \cdot \exp\left(-\pi t^2/s^2\right)$$

となる．

定義 8 (Shannon エントロピー)**.** X を確率分布とする．このとき，x の *shannon* エントロピーを

$$\begin{aligned}\mathrm{H}_1(X) &= -\sum_x \Pr[x] \cdot \log(\Pr[x]) \\ &= -\mathbb{E}_{x \leftarrow X}[\log(\Pr[x])]\end{aligned}$$

で定義する．

定義 9 (Collision エントロピー)**.** X を確率分布とする．このとき，x の *collision* エントロピーを

$$\begin{aligned}\mathrm{H}_2(X) &= -\log\left(\Pr\left[x \leftarrow X; x' \leftarrow X : x = x'\right]\right) \\ &= \log\left(\sum_x \Pr[x]^2\right) \\ &= -\log \mathbb{E}_{x \leftarrow X}[\Pr[x]]\end{aligned}$$

で定義する．

定義 10 (最小エントロピー)**.** X を確率分布とする．このとき，x の最小エントロピーを

$$\mathrm{H}_\infty(X) = -\log\left(\max_x \Pr\left[X = x\right]\right)$$

で定義する．

注釈 11.

$$\mathrm{H}_1(X) \geq \mathrm{H}_2(X) \geq \mathrm{H}_\infty(X) \Rightarrow 2^{-\mathrm{H}_1(X)} \leq 2^{-\mathrm{H}_2(X)} \geq 2^{-\mathrm{H}_\infty(X)}$$

が常に成り立つ．

例 1. 最小エントロピーが低いとき，X の中である特定の値が非常に高い確率で発生することを意味する．

$$\begin{aligned}(-\log_2 1/4) &= (-\log_2 2^{-2}) = 2 \\ (-\log_2 1/8) &= (-\log_2 2^{-3}) = 3\end{aligned}$$

平均条件付き最小エントロピーは [DORS08] の定義を参考．

定義 12 (平均条件付き最小エントロピー). X, Z を確率分布とする．Z が与えられたときの x の平均条件付き最小エントロピーを

$$\begin{aligned}\tilde{\mathrm{H}}_\infty(X \mid Z) &= -\log_2(\mathbb{E}_{z\leftarrow Z}\left[\max_{x\in X}\Pr\left[X=x \mid Z=z\right]\right]) \\ &= -\log\left(\mathbb{E}_{z\leftarrow Z}\left[2^{-\mathrm{H}_\infty(X\mid Z=z)}\right]\right)\end{aligned}$$

で定義する．

定義 13 (統計距離). X, Y を集合 S 上の確率分布とする．このとき，統計距離を

$$\Delta(X,Y) \coloneqq \frac{1}{2}\sum_{a\in S}|\Pr_X[X=a]-\Pr_Y[Y=a]|$$

で定義する．

定義 14 (Universal Hash). 有限集合 $\mathcal{X}, \mathcal{Y}$ $(|\mathcal{X}| \coloneqq N \geq |\mathcal{Y}| \coloneqq M)$ に対して，ハッシュ関数の族 $\mathcal{H} \coloneqq \{h : \mathcal{X} \to \mathcal{Y}\}$ を考える．$\mathcal{H}$ が

$$\forall x_1, x_2 \in \mathcal{X} \quad \wedge \quad x_1 \neq x_2 \Rightarrow \Pr_{h\leftarrow U(\mathcal{H})}[h(x_1)=h(x_2)] \leq \frac{1}{M}$$

を満たすとき，$\mathcal{H}$ は *universal hash* であるという．

以下の補題 (15) は，偏りのある大きな集合 $\mathcal{X}$ 上のある分布に従う確率変数 X を，universal hash の出力 $h(X)$ にすることで，小さな集合 $\mathcal{Y}$ 上のほぼ一様な分布に従う確率変数に変換できる．

補題 15 (Leftover Hash Lemma). $\mathcal{X}, \mathcal{Y}$ $(|\mathcal{X}| \coloneqq N \geq |\mathcal{Y}| \coloneqq M)$ を *universal hash* とする．X を $\mathcal{X}$ 上のある分布に従う確率変数，$U(\mathcal{Y})$ を $\mathcal{Y}$ 上の一様分布に従う確率変数で，h を $\mathcal{H}$ 上の一様分布に従う確率変数とみると，

$$\Delta\Big((h,h(X)),(h,U(\mathcal{Y}))\Big) \leq \frac{1}{2}\sqrt{M\cdot \mathsf{CP}(X)}$$

が成り立つ．ここで，

$$\mathsf{CP}(X) \coloneqq Pr[x_1 \leftarrow X; x_2 \leftarrow X : x_1 = x_2] = \sum_{x\in\mathcal{X}} Pr[X=x]^2$$

は衝突確率である．エントロピーの定義より，

$$\mathsf{CP}(X) = 2^{-\mathsf{H}_2(X)} \leq 2^{-\mathsf{H}_\infty(X)}$$

$m \coloneqq \lceil \log_2 M \rceil$ とおくと，

$$\Delta\Big((h,h(X)),(h,U(\mathcal{Y}))\Big) \leq 2^{-(\frac{\mathsf{H}_2(X)-m}{2}+1)} \leq 2^{-(\frac{\mathsf{H}_\infty(X)-m}{2}+1)}$$

となる．

証明. $U(S)$ を S 上の一様分布に従う確率変数とすると，

$$\mathsf{CP}(U(S)) = \sum_{a \in S} \Pr[U(S) = a]^2 = \frac{1}{|S|}$$

有限集合上の確率分布を考えればよいので，有限集合 S 上の確率変数 V を

$$\mathbf{v} = (v_1, \ldots, v_n) \quad where \quad v_i \coloneqq \Pr[V = i \in S]$$

と同一視する．

任意のベクトル $\mathbf{v} \in \mathbb{R}^n$ に対しての ℓ_1, ℓ_2 ノルムを

$$\|\mathbf{v}\|_1 \coloneqq \sum |v_i|, \|\mathbf{v}\|_2 \coloneqq \sqrt{\sum (v_i)^2}$$

とする．Cauchy-Schwarz の不等式より，

$$\|\mathbf{v}\|_1 = \langle \mathbf{v}, \mathbf{v}^{'} \rangle \leq \|\mathbf{v}_2\| \|\mathbf{v}^{'}\|_2 \leq \sqrt{|S| \cdot \|\mathbf{v}\|_2}$$

ここで，$\mathbf{v}^{'} \coloneqq (v_1^{'}, \ldots, v_n^{'})$ かつ $v_i^{'} \coloneqq \frac{v_i}{|v_i|}$ とする．($v_i v_i^{'} = v_i \cdot \frac{v_i}{|v_i|}$ ここで，右辺は v_i の符号なので，± 1 となる．したがって，$v_i v_i^{'} = |v_i|$ となる．)

有限集合 S 上の確率変数 X, Y の統計距離は，

$$\Delta(X, Y) \coloneqq \frac{1}{2} \sum_{a \in S} |Pr[X = a] - Pr[Y = a]$$

であるので，$\mathbf{v} = (v_1, \ldots, v_n)$ で $v_a \coloneqq (\Pr[X = a] - \Pr[Y = a])$ とおくと，

$$\Delta(X, Y) = \frac{1}{2} \|\mathbf{v}\|_1 \leq \frac{\sqrt{|S|}}{2} \|\mathbf{v}\|_2$$

$X, \mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}, U(\mathcal{Y})$ を universal hash（定義 (14)）とする．$D \coloneqq |\mathcal{H}|$ とする．

$$v_{h^{'}, y} \coloneqq \Pr\Big[(h, h(X)) = (h^{'}, y)\Big] - \Pr\Big[(h, U(\mathcal{Y})) = (h^{'}, y)\Big] \quad where \quad (h^{'}, y) \in \mathcal{H} \times \mathcal{Y}$$

と定義すると，

$$\Delta\Big((h, h(X)), (h, U(\mathcal{Y}))\Big) = \frac{1}{2} \|\mathbf{v}\|_1 \leq \frac{\sqrt{DM}}{2} \|\mathbf{v}\|_2$$

が成り立つ．

また，

$$\begin{aligned}
\|\mathbf{v}\|_2 &= \sum_{h',y} v_{h',y}^2 \\
&= \sum_{h',y} \Big(\Pr\Big[(h,h(X)) = (h',y)\Big] - \Pr\Big[(h,U((\mathcal{Y}) = (h',y)\Big] \Big)^2 \\
&= \sum_{h',y} \Big(\Pr\Big[(h,h(X)) = (h',y)\Big] - \frac{1}{DM} \Big)^2 \\
&= \sum_{h',y} \Big(\Pr\Big[(h,h(X)) = (h',y)\Big] - \frac{2}{DM} \Pr\Big[(h,h(X)) = (h',y)\Big] + \frac{1}{DM^2} \Big) \\
&= \mathsf{CP}(h(X),h) - \frac{1}{DM}
\end{aligned}$$

$$\begin{aligned}
\mathsf{CP}(h(X),h) &= \Pr_{h_1,h_2,x_1,x_2}[(h_1(x_1),h_1) = (h_2(x_2),h_2)] \\
&= \Pr_{h_1,h_2}[h_1 = h_2] \cdot \Pr[x_1,x_2,h] \Pr[h(x_1) = h(x_2)] \\
&= \mathsf{CP}(h) \cdot \Big(\Pr_{x_1,x_2}[x_1 \neq x_2] \cdot \Pr_{h,x_1,x_2}[h(x_1) = h(x_2) \mid x_1 \neq x_2] + \\
&\quad \Pr_{x_1,x_2}[x_1 = x_2] \cdot \Pr_{h,x}[h(x_1) = h(x_2) \mid x_1 = x_2] \Big) \\
&\leq \frac{1}{D} \cdot \Big(\max_{x_1 \neq x_2} \Pr_h[h(x_1) = h(x_2)] + \mathsf{CP}(X) \Big) \\
&\leq \frac{1}{D} \cdot \Big(\frac{1}{M} + \mathsf{CP}(X) \Big)
\end{aligned}$$

より，$\varepsilon \coloneqq \sqrt{M \cdot \mathsf{CP}(X)}$ とおくと，

$$\mathsf{CP}(h(X),h) \leq \frac{1}{D}\Big(\frac{1}{M} + \mathsf{CP}(X) \Big) = \frac{1+\varepsilon^2}{DM}$$

よって，

$$\|\mathbf{v}\|_2 = \sqrt{\mathsf{CP}(h(X),h) - \frac{1}{DM}} = \frac{\varepsilon}{\sqrt{DM}}$$

よって，

$$\Delta\Big((h,h(X)), (h,U(\mathcal{Y})) \Big) \leq \frac{\sqrt{DM}}{2} \|\mathbf{v}\|_2 = \frac{1}{2}\varepsilon = \frac{1}{2}\sqrt{M \cdot \mathsf{CP}(X)}$$

□

定義 16 (Rényi Divergence)**.** P, Q を $\mathsf{Supp}(P) \subseteq \mathsf{Supp}(Q)$ を満たす離散確率分布とする．$a \in (1,\infty)$ に対し，位数 a の *Rényi Divergence* を

$$\mathsf{RD}_a(P,Q) = \left(\sum_{x \in \mathsf{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{\frac{1}{a-1}}$$

で定義する．

RD は，統計距離をアナロジーとした，いくつかの性質を満たす．特に，RD の乗法性は，統計距離における加法性に該当する．以下の性質，定理の証明は，[vEH14], [LSS14]，[BS23] に載っている．

補題 17. P, Q を $\mathsf{Supp}(P) \subseteq \mathsf{Supp}(Q)$ の 離散確率分布とする．$a \in (1, \infty)$ に対して，以下が成り立つ．

データ処理不等式： 任意の関数 g に対して

$$\mathsf{RD}_a(g(P) \| g(Q)) \leq \mathsf{RD}_a(P \| Q)$$

が成り立つ．ここで，$g(P)$ は $y \leftarrow P$ によって誘導された $g(y)$ の確率分布である．

確率保存則： $E \subset \mathsf{Supp}(Q)$ を事象とする．このとき，$a \in (1, \infty)$ に対し，

$$Q(E) \cdot \mathsf{RD}_a(P \| Q) \geq P(E)^{\frac{a}{1-a}}$$

が成り立つ．

乗法性： P, Q をランダム変数 (Y_1, Y_2) の組の確率分布であるとする．$i \in \{1, 2\}$ に対し，P_i は P の下の Y_i の周辺分布を意味し，$P_{2|1}(\cdot|y_1)$ は $Y_1 = y_1$ が与えられたうえでの Y_2 の条件付き確立分布を意味する．このとき，$a \in (1, \infty)$ に対し，

$$\mathsf{RD}_a(P \| Q) \leq \mathsf{RD}_a(P_1 \| Q_1) \cdot \max_{y_1 \in Y_1} \mathsf{RD}_a(P_{2|1}(\cdot|y_1)) \| Q_{2|1}(\cdot|y_1))$$

が成り立つ．

補題 18. D_1, D_2 を集合 Z 上の確率分布とし，$e_1, \ldots, e_N$ を $\mathbb{Z} \cap [-B, B]$ の範囲にある（独立でない）確率変数とする（$B \in \mathbb{Z}$）．ここで，ある $a \in (1, \infty)$ および $\rho \geq 1$ が存在して，任意の $|\beta| \leq B$ であるとき，

1. $\mathsf{Supp}(D_1 + \beta) \subseteq \mathsf{Supp}(D_2)$
2. $\mathsf{RD}_a(D_1 + \beta \| D_2) \leq \rho$

が成り立つならば，

$$\mathsf{RD}_a((D_1 + e_N, \ldots, D_1 + e_1) \| D_2^N) \leq \rho^N$$

が成り立つ．

2.3 線形秘密分散

本研究では，閾値型アクセス構造に対する線形秘密分散 (LSSS) を使う．ディーラーは Share を実行し，参加者に対し，秘密の部分情報を配布する．有効集合の参加者が集まると，Rec アルゴリズムによって，秘密を正しく復元できる．

定義 19 (単調アクセス構造)**.** $P = \{P_1, \cdots, P_N\}$ を参加者の集合とする．このとき，単調アクセス構造 *(monotone access structure)* とは，任意の $S \in \mathbb{A}$ に対して，$T \supset S$ ならば $T \in \mathbb{A}$ となるような 部分集合 $\mathbb{A} \subset 2^P$ のことである．

各参加者 P_i をそのインデックス i に対応づける．これによって，各集合 $S \in \mathbb{A}$ を $[N]$ の部分集合として表現する．

任意の $S \subset [N]$, およびベクトル $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_N)$ に対して，$\mathbf{v}\mid_S$ を，インデックス $i \in S$ に対応する要素 $\mathbf{v}_i$ のみを含むベクトルの集合とする．

定義 20 (効率的アクセス構造 [BGG+18])**.** 単調アクセス構造が与えられているとき，任意の $S \subset P$ に対し，$f_{\mathbb{A}}(\mathbf{x}|_S) = 1$ となるのは，$S \in \mathbb{A}$ また，その時に限るような，多項式時間回路 $f_{\mathbb{A}} : \{0,1\}^N \to \{0,1\}$ があるとき，アクセス構造は効率的であるという．すなわち，$\mathbb{A}$ が λ の関数のとき，$\mathbb{A}$ への所属判定が多項式時間 $\mathrm{poly}(\lambda)$ で検証できることをいう．

以後，効率的なアクセス構造のみ扱う．

例 2. $P = \{1,2,3,4\}$ のとき，$\mathbb{A} = \{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$ は単調アクセス構造である．

定義 21 ((t,N) 閾値アクセス構造)**.** 参加者の集合を $P = \{P_1, \cdots, P_N\}$ とする．任意の $S \subseteq P, S \in \mathbb{A}$ と $|S| \geq t+1$ が同値であるとき，アクセス構造 $\mathbb{A}$ は (t,N) 閾値アクセス構造をもつという．

定義 22 (線形秘密分散方式)**.** 正の整数 q, L, n と単調アクセス構造 $\mathbb{A}$ が与えられているとする．以下で定義される多項式時間アルゴリズムの組 $\mathsf{LSS} = (\mathsf{Share}, \mathsf{Rec})$ が以下の性質を満たすとき線形秘密分散方式（LSSS）と言う．

- $\mathsf{Share} : \mathbb{Z}_q \to (\mathbb{Z}_q^L)^N$
- $\mathsf{Rec}_S : (\mathbb{Z}_q^L)^{|S|} \to \mathbb{Z}_q, \quad for \quad S \subset [N]$

プライバシー： 任意の $s \notin \mathbb{A}$ に対して，任意の $x, x' \in \mathbb{Z}_q$ および $\mathbf{v} \in \mathbb{Z}_q^{L|S|}$ について，

$$\Pr\left[\mathsf{Share}(x)|_S = \mathbf{v}\right] = \Pr\left[\mathsf{Share}(x')|_S = \mathbf{v}\right]$$

が成り立つ．

再構成性： 任意の $S \in \mathbb{A}$，任意の $x \in \mathbb{Z}_q$，および $\mathbf{v} = \mathsf{Share}(x)$ について，復元アルゴリズムは，

$$\mathsf{Rec}_S(\mathbf{v}|_S) = x.$$

を出力する．

線形性： 任意の $\alpha, \beta \in \mathbb{Z}_q$，および $|S| > t$ を満たす集合 S，任意のシェアベクトル $\mathbf{v}, \mathbf{b}$ に対し，

$$\mathsf{Rec}_S(\alpha\mathbf{u}|_S + \beta\mathbf{v}|_S) = \alpha\mathsf{Rec}_S(\mathbf{u}|_S) + \beta\mathsf{Rec}_S(\mathbf{v}|_S)$$

が成り立つ．

シェアの集合が $S = [N]$ である場合，Rec の代わりに $\mathsf{Rec}_{[N]}$ と書く．

定義 23 (最大無効集合，最小有効集合)．$x \in \mathbb{Z}_q, (\mathbf{v}_1, \ldots, \mathbf{v}_N) = \mathsf{Share}(x)$，ただし，$\mathbf{v}_i = (\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,L})$ とする．インデックスの組の集合 $T \subseteq [N] \times [L]$ が無効集合であるとは，対応するシェア $(v_{i,j})_{(i,j)\in T}$ が x に関する情報を一切漏らさないことを意味する．つまり，$T \notin \mathbb{A}$．それ以外の場合，T を有効集合であると言う．さらに，

最大無効集合: $T \subseteq [N] \times [L]$ が無効集合で，かつ $(i,j) \in [N] \times [L] \setminus T$ に対し，集合 $T \cup \{(i,j)\}$ が有効集合となるとき，T は最大無効集合であると言う．

最小有効集合: $T \subseteq [N] \times [L]$ が有効集合で，かつ任意の $T' \subset T$ に対して，T' が無効集合であるとき、T は最小有効要素集合であると言う．

定義 24 (Strong-$\{0,1\}$-Reconstruction)．任意の秘密 x，$(\mathbf{v}_1, \ldots, \mathbf{v}_N) = \mathsf{Share}(x)$ と，任意の有効集合 $T \subseteq [N] \times [L]$ に対し，ある部分集合 $T' \subseteq T$ が存在し，

$$\sum_{(i,j)\in T'} \mathbf{v}_{i,j} = x$$

が成り立つとき（ただし，$\mathbf{v}_i = (\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,L})$），*Strong-*$\{0,1\}$*-Reconstruction* であるという．また，$\tau_{\max}$ で，最大無効集合の最小サイズを表し，$\tau_{\min}$ で最小有効集合の最大サイズを表す．

Share が加法によって定義されている (t,N)LSSS は，strong-$\{0,1\}$-LSSS である．

例 3 ($(N-1,N)$ 加法 LSSS)．$(N-1,N)$ 加法 LSSS では，復元に N 人の参加者が必要である．秘密を $s \in \mathbb{Z}_q$ とする．LSS を以下のように定義する．

- $\mathsf{Share}(s)$*:* $s = \sum_{i=1}^{N} s_i$ となるよう，s_i をサンプルし，各 s_i を参加者 P_i に分配する．
- $\mathsf{Rec}(s_1, \ldots, s_N)$*:* N 人の参加者が集まれば，$\sum_{i=1}^{N} s_i = s$ によって秘密を復元できる．

このとき，参加者に分配されるシェアは一つなので，$L = 1$ となる．また，$\tau_{\max} = n - 1, \tau_{\min} = n$ である．

例 4 ($(t-1, N)$ 複製 LSSS)．$(t-1, N)$ 複製 LSSS では，加法 LSSS のシェアを一人に複数分配することで，$(t-1, N)$LSSS を実現する方式である．任意の t 人が集まると，シェアの和によって，秘密を復元できる．秘密を $s \in \mathbb{Z}_q$ とする．LSS を以下のように定義する．

- Share(s)*:* 任意のサイズ t の集合 $A \subset [N]$ に対し，$\sum_A s_A = s$ となるようにシェア $\{s_A\}_A$ を作成し，A 内の参加者 P_i に対し，$i \notin A$ のシェアを分配する．すなわち，各参加者のシェアサイズは $L = \binom{N-1}{t}$ となる．例えば，参加者が 5 人で，閾値 $t = 2$ の場合，秘密 s を $\binom{N}{t} = 10$ 個のシェアに分割し，各参加者に $\binom{N-1}{t} = 6$ 個のシェアを分配する．

  また，あるサイズ t の集合 A' に対し，シェア $s_{A'}$ を作成したとき，$A \neq A'$ となる全ての s_A が無効なものである．$N - t$ 人の参加者が復元に使える複製 $s_{A'}$ を受け取るため，最大無効集合は，$\tau_{\max} = NL - (N-t) = (N-t)(\binom{N}{t} - 1)$ となる．

- Rec*:* t 個以上のシェアが集まれば，加法によって復元できる．また，最低でも全ての s_A を含んでいれば復元可能なので，$\tau_{\min} = \binom{n}{t}$ となる．

線形秘密分散方式は行列によって表現できる．また，Regev 暗合の秘密鍵を分散するため，ベクトルの秘密分散へと拡張する．

ベクトルの秘密分散　以下，ベクトル $\mathbf{s} \in \mathbb{Z}_q^n$ を分散する方法について述べる．

$\mathbf{M}[j]$ を行列 $\mathbf{M}$ の第 j 行目とする．

1. アクセス構造に基づきシェア行列を定義: $\mathbf{M} \in \mathbb{Z}_q^{\ell \times k}$
2. 乱数をサンプル: $\mathbf{r}_1, \ldots, \mathbf{r}_{N-1} \in U(\mathbb{Z}_p^n)$
3. $\mathbf{R} = (\mathbf{s}, \mathbf{r}_1, \ldots, \mathbf{r}_{k-1})^t \in \mathbb{Z}_q^{k \times N}$ とおく．
4. シェアの生成: $\mathbf{V} = \mathbf{M} \cdot \mathbf{R} \in \mathbb{Z}_q^{\ell \times N}$ を計算し，各参加者 P_i は，部分集合 $T_i \subseteq [\ell]$ 行，すなわち，$\{\mathbf{v}_j\}_{j \in T_i}$ を受け取る．

分散されたベクトルは以下の手順で再構成する．

1. S を有効集合とする．$\sum_{j \in \cup_{i \in S} \mathbf{T}_i} c_j \cdot \mathbf{M}[j] = (1, 0, \ldots, 0)$ を満たすベクトル $\{x_j\}_{j \in \cup_{i \in S} \mathbf{T}_i}$ を計算する．また，このようなベクトルを再構成ベクトルと言う．
2. $\sum_{j \in \cup_{i \in S} T_i} x_j \cdot \mathbf{V}[j] = \mathbf{s} \in \mathbb{Z}_q^N$ を計算する．

また，各参加者 P_i の秘密鍵シェアを $\tilde{\mathbf{s}}_i^t$ とする．$\tilde{\mathbf{s}}_i^t$ は，$\{\mathbf{v}_j\}_{j \in T_i}$ と $\{x_j\}_{j \in T_i}$ を用いて，

$$\tilde{\mathbf{s}}_i^t = \sum_{j \in T_i} x_j \cdot \mathbf{V}[j] \in \mathbb{Z}_q^N$$

と表される．

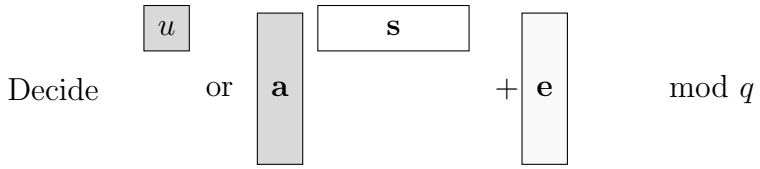
2.4 LWE問題

LWE 問題は，Regev[Reg05] によって提案された．以下，[青安 19] を参考にした．

λ をセキュリティパラメータ，$n, q = \mathrm{poly}(\lambda)$ を正整数，χ を平均 0，分散 σ^2 の $\mathbb{Z}$ 上の離散ガウス分布とする．ベクトル $\mathbf{s} \in \mathbb{Z}_q^n$ を固定する．確率分布 $A_{\mathbf{s},\chi}$ を，一様ランダムに選ばれた $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ とノイズ $e \leftarrow \chi$ に対して，$(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ を出力するものとする．ただし，$b = \langle \mathbf{s}, \mathbf{a} \rangle + e \mod q$ とする．

LWE 問題には，判定問題と探索問題がある:

1. 判定 LWE 問題: 与えられた $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ が，確率分布 $A_{\mathbf{s},\chi}$ からサンプルされた元 か，$\mathbb{Z}_q^n \times \mathbb{Z}_q$ から一様ランダムにサンプルされた元かを判定する．

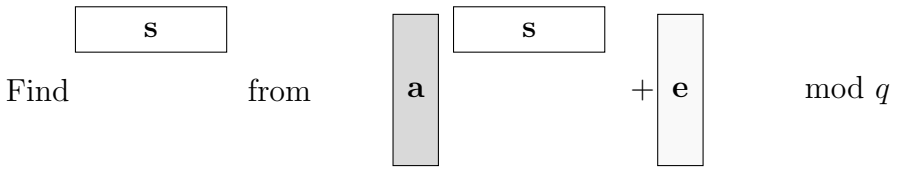


   ただし，$u \leftarrow \mathbb{Z}_q$ とする．判定 LWE 問題が困難であるとは，PPT 攻撃者 $\mathcal{A}$ に対して，

$$\mathcal{A}^{\mathsf{LWE}} = |\Pr[\mathcal{A}(\mathbf{a}, b) = 1] - \Pr[\mathcal{A}(\mathbf{a}, u) = 1]| < \mathsf{negl}(\lambda)$$

   が成り立つことをいう．

2. 探索 LWE 問題: 確率分布 $A_{\mathbf{s},\chi}$ からサンプルされた $(\mathbf{a}, b)$ から $\mathbf{s}$ を当てる．



探索 LWE 問題は，ノイズがない場合，掃き出し法によって多項式時間で解を求めることが可能である．つまり，ノイズの大きさが問題の困難性の理由となっている．

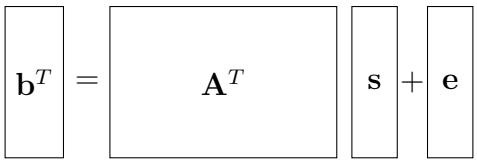
Regev 暗号では，上記の設定に加え，ある固定値 $m = \mathrm{poly}(\lambda)$ を考え，確率分布 $A_{\mathbf{s},\chi}$ からサンプルされた異なる m 個の組

$$\begin{cases} (\mathbf{a}_1, b_1), & b_1 = \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \mod q \\ & \vdots \\ (\mathbf{a}_m, b_m), & b_m = \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \mod q \end{cases}$$

から LWE 問題を解くことを考える．第 i 列ベクトルを $\mathbf{a}_i$ とする $n \times m$ 行列を $\mathbf{A}$ とし，$\mathbf{b} = (b_1, \ldots, b_m)$ とおく．このとき，m 個の LWE サンプルの組は，$(\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ と表せ，関係式

$$\mathbf{b} = \mathbf{s}^T \mathbf{A} + \mathbf{e}^T \mod q$$

を満たす.



この形式に合わせ，判定 LWE 問題を書き換えると，以下のようになる.

定義 25 (判定 LWE 問題（行列）). $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ とする．与えられた $(\mathbf{A}, \mathbf{b})$ が $(\mathbf{A}, \mathbf{b}_0) \leftarrow A_{\mathbf{s},\chi,m}$ のように選ばれた元か，$(\mathbf{A}, \mathbf{b}_1) \leftarrow U(\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m)$ のように一様ランダムに選ばれた元か判定する問題を判定 *LWE* 問題という.

このとき，攻撃者の優位性を

$$\mathsf{Adv}^{\mathsf{LWE}} := |\Pr[\mathcal{A}(\mathbf{A}, \mathbf{b}_0) = 1] - \Pr[\mathcal{A}(\mathbf{A}, \mathbf{b}_1) = 1]|$$

と定義する．$\mathsf{Adv}^{\mathsf{LWE}} = \mathsf{negl}(n)$ のとき，判定 *LWE* 問題は解読困難であるという.

第3章　閾値型公開鍵暗号

本章では，閾値型公開鍵暗号方式 (ThPKE) と安全性に関する定義を与える．

3.1　ThPKE の構文

定義 26 (ThPKE)**.** 次のような PPT アルゴリズムの組

$$\mathsf{ThPKE} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{PartDec}, \mathsf{Combine})$$

を，メッセージ空間 $\mathcal{M}$ に対する閾値型公開鍵暗号 ThPKE という．

$\mathsf{Setup}(1^\lambda, N, t) \to (\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$ **：** セキュリティパラメータ λ, 参加者の数 N, 閾値 $t \in \{1, \ldots, N-1\}$ を入力し，公開パラメータ pp，公開鍵 pk 秘密鍵の集合 $\mathsf{sk}_1, \ldots, \mathsf{sk}_N$ を出力する．

$\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$**：** 公開鍵 pk と平文 $m \in \mathcal{M}$ を入力し，暗号文 ct を出力する．

$\mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}) \to d_i$ **：** 参加者 $i \in [N]$ に対応する秘密鍵 sk_i と暗号文 ct を入力し，部分復号シェア d_i を出力する．

$\mathsf{Combine}(\{d_i\}_{i\in S}, \mathsf{ct}) \to m'$ **：** 復号シェア $\{d_i\}_{i\in S} \quad (S \subset [N] \wedge |S| \geq t+1)$ と暗号文 ct を入力し，メッセージ $m' \in M \cup \{\perp\}$ を出力する．

定義 27 (復号の正当性)**.** ある閾値値完全準同型暗号（ThPKE）方式が復号の正しいとは，次の条件が成り立つ場合を指す．すなわち，任意の (λ, N, t, S)（ただし $(S \subseteq [N])$ で $(|S| \geq t+1)$ を満たす），任意の $(m \in \mathcal{M})$ に対して，ある無視可能関数 $\mathsf{negl}(\lambda)$ が存在し，

$$\begin{aligned}
&(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N) \to \mathsf{Setup}(1^\lambda, N, t) \\
&\mathsf{ct}_j \to \mathsf{Enc}(\mathsf{pk}, m) \\
&d_i \to \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}) \quad for\ i \in S
\end{aligned}$$

とする．このとき，次が成り立つ：

$$\Pr\left[\mathsf{Combine}(\{d_i\}_{i\in S}, \mathsf{ct}) = m\right] = 1 - \mathsf{negl}(\lambda)$$

定義 28 (PKE)**.** $n = 1$ の ThPKE を公開鍵暗号方式 PKE という．このとき，PartDec, Combine を一つのアルゴリズム Dec にまとめる．つまり，Dec は，秘密鍵 sk と暗号文 ct を入力し，メッセージ $m' \in \{\mathcal{M} \cup \{\perp\}\}$ を出力する．

定義 29 (PKE の (β, ε)-線形復号性)**.** $\mathsf{PKE} \coloneqq (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ を公開鍵暗号方式とし，平文空間を $\mathcal{M} \subseteq R_p$ ，暗号文空間を R_q^r とする．Setup が秘密鍵 $\mathsf{sk} \in R_q^r$ を出力するとする．ただし，$\mathsf{sk} = (-\mathbf{s}, 1)$ で，$\mathbf{s} \in R_q^{r-1}$ とする．

$\beta = \beta(\lambda) \in \mathbb{N}, \varepsilon = \varepsilon(\lambda) \in [0, 1]$ とする．PKE が (β, ε)-線形復号であるとは，任意の $\lambda \in \mathbb{N}$ に対し，$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$，平文 $m \in R_p$，暗号文 $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m) \in R_q^r$ に対し，

$$\langle \mathsf{sk}, \mathsf{ct} \rangle = \lfloor q/p \cdot m \rceil + e \mod q$$

が成り立つことをいう．ここで，$e \in R_q$ であり，

$$\Pr\left[\|e\|_\infty \leq \beta\right] \geq 1 - \varepsilon$$

すなわち，$\Pr\left[\|e\|_\infty > \beta\right] \leq \varepsilon$ を満たす．

定義 30 (Regev 暗号)**.** 次のようなアルゴリズムの組 $\mathsf{Regev} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ を *Regev* 暗号という．このとき，平文空間を $\mathcal{M}$ とする．

n, m, q を正整数，$m \approx 3n \log n, q \approx n^2$，$\chi \coloneqq D_{\mathbb{Z},s}$，$\chi$ の幅を $s \approx \sqrt{n}$ とする．(n, m, q, χ) は公開パラメータ pp であり，それぞれ，安全性パラメータ，*LWE* サンプルの個数，法，ノイズパラメータを意味する．

Setup: 次のように公開鍵と秘密鍵を生成する．

1. $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
2. $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n \times m})$,
3. $\mathbf{e} \sim \chi^m$,
4. $\mathbf{b}^t \coloneqq \mathbf{s}^t \mathbf{A} + \mathbf{e}^t \in \mathbb{Z}_q^m$,
5. 公開鍵 $\mathsf{pk} \coloneqq (\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$, 秘密鍵 $\mathsf{sk} \coloneqq (-\mathbf{s}^T, 1) \in \mathbb{Z}_q^{(n+1)}$ を出力する．

Enc: 公開鍵 pk と平文 $\mu \in \mathbb{Z}_p$ を受け取り，次のように暗号文を生成する．

1. $\mathbf{r} \leftarrow \{0, 1\}^m$,
2. $\mathbf{c}_0 \coloneqq \mathbf{A}\mathbf{r}$,
3. $\mathbf{c}_1 \coloneqq \mathbf{b}^t \mathbf{r} + \mu \cdot \left\lfloor \frac{q}{p} \right\rceil$,
4. $\mathsf{ct} \coloneqq (\mathbf{c}_0, c_1) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

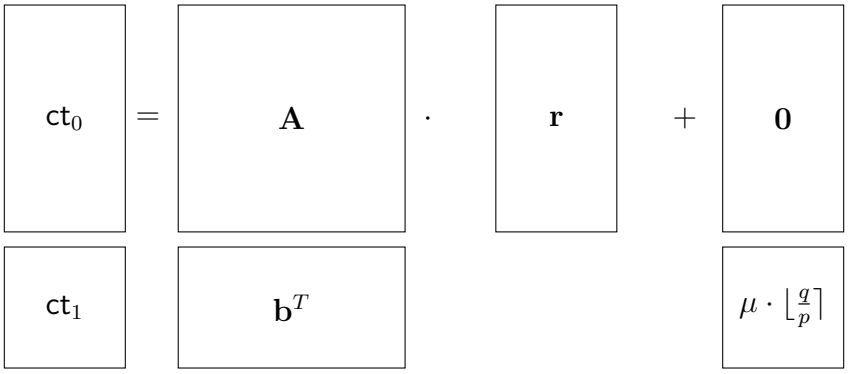


図 3.1: Regev 暗合の形

Dec: 秘密鍵 sk と暗号文 ct を受け取り，次のように平文を復元する．

1. $\mu' \coloneqq \langle \mathsf{ct}, \mathsf{sk} \rangle$,
2. $\lfloor \mu' \rceil \mod q$ の値を出力.

定理 31. *Regev* 暗号は，(β, ε)-線形復号性を満たす.

証明. $\mathsf{sk} = (-\mathbf{s}^t, 1), \mathsf{ct} = (\mathbf{c}_0, c_1)$ とすると，

$$\begin{aligned}\langle \mathsf{sk}, \mathsf{ct} \rangle &= \mathbf{c}_1 - \mathbf{s}^t c_0 \\ &= (\mathbf{b}^t \mathbf{r} + \mu \lfloor q/p \rceil) - \mathbf{s}^t (A\mathbf{r}) \\ &= ((\mathbf{s}^t \mathbf{A} + \mathbf{e}^t)\mathbf{r} + \mu \lfloor q/p \rceil) - \mathbf{s}^t (\mathbf{A}\mathbf{r}) \\ &= \mu \lfloor q/p \rceil + \mathbf{e}^t \mathbf{r}\end{aligned}$$

となる．$\mathbf{e}^t = (e_1, \ldots, e_m)$ とおくと，$-|\sum_i e_i| \leq \mathbf{e}^t \mathbf{r} \leq |\sum_i e_i|$ で，各 $e_i \sim \chi$ である．$\chi \coloneqq D_{\mathbb{Z},s}$ は 0-subgaussian であるので，0-Sub Gaussian Tail Bound が成り立ち，$X \coloneqq \sum_i e_i$ は

$$\Pr\left[|X| > t\sqrt{m}\right] \leq 2e^{\pi(\frac{t}{s})^2}$$

が成り立つ．いま，$t = s \cdot \omega(\sqrt{\ln n})$ とおくと，$\Pr\left[|X| > t\sqrt{m}\right] = \mathsf{negl}(n)$ となる．よって，$s\sqrt{m} \cdot \omega(\sqrt{\ln n})$ が $q/2p$ より小さければ復号は圧倒的な確率で成功する． □

この定理は，ノイズが大きすぎなければ，復号が正しく行われることを主張している．p の値を増やし，平文空間を大きくするほど，許容できるノイズの量が小さくなる．

3.2 堅牢性

閾値型の安全性ゲームでは，攻撃者は汚染集合を定め，対応する秘密鍵シェアを受け取る操作をしばしば用いる．これを静的汚染 (static corruption setting) という．

ThPKE の堅牢性に関する定義を二つ述べる．

一つ目，弱選択暗号文堅牢性は，攻撃者が全ての秘密鍵シェアにアクセス可能であっても，一つの暗号文 ct に対し，Combine によって，二つの異なるメッセージを返すような部分復号集合を作成するのが困難であることを言っている．

二つ目，強選択平文堅牢性は，攻撃者が汚染集合と正直に生成された暗号文を受け取ったとき，正直な参加者の部分復号を利用しても，Combine によって，異なるメッセージを返すことが困難であることを言っている．

定義 32 (弱選択暗号文堅牢性)**.** 任意の λ, N, t と任意の PPT 攻撃者 $\mathcal{A}$ に対し，

$$\mathsf{Adv}^{\text{w-cc-robust}}_{\mathsf{ThPKE}}(\mathcal{A}) \coloneqq \Pr\left[\mathsf{Expt}^{\text{w-cc-robust}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, N, t) = 1\right] = \mathsf{negl}(\lambda)$$

が成り立つとき, ThPKE は弱選択暗号文堅牢性であるという．このとき, $\mathsf{Expt}^{\text{w-cc-robust}}_{\mathcal{A},\mathsf{ThPKE}}$ は図（*3.2*）の実験である．

$\mathsf{Expt}^{\text{w-cc-robust}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, N, t)$

$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N) \leftarrow \mathsf{Setup}(1^\lambda, N, t)$

$(\mathsf{ct}, S, S^{'}, \{d_i\}_{i\in S}, \{d_i^{'}\}_{i\in S^{'}}) \leftarrow \mathcal{A}(\mathsf{pp}, \mathsf{pk}, \{\mathsf{sk}_i\}_{i\in[N]})$

$m \leftarrow \mathsf{Combine}(\{d_i\}_{i\in S}, \mathsf{ct})$

$m^{'} \leftarrow \mathsf{Combine}(\{d_i^{'}\}_{i\in S^{'}}, \mathsf{ct})$

return $m^{'} \neq m \wedge \perp \notin \{m, m^{'}\}$

図 3.2: ThPKE の弱選択暗号文堅牢性ゲーム

ThPKE の弱選択暗号文堅牢性ゲームのプロトコル

Challenger		**Adversary**
$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$		$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$
	$\mathsf{ct}, S, S^{'}, \{d_i\}_{i\in S}, \{d_i^{'}\}_{i\in S^{'}} \longleftarrow$	$\mathcal{A}(\mathsf{pp}, \mathsf{pk}, \{\mathsf{sk}_i\}_{i\in[N]})$
$m \leftarrow \mathsf{Combine}(\{d_i\}_{i\in S}, \mathsf{ct})$		
$m^{'} \leftarrow \mathsf{Combine}(\{d_i^{'}\}_{i\in S^{'}}, \mathsf{ct})$		
win if $m^{'} \neq m$		

定義 33 (強選択平文堅牢性)**.** 任意の λ, N, t と任意の PPT 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し，

$$\mathsf{Adv}^{\text{s-cp-robust}}_{\mathsf{ThPKE}}(\mathcal{A}) \coloneqq \Pr\left[\mathsf{Expt}^{\text{s-cp-robust}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, N, t) = 1\right] = \mathsf{negl}(\lambda)$$

が成り立つとき, ThPKE は強選択平文堅牢性であるという．このとき, $\mathsf{Expt}^{\text{s-cp-robust}}_{\mathcal{A},\mathsf{ThPKE}}$ は図（*3.3*）の実験である．

$\mathsf{Expt}^{\text{s-cp-robust}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, N, t)$

$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \cdots, \mathsf{sk}_N) \leftarrow \mathsf{Setup}(1^\lambda, N, t)$
$(S, m) \leftarrow \mathcal{A}_1(\mathsf{pp}, \mathsf{pk}) : S \subset [N] \wedge |S| \leq t$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
$d_j \leftarrow \mathsf{PartDec}(\mathsf{sk}_j, \mathsf{ct}), \forall j \in [N] \setminus S$
$\{d_i\}_{i \in S} \leftarrow \mathcal{A}_2(\mathsf{pk}, \{\mathsf{sk}_i\}_{i \in S}, \{d_j\}_{j \notin S}, \mathsf{ct})$
$m^{'} \leftarrow \mathsf{Combine}(\{d_i\}_{i \in [N]}, \mathsf{ct})$
return $m \neq m^{'}$

図 3.3: ThPKE の強選択平文堅牢性ゲーム

ThPKE の強選択平文堅牢性ゲームのプロトコル

Challenger		**Adversary**
$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$		$(\mathsf{pp}, \mathsf{pk})$
	$\xleftarrow{\text{(S,m)}}$	$\mathcal{A}_1(\mathsf{pp}, \mathsf{pk})$
	$\xrightarrow{\{\mathsf{sk}_i\}_{i \in S}}$	
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$		
$d_j \leftarrow \mathsf{PartDec}(\mathsf{sk}_j, \mathsf{ct}), \forall j \notin S$		
	$\xrightarrow{\mathsf{ct}, \{d_j\}_{j \notin S}}$	
	$\xleftarrow{\{d_i\}_{i \in S}}$	$\mathcal{A}_2(\mathsf{pk}, \{\mathsf{sk}_i\}_{i \in S}, \{d_i\}_{j \notin S}, \mathsf{ct})$
$m^{'} \leftarrow \mathsf{Combine}(\{d_i^{'}\}_{i \in [N]}, \mathsf{ct})$		
win if $m^{'} \neq m$		

不正者の数 t が $t < N/2$ のとき，任意の ThPKE は弱選択暗号文堅牢性から強選択平文堅牢性に変換可能である．Combine アルゴリズムを任意の $t+1$ サイズの部分集合に対して実行すれば，正直な参加者のみの部分集合が見つかる．つまり，復号を正確に行う部分集合が見つかる．

3.3 ThPKE の一方向性

アルゴリズムが一方向性（OW）を満たすとは，入力から出力の計算は容易だが，出力から逆像の計算が計算量的に困難であることをいう．OW-CPA 安全であるとは，攻撃者が自由に選択した平文に対する暗号文を入手できる状況で，解読対象の平文に関する情報が完全には洩れないことを意味する．すなわち，部分情報の漏洩は許容する．公開鍵暗号方式では，誰もが任意の平文を暗号化することができるので，最低限満たす必要のある安全性である．

ゲームの概要としては，攻撃者は最初に静的汚染を行い，その後，二つのオラクル $\mathsf{OEnc}, \mathsf{OPartDec}$ にアクセスする．これによって，受け取った汚染集合に対する部分復号を用いて戦者の平文を推測する．

定義 34 (ThPKE の ℓ-OW-CPA 安全性)**.** PPT 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し，

$$\mathsf{Adv}^{\ell\text{-OW-CPA}}_{\mathsf{ThPKE}}(\mathcal{A}) \coloneqq \Pr\left[\mathsf{Expt}^{\ell\text{-OW-CPA}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, n, t) = 1\right] = \mathsf{negl}(\lambda)$$

が成り立つとき，ThPKE 方式は，セキュリティパラメータ λ , 閾値パラメータ n, t , クエリ回数の上限 ℓ に対し，ℓ-OW-CPA 安全であるという．ここで，$\mathsf{Expt}^{\ell\text{-OW-CPA}}_{\mathcal{A},\mathsf{ThPKE}}$ は，図 *(3.4)* に定めるゲームである．初期状態は，$\mathsf{ctr} = 0, \mathsf{idx} = 0, \mathsf{L} = \phi$ である．また，$\mathsf{Adv}^{\ell\text{-OW-CPA}}_{\mathsf{ThPKE}}(A)$ を PPT 攻撃者 $\mathcal{A}$ の優位性いう．

$\mathsf{Expt}^{\ell\text{-OW-CPA}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, N, t)$

$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}'(1^\lambda)$
$S \leftarrow \mathcal{A}_1(\mathsf{pp}, \mathsf{pk}) : S \subset [N] \wedge |S| \leq t$
$(m', j) \leftarrow \mathcal{A}_2^{\mathsf{OEnc},\mathsf{OChallEnc},\mathsf{OPartDec}}(\mathsf{pk}, \{\mathsf{sk}_i\}_{i\in S})$
$(b_j, m_j, \mathsf{ct}_j) \coloneqq \mathsf{L}[j]$
Output: $m_j = m' \wedge b_j = 1$

$\mathsf{OEnc}(m)$

if $m \notin \mathcal{M}$ **then return** $\perp$
$\mathsf{idx} = \mathsf{idx} + 1$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
$\mathsf{CT} = \mathsf{CT} \cup \{\mathsf{ct}\}$
$\mathsf{L}[\mathsf{idx}] \coloneqq (0, m, \mathsf{ct})$
Output: ct

$\mathsf{OChallEnc}()$

$\mathsf{idx} = \mathsf{idx} + 1$
$m \leftarrow \mathcal{M}$
$\mathsf{ChallM} = \mathsf{ChallM} \cup \{m\}$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
$\mathsf{ChallCT} = \mathsf{ChallCT} \cup \{\mathsf{ct}\}$
$\mathsf{L}[\mathsf{idx}] \coloneqq \{(1, m, \mathsf{ct})\}$
Output: ct

$\mathsf{OPartDec}(\iota)$

$\mathsf{ctr} = \mathsf{ctr} + 1$
if $\mathsf{ctr} > \ell$ **then return** $\perp$
if $\iota > |L|$ **then return** $\perp$
$(b, m, \mathsf{ct}) \coloneqq \mathsf{L}[\iota]$
if $b = 1$ **then return** $\perp$
$d_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}), i \in [N]$
$\mathsf{d} = (d_i)_{i\in[N]}$
$\mathsf{PartD} = \mathsf{PartD} \cup \{\mathsf{d}\}$
Output: d

図 3.4: ThPKE の ℓ-OW-CPA ゲーム

ThPKE の ℓ-OW-CPA ゲーム

Challenger		**Adversary**
$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$		$(\mathsf{pp}, \mathsf{pk})$
	$\xleftarrow{S}$	$\mathcal{A}_1(\mathsf{pp}, \mathsf{pk})$
	$\xrightarrow{\{\mathsf{sk}_i\}_{i\in S}}$	
	$\xleftarrow{(m', j)}$	$\mathcal{A}_2^{\mathsf{OEnc},\mathsf{OChallEnc},\mathsf{OPartDec}}(\mathsf{pk}, \{\mathsf{sk}_i\}_{i\in S})$

win if
$m_j = m' \wedge b_j = 1$

各 Oracle へのクエリ順序は問わない

OEnc

	$\xrightarrow{m}$	if $m \notin \mathcal{M}$ abort
		$\mathsf{idx} = \mathsf{idx} + 1$
$\mathsf{CT} = \mathsf{CT} \cup \{\mathsf{ct}\}$	$\xleftarrow{\mathsf{ct}}$	
		$\mathsf{L}[\mathsf{idx}] = (0, m, \mathsf{ct})$

OChallEnc

		$\mathsf{idx} = \mathsf{idx} + 1$
		$m \leftarrow \mathcal{M}$
		$\mathsf{ChallM} = \mathsf{ChallM} \cup \{m\}$
$\mathsf{ChallCT} = \mathsf{ChallCT} \cup \{\mathsf{ct}\}$	$\xleftarrow{\mathsf{ct}}$	$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
		$\mathsf{L}[\mathsf{idx}] = (1, m, \mathsf{ct})$

OPartDec

		$\mathsf{ctr} = \mathsf{ctr} + 1$
		if $\mathsf{ctr} > \ell$ abort
	$\xrightarrow{\iota}$	if $\iota > \lvert L \rvert$ abort
		$(b, m, \mathsf{ct}) = \mathsf{L}[\iota]$
		if $b = 1$ abort
$\mathsf{PartD} = \mathsf{PartD} \cup \{\mathbf{d}\}$	$\xleftarrow{\mathbf{d}}$	$d_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$

3.4 識別不可能性

異なる平文 m_0, m_1 に対し，その暗号文 $\mathsf{Enc}(m_0)$ と $\mathsf{Enc}(m_1)$ を識別できないとき，識別不可能，または IND 安全であるという．また，選択平文攻撃が可能な攻撃者に対し，いかなる部分情報も洩れないとき，IND-CPA 安全であるという．

ThPKE の IND-CPA を定義する前に，PKE の IND-CPA を確認する．

定義 35 (PKE の IND-CPA 安全性)**.** PPT 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し，

$$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{PKE}}(\mathcal{A}) \coloneqq \left| \Pr\left[\mathsf{Expt}^{\text{IND-CPA}}_{\mathcal{A},\mathsf{PKE}}(1^\lambda) = 1\right] - \frac{1}{2} \right| = \mathsf{negl}(\lambda)$$

が成り立つとき，$\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ は，セキュリティパラメータ λ に対し，IND-CPA 安全であるという．ここで，$\mathsf{Expt}^{\text{IND-CPA}}_{\mathcal{A},\mathsf{PKE}}$ は，図 *(3.5)* に定めるゲームである．また，$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{PKE}}(\mathcal{A})$ を PPT 攻撃者 $\mathcal{A}$ の優位性という．

$\mathsf{Expt}^{\text{IND-CPA}}_{\mathcal{A},\mathsf{PKE}}(1^\lambda)$

$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pp}, \mathsf{pk})$
$b \leftarrow \{0, 1\}$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$
$b' \leftarrow \mathcal{A}(\mathsf{sk}, \mathsf{ct})$
Output: $b = b'$

図 3.5: PKE の IND-CPA ゲーム

IND-CPA のプロトコル

Challenger		**Adversary**
$(\mathsf{pk}, \mathsf{sk})$		pk
	$\xleftarrow{m_0, m_1}$	$\mathcal{A}(\mathsf{pp}, \mathsf{pk})$
$b \leftarrow \{0, 1\}$		
$\mathsf{ct}_b \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$	$\xrightarrow{\mathsf{ct}_b}$	
	$\xleftarrow{b'}$	$\mathcal{A}(\mathsf{sk}, \mathsf{ct})$
win if $b = b'$		

定理 36. 判定 *LWE* 問題に対する攻撃者の優位性を $\varepsilon^{\mathsf{LWE}}(n)$ とする．このとき，任意の PPT 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し，

$$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Regev}}(\mathcal{A}) \leq \varepsilon^{\mathsf{LWE}} + 2^{-\frac{m-(n+1)\log(q)}{2}-1}$$

が成り立つ．$\varepsilon^{\mathsf{LWE}}(n) = \mathsf{negl}(n), m \approx 3n\log n, q \approx n^2$ とすると，右辺は無視できる．

証明. ゲーム変換で示す．ゲームを通じ，チャレンジビット $b \in \{0,1\}$ は一様ランダムに選ぶ．また，ゲーム G_i での攻撃者の出力 b' に対し，$\varepsilon_i \coloneqq \Pr_{G_i}\left[b = b'\right] - \frac{1}{2}$ とする．

ゲーム G_0　定義 (35)（PKE の IND-CPA ゲーム）と同じ．公開鍵 pk，秘密鍵 sk は挑戦者により以下のように生成される．

1. $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
2. $A \leftarrow U(\mathbb{Z}_q^{n\times m})$,
   - $\mathbf{e} \sim \chi^m$,
   - $\mathbf{b}^t \coloneqq \mathbf{s}^t A + \mathbf{e}^t \in \mathbb{Z}_q^m$,
3. $\mathsf{pk} \coloneqq (A, \mathbf{b}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$, $\mathsf{sk} \coloneqq \mathbf{s} \in \mathbb{Z}_q^n$.

のように作られる．
定義より，$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Regev}}(n) = \varepsilon_0$ である．

ゲーム G_1　挑戦者は，外部オラクルによって公開鍵 $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$ を生成する．

1. $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$
2. $(\mathbf{A}, \mathbf{b}) \leftarrow \mathbf{A}_{\mathbf{s},\chi,m}$

を実行し，$(\mathbf{A}, \mathbf{b})$ を挑戦者に渡す．攻撃者の視点では，$\varepsilon_1 = \varepsilon_0$

ゲーム G_2　挑戦者は，外部オラクルによって公開鍵 $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$ を生成する．

1. $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$,
2. $\mathbf{b} \leftarrow U(\mathbb{Z}_q^m)$

のように一様ランダムに $(\mathbf{A}, \mathbf{b})$ を生成する．

ゲーム G_3　チャレンジ暗号文の作り方を変更する．平文 $\mu_0, \mu_1 \in \mathbb{Z}_p$ を攻撃者から受け取り，$b \leftarrow U(\mathbb{Z}_p)$ を選んだあと，

1. $\mathbf{c}_0 \leftarrow U(\mathbb{Z}_q^n)$,
2. $k \leftarrow U(\mathbb{Z}_q)$,
3. $\mathbf{c}_1 \coloneqq k + \mu_b \cdot \lfloor q/p \rceil \mod q$,
4. $\mathsf{ct} \coloneqq (\mathbf{c}_0, c_1)$.

とする．これ以外は，G_2 と同じ．

G_1 と G_2 の違いは，攻撃者に与える情報が，$(A, \mathbf{b}_0)$ か，$(A, \mathbf{b}_1)$ かである．

攻撃者 $\mathcal{A}_1$ は，$(A, \mathbf{b}_i)$ を入力として受け取り，予測 b_i' を出力する．$(i = 0, 1)$ つまり，$\mathcal{A}_1(A, \mathbf{b}_i) = b_i'$.

LWE 問題の識別アルゴリズムを実行できる攻撃者 $\mathcal{A}_2$ を考える．$\mathcal{A}_2$ は，$\mathcal{A}_1$ の予測 b_i を受け取り，$b = b_i'$ であれば 1 を出力し，それ以外は 0 を出力する．

$$\begin{aligned}\Pr[\mathcal{A}_2(b_0) = 1] - \Pr[\mathcal{A}_2(b_1) = 1] &= \Pr_{G_1}\left[b = b'\right] - \Pr_{G_2}\left[b = b'\right] \\ &\leq \varepsilon^{\mathsf{LWE}}(n)\end{aligned}$$

攻撃者の優位性を考えると，

$$\varepsilon_1 - \varepsilon_2 \leq \varepsilon^{\mathsf{LWE}}(n)$$

が成り立つ．

G_3 において，k は一様ランダムに選ばれた値なので，μ_b を one-time pad していることになり，c_1 から μ_b の情報は全く洩れない．よって，$\varepsilon_3 = 0$ となる．

$$\bar{\mathbf{A}} \coloneqq \begin{pmatrix}\mathbf{A} \\ \mathbf{b}^T\end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m} \quad \text{where} \quad \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{b} \leftarrow \mathbb{Z}_q^m$$

とする．ゲーム G_2 で作られた $(\bar{\mathbf{A}}, \bar{\mathbf{A}}\mathbf{r})$ とゲーム G_3 で作られた $(\bar{\mathbf{A}}, (\mathbf{c}_0, k)^T)$ の統計距離を考える．$\mathsf{H}_\infty(\mathbf{r}) = m$ と補題 (15) により，

$$\Pr_{G_2}\left[b = b'\right] - \Pr_{G_3}\left[b = b'\right] \leq 2^{-\frac{m-(n+1)\log q}{2}-1}$$

となる．また，

$$\varepsilon_2 - \varepsilon_3 \leq 2^{-\frac{m-(n+1)\log q}{2}-1}$$

が成り立つ．

以上より，$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Regev}} \coloneqq \varepsilon_0 = \varepsilon_0 - \varepsilon_3 = \sum_{i=0}^{2}(\varepsilon_i - \varepsilon_{i+1}$ より，

$$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Regev}} \leq \varepsilon^{\mathsf{LWE}}(n) + 2^{-\frac{m-(n+1)\log q}{2}-1}$$

となるので，$\varepsilon^{\mathsf{LWE}} = \mathsf{negl}(n), m \approx 3n\log n, q \approx n^2$ であれば，右辺は n に関して無視できる確率になり，$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Regev}}$ も無視できる確率となる． □

OW-CPA ゲームの時と同様に，攻撃者は静的汚染を行い，その後，挑戦者に二つのメッセージを送り，どちらかの暗号文を受け取る．最後に，二つのオラクル $\mathsf{OEnc}, \mathsf{OPartDec}$ にクエリし，汚染集合に対応する部分復号を受け取る．

定義 37 (adaptive-ℓ-IND-CPA 安全性)**.** PPT 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し，

$$\mathsf{Adv}^{\text{adaptive-}\ell\text{-IND-CPA}}_{\mathsf{ThPKE}}(\mathcal{A}) \coloneqq \left|\Pr\left[\mathsf{Expt}^{\text{adaptive-}\ell\text{-IND-CPA}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, n, t) = 1\right] - \frac{1}{2}\right| = \mathsf{negl}(\lambda)$$

が成り立つとき，ThPKE 方式は，セキュリティパラメータ λ ，閾値パラメータ n, t ，クエリ回数の上限 ℓ に対し，adaptive-ℓ-IND-CPA 安全であるという．ここで， $\mathsf{Expt}^{\text{adaptive-}\ell\text{-IND-CPA}}_{\mathcal{A},\mathsf{ThPKE}}$ は，図 *(3.6)* に定めるゲームである．初期状態は， $\mathsf{ctr} = 0, \mathsf{idx} = 0, \mathsf{L} = \phi$ である．また，$\mathsf{Adv}^{\text{adaptive-}\ell\text{-IND-CPA}}_{\mathsf{ThPKE}}(\mathcal{A})$ を PPT 攻撃者 $\mathcal{A}$ の優位性という．

$\mathsf{Expt}^{\text{adaptive-}\ell\text{-IND-CPA}}_{\mathcal{A},\mathsf{ThPKE}}(1^\lambda, N, t)$

$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N) \leftarrow \mathsf{Setup}(1^\lambda, N, t)$
$S \leftarrow \mathcal{A}_1(\mathsf{pp}, \mathsf{pk}) : S \subset [N] \wedge |S| \leq t$
$b \leftarrow \{0, 1\}$
$b' \leftarrow \mathcal{A}_2^{\mathsf{OEnc}, \mathsf{OChallEnc}, \mathsf{OPartDec}}(\mathsf{pk}, \{\mathsf{sk}_i\}_{i \in S})$
Output: $b = b'$

$\mathsf{OEnc}(m)$

if $m \notin \mathcal{M}$ **then return** $\perp$
$\mathsf{idx} = \mathsf{idx} + 1$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
$\mathsf{L}[\mathsf{idx}] \coloneqq \{(m, m, \mathsf{ct})\}$
Output: ct

$\mathsf{OChallEnc}(m^{(0)}, m^{(1)})$

if $(m^{(0)}, m^{(1)}) \notin \mathcal{M} \times \mathcal{M}$ **then return** $\perp$
$\mathsf{idx} = \mathsf{idx} + 1$
$\mathsf{ct}_b \leftarrow \mathsf{Enc}(\mathsf{pk}, m^{(b)})$
$\mathsf{L}[\mathsf{idx}] \coloneqq \{(m^{(0)}, m^{(1)}, \mathsf{ct}_b)\}$
Output: ct_b

$\mathsf{OPartDec}(\iota)$

$\mathsf{ctr} = \mathsf{ctr} + 1$
if $\mathsf{ctr} > \ell$ **then return** $\perp$
if $\iota > |L|$ **then return** $\perp$
$(m^{(0)}, m^{(1)}, \mathsf{ct}) \coloneqq \mathsf{L}[\iota]$
if $m^{(0)} \neq m^{(1)}$ **then return** $\perp$
$d_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}), i \in [N]$
Output: $(d_i)_{i \in [N]}$

図 3.6: ThPKE の adaptive-ℓ-IND-CPA ゲーム

ThPKE の adaptive-IND-CPA のプロトコル

Challenger		**Adversary**
$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$		$(\mathsf{pp}, \mathsf{pk})$
	$\xleftarrow{S}$	$\mathcal{A}_1(\mathsf{pp}, \mathsf{pk})$
	$\xrightarrow{\{\mathsf{sk}_i\}_{i\in S}}$	
$b \leftarrow \{0,1\}$		
	$\xleftarrow{b'}$	$\mathcal{A}_2^{\mathsf{OEnc},\mathsf{OChallEnc},\mathsf{OPartDec}}(\mathsf{pk}, \{\mathsf{sk}_i\}_{i\in S})$
win if		
$b = b'$		

各 Oracle へのクエリ順序は問わない

OEnc

$\xrightarrow{m}$	if $m \notin \mathcal{M}$ abort
	$\mathsf{idx} = \mathsf{idx} + 1$
$\xleftarrow{\mathsf{ct}}$	$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$
	$\mathsf{L}[\mathsf{idx}] = (m, m, \mathsf{ct})$

OChallEnc

$\xrightarrow{(m^{(0)}, m^{(1)})}$	if $(m^{(0)}, m^{(1)}) \notin \mathcal{M} \times \mathcal{M}$ abort
	$\mathsf{idx} = \mathsf{idx} + 1$
$\xleftarrow{\mathsf{ct}_b}$	$\mathsf{ct}_b \leftarrow \mathsf{Enc}(\mathsf{pk}, m^{(b)})$
	$\mathsf{L}[\mathsf{idx}] = (m^{(0)}, m^{(1)}, \mathsf{ct}_b)$

OPartDec

		$\mathsf{ctr} = \mathsf{ctr} + 1$
		if $\mathsf{ctr} > \ell$ abort
	$\xrightarrow{\iota}$	if $\iota > \lvert L \rvert$ abort
		$(m^{(0)}, m^{(1)}, \mathsf{ct}) = \mathsf{L}[\iota]$
		if $m^{(0)} \neq m^{(1)}$ abort
$\mathsf{PartD} = \mathsf{PartD} \cup \{\mathbf{d}\}$	$\xleftarrow{\mathbf{d}}$	$d_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$

第4章　OW-CPA から IND-CPA への変換

4.1　ランダムオラクルモデルによる変換

ランダムオラクルモデル (ROM) は，ハッシュ関数を理想的ランダム関数と想定したモデルである．ランダム関数は，任意の入力に対し，独立かつ一様ランダムな値を出力する関数である．ROM では，ランダム関数はオラクルとしてすべての参加者が利用可能である．

OW-CPA 安全な $\mathsf{ThPKE} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{PartDec}, \mathsf{Combine})$ が与えられているとき, 以下のようにして, IND-CPA 安全な $\mathsf{ThPKE}' = (\mathsf{Setup}', \mathsf{Enc}', \mathsf{PartDec}', \mathsf{Combine}')$ への変換ができる．また，この ROM 変換によって，弱選択暗号文堅牢性を満たすことが示される．

$\delta \in \mathbb{N}$ を ROM 変換のパラメータ，$F : \mathcal{M}^{\delta} \to \mathcal{M}'$ および $G : \mathcal{M}^{\delta} \to \{0,1\}^{2\lambda}$ をランダムオラクル，$\mathcal{M}$ を ThPKE の平文空間，アーベル群 $(\mathcal{M}', +)$ を ThPKE' の平文空間とする．

Setup': $(1^{\lambda}, N, t)$ を入力とし, $(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N) \leftarrow \mathsf{Setup}(1^{\lambda}, N, t)$ を出力する．

Enc': (pk, m) を入力とし（$m \in \mathcal{M}'$）, 次のように暗号文を生成する:

1. 乱数をサンプル: $\mathbf{x} \coloneqq (x_1, \ldots, x_{\delta}) \leftarrow U(\mathcal{M}^{\delta})$,
2. $c_0 = m + F(\mathbf{x}), c_{\delta+1} = G(\mathbf{x})$ を計算,
3. 各 $j \in [\delta]$ に対し，$c_j \leftarrow \mathsf{Enc}(\mathsf{pk}, x_j)$ を計算,
4. $\mathsf{ct} \coloneqq (c_0, c_1, \ldots, c_{\delta}, c_{\delta+1}) = (m + F(\mathbf{x}), \mathsf{Enc}(x_1), \ldots, \mathsf{Enc}(x_{\delta}), G(\mathbf{x}))$ を暗号文として出力.

$\mathsf{PartDec}'$: $(\mathsf{sk}_i, \mathsf{ct})$ を入力とし（$i \in [N]$），次のように部分復号を出力する：

1. 任意の $j \in [\delta]$ に対し，$d_{ij} \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, c_j)$ を計算,
2. $\mathbf{d}_i \coloneqq (d_{ij})_{j \in [\delta]}$ を部分復号として出力.

$\mathsf{Combine}'$: $((\mathbf{d}_i)_{i \in S}, \mathsf{ct})$ を入力とし，次のように平文を出力する．

1. $j \in [\delta]$ に対し，$x_j' \leftarrow \mathsf{Combine}(\{d_{ij}\}_{i \in S}, c_j)$,
2. $\mathbf{x}' \coloneqq (x_1', \ldots, x_{\delta}')$ とする．

3. $m' \coloneqq c_0 - F(\mathbf{x}')$ を計算,

4. $c_{\delta+1} = G(\mathbf{x}')$ なら m' を出力，それ以外なら，$\perp$ を出力.

この変換によって，平文と暗号文のビットサイズ比は,

$$\frac{|\mathsf{ct}|}{|m|} = \frac{|m| + \delta \cdot |c| + 2\lambda}{|m|}$$

となる．ここで，$|c|$ は ThPKE による暗号文である．つまり，変換パラメータ δ に応じて，暗号文のサイズは増加する.

補題 38 (復号の正当性 [BS23]). *ROM* 変換によって構成された ThPKE' は ThPKE の復号の正当性を満たし，かつ $\delta = \mathsf{poly}(\lambda)$ のとき，復号の正当性を満たす.

補題 39 (ThPKE' の弱選択暗号文堅牢性 [BS23]). ThPKE' は弱選択暗号文堅牢性を満たす.

定理 40 (安全性評価 [BS23]). $\delta, \ell \in \mathbb{N}$ とする．ThPKE が $(\ell\delta)$-OW-CPA 安全ならば，ThPKE' は *ROM* 変換によって， adaptive-ℓ-IND-CPA 安全となる．具体的には，任意の adaptive-ℓ-IND-CPA 安全な攻撃者 $\mathcal{A}$ が最大 q_F 回のクエリをランダムオラクル F に送り，q_c 回のクエリを $\mathsf{OChallEnc}'$ を送ると,

$$\mathsf{Adv}^{\text{adaptive-}\ell\text{-IND-CPA}}_{\mathsf{ThPKE}'}(\mathcal{A}) \leq q_c \cdot q_F^{1/\delta} \cdot \mathsf{Adv}^{(\ell\delta)\text{-OW-CPA}}_{\mathsf{ThPKE}}(\mathcal{B})$$

を満たす $(\ell\delta)$-OW-CPA ゲームに対する攻撃者 $\mathcal{B}$ が存在する.

第5章　LSS による ThPKE の構成

この章では，[BS23] の手法を PKE，特に，Regev 暗号に適用する方法を述べる．$\{0,1\}$-LSSS に基づき，OW-CPA 安全な ThPKE 方式を構成する．

5.1　PKE の線形復号

5.2　strong-$\{0,1\}$-reconstruction による構成

LSSS 構成で以下のものを使う．

- D_{flood}: β_{flood} で上界が与えられた $\mathbb{Z}_q$ 上のノイズ分布．
- D_{sim}: $\mathbb{Z}_q$ 上のノイズ分布．ある $a \in (1,\infty)$ ，$\varepsilon_{\mathsf{RD}_a} > 1$ ，任意の $|B| \leq \beta_{\mathsf{fhe}}$ を満たす B に対し $\mathsf{RD}_a(D_{\mathsf{sim}} \| D_{\mathsf{flood}} + B) \leq \varepsilon_{\mathsf{RD}_a}$ となる．
- LSS: strong-$\{0,1\}$-reconstruction 性の (t,N)-線形秘密分散方式 $\mathsf{LSS} = (\mathsf{Share}, (\mathsf{Rec}_S)_{S\subset[N]})$．パラメータは $L, \tau_{\max}, \tau_{\min}$ で，シェアは $\mathbb{Z}_q^L$ の元である．
- Regev: メッセージ空間 $\mathcal{M} \subseteq \mathbb{Z}_q$，暗号文空間 $\mathbb{Z}_q$ の OW-CPA 安全な方式，$\mathsf{Regev} = (\mathsf{Setup}', \mathsf{Enc}, \mathsf{Dec})$ で，ある $\beta_{\mathsf{pke}} < q/(2p) - \tau_{\min}\beta_{\mathsf{flood}}$ となる無視可能な値 ε に対して $(\beta_{\mathsf{pke}}, \varepsilon)$-線形復号性を行う．[1]

$\mathsf{ThPKE} := (\mathsf{Setup}, \mathsf{Enc}, \mathsf{PartDec}, \mathsf{Combine})$ の Enc は Regev のアルゴリズムを引き継ぎ，新しく Setup, PartDec, Combine を定義する．

[1] e_{flood} 分だけ許容できるノイズの範囲が小さくなる．strong-$\{0,1\}$-reconstruction より，復号できる最小のシェア数だけ考えればよい．

$\mathsf{Setup}(1^\lambda, n, t)$

$(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}'(1^\lambda)$

// $\mathsf{sk} \in (\mathbb{Z}_q^n)^L$

$(\mathsf{sk}_1, \ldots, \mathsf{sk}_N) \leftarrow \mathsf{LSS.Share}(\mathsf{sk})$

// $\mathsf{sk}_i \in \mathbb{Z}_q^n$

Output: $(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$

$\mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$

$j \in [L]$ に対し，$e_i \leftarrow D_{\mathsf{flood}}$

// $\mathsf{sk}_i = (\mathsf{sk}_{i,1}, \ldots, \mathsf{sk}_{i,L}) \in (\mathbb{Z}_q)^L$

$\mathbf{d}_{i,j} \leftarrow \langle \mathsf{ct}, \mathsf{sk}_{i,j} \rangle + e_{i,j}$

Output: $\mathbf{d}_i \leftarrow (\mathbf{d}_{i,1}, \ldots, \mathbf{d}_{i,L})$

$\mathsf{Combine}(\{\mathbf{d}_i\}_{i \in S}, \mathsf{ct})$

$y \leftarrow \mathsf{Rec}_S((\mathbf{d}_i)_{i \in S})$

Output: $\lfloor (p/q) \cdot y \rceil$

図 5.1: ThPKE 構成のため，新しく定義したアルゴリズム

定理 41. 図 *(5.1)* の構成は，復号の正当性を満たす．

証明は (A.1).

定理 42. 任意の攻撃者 $\mathcal{A}$ が，平文空間 $\mathcal{M}$ の ℓ-OW-CPA 安全な ThPKE 方式を破るならば，IND-CPA 安全な PKE に対する攻撃者 $\mathcal{B}$ が存在し，以下が成り立つ：

$$\mathsf{Adv}^{\ell\text{-OW-CPA}}_{\mathsf{ThPKE}}(\mathcal{A}) \leq \left[(\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{PKE}}(\mathcal{B}) + 2^{-\log_2(|M|)}) \cdot \varepsilon_{\mathsf{RD}_a}^{\ell(NL - \tau_{\max})} \right]^{(a-1)/a} + \ell\varepsilon$$

証明. 以下に示す，G_0 から G_4 のゲーム変換で示す．

ゲーム G_0　ℓ-OW-CPA 安全の定義と同じ．攻撃者 $\mathcal{A}$ の得られる情報は

$$\text{view} = (\mathsf{pp}, \mathsf{pk}, \{\mathsf{sk}_i\}_{i \in S}, \mathsf{CT}, \mathsf{ChallCT}, \mathsf{PartD})$$

である．

各部分復号クエリにおいて，攻撃者 $\mathcal{A}$ はインデックス ι を入力し，$(d_i)_{i \in [n]}$ を受け取る．攻撃者が $t+1$ 個以上の部分復号復号シェアを得ると，m を reconstruct できる．よって，

$$\mathsf{Adv}^{\ell\text{-OW-CPA}}_{\mathsf{ThPKE}}(\mathcal{A}) = \mathsf{Adv}^{G_0}_{\mathsf{ThPKE}}(\mathcal{A})$$

ゲーム G_1　$S \subset [N]$ を汚染集合とし，$S_L = \{(i,j)\}_{i \in S, j \in [L]}$ を対応するシェアとする．$T \supseteq S_L$ を最大無効なシェア要素の集合として固定する．部分復号の計算方法を以下のように変更する:

1. $(i,j) \in T$ の場合，$\tilde{\mathbf{d}}_{i,j} = \langle \mathsf{ct}, \mathsf{sk}_{i,j} \rangle$,
2. $(i,j) \in ([N] \times [L]) \setminus T$ の場合，$T_{i,j} \subseteq T \cup \{(i,j)\}$ を最小有効シェアの集合とし，次のように計算する：$\tilde{\mathbf{d}}_{(i,j)} = \langle \mathsf{ct}, \mathsf{sk} \rangle - \sum_{(k,l) \in T_{i,j} \setminus \{(i,j)\}} \tilde{\mathbf{d}}_{k,l}$
3. $i \in [N]$ に対して，$\mathbf{d}_i = \tilde{\mathbf{d}}_i + \mathbf{e}_i$　$(\mathbf{e}_i \leftarrow D_{\mathsf{flood}})$ を計算する．

ゲーム G_2　部分復号を出力する前に，線形復号性を満たすか確認する：

$$\langle \mathsf{ct}, \mathsf{sk} \rangle = \lfloor q/q \rceil \cdot m + e_{\mathsf{ct}}$$

ただし, e_{ct} は $\|e_{\mathsf{ct}}\|_\infty \leq \beta_{\mathsf{pke}}$ を満たすものとする．この条件を満たさない場合, ゲームは abort される（中止）.

ゲーム G_3　このゲームでは，無効集合 T に属さないシェアのノイズをシミュレーションされたものに置き換える:

1. G_1 のステップ (2) を変更: $(i,j) \in ([N] \times [L]) \setminus T$ の場合，$\tilde{\mathbf{d}}_{(i,j)} = \left\lfloor \frac{q}{p} \cdot m \right\rceil - \sum_{(k,l) \in T_{i,j} \setminus \{(i,j)\}} \tilde{\mathbf{d}}_{k,l}$.
2. G_1 のステップ (3) ノイズのサンプリング方法を以下のように変更：
   - $(i,j) \in T$ の場合，$\mathbf{e}_{i,j} \leftarrow D_{\mathsf{flood}}$.
   - $(i,j) \notin T$ の場合，$\mathbf{e}_{i,j} \leftarrow D_{\mathsf{sim}}$.

ゲーム G_4　秘密鍵のシェアの生成方法を変更する：

1. $(\mathsf{sk}_1^{'}, \ldots, \mathsf{sk}_N^{'}) \leftarrow \mathsf{LSS.Share}(0)$
2. 攻撃者 $\mathcal{A}$ に対して, 汚染された参加者 $S \subseteq [N]$ に属する密鍵のシェア $\{\mathsf{sk}_i^{'}\}_{i \in S}$ を与える.

ゲーム G_5　OChallEnc を OChallEnc$^{'}$ に置き換える.
　OChallEnc$^{'}$ では，２つの独立したメッセージ m と $m^{'}$ をサンプリングする．m はチャレンジメッセージリスト ChallM に追加され，$m^{'}$ の暗号化がチャレンジ暗号文リスト ChallCT に追加される.

OChallEnc'

$\mathrm{idx} = \mathrm{idx} + 1$
$m, m^{'} \leftarrow M$
$\mathsf{ChallM} = \mathsf{ChallM} \cup \{m\}$
$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m^{'})$
$\mathsf{ChallCT} = \mathsf{ChallCT} \cup \{\mathsf{ct}\}$
$L[\mathrm{idx}] \coloneqq \{(1, m, \mathsf{ct})\}$ **return** ct

---

□

補題 43. ゲーム G_0 と G_1 における任意の PPT 攻撃者 $\mathcal{A}$ に対して,

$$\mathsf{Adv}^{G_0}_{\mathsf{ThPKE}}(\mathcal{A}) = \mathsf{Adv}^{G_1}_{\mathsf{ThPKE}}(\mathcal{A})$$

が成立する.

証明. 最大無効集合 T に属するすべてのシェアは, G_0 と同様の方法で部分復号を行い, T に属さないシェアは, 正しい秘密鍵による復号 $\langle \mathsf{ct}, \mathsf{sk} \rangle$ と無効集合の部分復号によって決定的に決まるため. G_1 における攻撃者 $\mathcal{A}$ の視点は, LSS の $\{0,1\}$-LSSS により, G_0 における視点と同一である.

$$\mathsf{Adv}^{G_0}_{\mathsf{ThPKE}}(\mathcal{A}) = \mathsf{Adv}^{G_1}_{\mathsf{ThPKE}}(\mathcal{A})$$

□

補題 44. ゲーム G_1, G_2 における任意の PPT 攻撃者 $\mathcal{A}$ に対し,

$$\mathsf{Adv}^{G_1}_{\mathsf{ThPKE}}(\mathcal{A}) \leq \mathsf{Adv}^{G_2}_{\mathsf{ThPKE}}(\mathcal{A}) + \ell\varepsilon$$

が成り立つ.

証明. PKE の (β, ε)-線形復号性により, 暗号文が復号時に出力する誤差は確率 ε で許容範囲を超える. よって, ブールの不等式より, ℓ 回のクエリについて, 許容範囲外の誤差が発生する確率は上式のように制限される. □

補題 45. ゲーム G_2, G_3 における PPT 攻撃者 $\mathcal{A}$ に対し,

$$\mathsf{Adv}^{G_2}_{\mathsf{ThPKE}}(\mathcal{A}) \leq (\mathsf{Adv}^{G_3}_{\mathsf{ThPKE}}(\mathcal{A}) \cdot \varepsilon_{\mathsf{RD}_a}^{\ell(NL-\tau_{\max})})^{(a-1)/a}$$

が成り立つ. ここで, $\tau_{\max}$ は LSS の最大無効集合の最小サイズを表す.

証明. ゲーム G_2 と G_3 における, 攻撃者の視点間の Rényi Divergence を計算する. 各視点は, 攻撃者 $\mathcal{A}$ の内部コインと

$$\mathsf{view} = (\mathsf{pp}, \mathsf{pk}, \{\mathsf{sk}_i\}_{i \in S}, \mathsf{CT}, \mathsf{ChallCT}, \mathsf{PartD})$$

から構成される. ゲーム G_2, G_3 における view の分布をそれぞれ D_2, D_3 とする.

部分復号クエリは適応的に行われるため, η 番目のクエリは, それ以前の $\mathsf{OEnc}, \mathsf{OChallEnc}, \mathsf{OPartDec}$ に対するクエリの応答に依存する. 一方, クエリは view と内部コインによって, 決定的であるため, D_2', D_3' を η 番目のクエリを除いた分布とすると, 補題 (17) のデータ処理不等式より,

$$\mathsf{RD}_a(D_2 \| D_3) \leq \mathsf{RD}_a(D_2' \| D_3')$$

が成り立つ.

D_2', D_3' は, $(i,j) \notin T$ に対する部分復号 $\mathbf{d}^{\eta}_{i,j}$ の計算方法のみ異なる. ゲーム G_2 では,

$$\mathbf{d}^{\eta}_{i,j} = \langle \mathsf{ct}^{\eta}, \mathsf{sk} \rangle - \sum_{(k,l) \in T_{i,j} \setminus \{(i,j)\}} \tilde{\mathbf{d}}_{k,l} + \mathbf{e}_{i,j} \quad \text{where} \quad \mathbf{e}_{i,j} \leftarrow D_{\mathsf{flood}}$$

ゲーム G_3 では,

$$\mathbf{d}_{i,j}^{\eta} = \lfloor q/p \cdot m^{\eta} \rceil - \sum_{k,l \in T_{i,j} \setminus \{(i,j)\}} \tilde{\mathbf{d}}_{k,l} + \mathbf{e}_{i,j} \quad \text{where} \quad \mathbf{e}_{i,j} \leftarrow D_{\mathsf{sim}}$$

である．つまり，ゲーム G_2 のノイズ項 $e_{\mathsf{ct}} + e_{\mathsf{flood}}$ を e_{sim} に置き換えた．したがって，攻撃者の視点では $nL - |T|$ 個 の $(i,j) \notin T$ ペアに対する $\mathbf{d}_{i,j}^{\eta}$ のサンプリング方法が G_2 から G_3 に変更された．

$\mathsf{RD}_a(D_2^{'} \| D_3{'})$ を計算するため，次を計算する．

$$\mathsf{RD}_a(((e_1 + D_{\mathsf{flood}})^{nL-|T|}, \ldots, (e_\ell + D_{\mathsf{flood}})^{nL-|T|}) \| D_{\mathsf{sim}}^{\ell(nL-|T|)})$$

補題（18）に $N = \ell(nL - |T|), D_1 = D_{\mathsf{flood}}, D_2 = D_{\mathsf{sim}}$ を適用することで,

$$\mathsf{RD}_a(D_2^{'} \| D_3^{'}) \leq \varepsilon_{\mathsf{RD}_a}^{\ell(nL-|T|)}$$

を得る．つまり，$\mathsf{RD}_a(D_2 \| D_3) \leq \varepsilon_{\mathsf{RD}_a}^{\ell(NL-|T|)}$ となるので，$\mathsf{RD}_a(D_2 \| D_3)$ に Rényi Divergence の確率保存を適用することで，示せた． □

補題 46. ゲーム G_3 と G_4 における，任意の PPT 攻撃者 $\mathcal{A}$ に対し,

$$\mathsf{Adv}_{\mathsf{ThPKE}}^{G_3}(\mathcal{A}) = \mathsf{Adv}_{\mathsf{ThPKE}}^{G_4}(\mathcal{A})$$

が成り立つ.

証明. 定義 (22) のプライバシーによって, G_3 と G_4 は識別不能である．したがって,

$$\mathsf{Adv}_{\mathsf{ThPKE}}^{G_3}(\mathcal{A}) = \mathsf{Adv}_{\mathsf{ThPKE}}^{G_4}(\mathcal{A})$$

となる． □

補題 47. ゲーム G_4 と G_5 における任意の PPT 攻撃者 $\mathcal{A}$ に対して,

$$\mathsf{Adv}_{\mathsf{ThPKE}}^{G_4} \leq \mathsf{Adv}_{\mathsf{ThPKE}}^{G_5} + |\mathsf{ChallM}| \cdot \mathsf{Adv}_{\mathsf{PKE}}^{\text{IND-CPA}}$$

が成り立つ.

証明. ベースとなる PKE 方式の IND-CPA 安全を仮定すると，$\mathsf{OChallEnc}^{'}$ への各クエリに対し，攻撃者 $\mathcal{A}$ の視点は G_4 と G_5 を計算量的に区別できない．従って，$|\mathsf{ChallM}|$ 回のクエリ数を考慮すると，示せる． □

補題 48. ゲーム G_5 において，任意の PPT 攻撃者 $\mathcal{A}$ に対して,

$$\mathsf{Adv}_{\mathsf{ThPKE}}^{G_5} \leq 2^{-\log_2(|M|)}$$

が成り立つ.

証明. ゲーム G_5 における $\mathcal{A}$ の視点を

$$\mathsf{view} = (\mathsf{pp}, \mathsf{pk}, \{\mathsf{sk}_i\}_{i\in S}, \mathsf{CT}, \mathsf{ChallCT}, \mathsf{PartD})$$

とする．ここで，ChallM に含まれるすべてのチャレンジメッセージは， ChallCT に含まれるチャレンジ暗号文と独立している．また，秘密鍵シェア $\{\mathsf{sk}_i\}_{i\in S}$ は秘密鍵 sk ，チャレンジメッセージ ChallM ，PartD と独立しており，公開パラメータ pp, 公開鍵 pk, 暗号文が保存された CT は ChallM と独立である．したがって，$\tilde{\mathrm{H}}_\infty(m \mid \mathsf{view}) = \tilde{\mathrm{H}}_\infty(m)$ である．以上により，

$$\mathsf{Adv}^{G_5}_{\mathsf{ThFHE}}(\mathcal{A}) \leq \sum_{m\in\mathsf{ChallM}} 2^{-\tilde{\mathrm{H}}_\infty(m\,|\,\mathsf{view})} = \sum_{m\in\mathsf{ChallM}} 2^{-\tilde{\mathrm{H}}_\infty(m)}$$

また，各 $m \in$ ChallM はメッセージ空間 $\mathcal{M}$ 上で一様ランダムにサンプリングされているため，任意のメッセージ $m \in \mathcal{M}$ の出現確率は，$\Pr[m] = \frac{1}{|\mathcal{M}|}$ である．従って，定義（10）より，

$$\begin{aligned}\tilde{\mathrm{H}}_\infty(m) &= -\log_2(\max_{m\in\mathcal{M}} \Pr[m]) \\ &= -\log_2(\frac{1}{|\mathcal{M}|}) \\ &= \log_2(|\mathcal{M}|)\end{aligned}$$

であるから，

$$\mathsf{Adv}^{G_5}_{\mathsf{ThPKE}}(\mathcal{A}) \leq |\mathsf{ChallM}| \cdot 2^{-\log_2(|\mathcal{M}|)}$$

が成り立つ. □

つまり，定理 (36) と，定理 (42) より，図 ((5.1)) による構成で作られた ThPKE は，

$$\begin{aligned}\mathsf{Adv}^{\ell\text{-OW-CPA}}_{\mathsf{ThPKE}}(\mathcal{A}) &\leq \left[(\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Regev}}(\mathcal{B}) + 2^{-\log_2(|M|)}) \cdot \varepsilon^{\ell(NL-\tau_{\max})}_{\mathsf{RD}_a}\right]^{(a-1)/a} + \ell\varepsilon \\ &\leq \left[(\varepsilon^{\mathsf{LWE}} + 2^{-\frac{m-(n+1)\log q}{2}-1} + 2^{-\log_2(|M|)}) \cdot \varepsilon^{\ell(NL-\tau_{\max})}_{\mathsf{RD}_a}\right]^{(a-1)/a} + \ell\varepsilon\end{aligned}$$

を満たす.

5.3 分散方法による評価

42 の式を 2 章で紹介した (t, N) 線形秘密分散の加法 (3)，複製 (4) の 2 通りで評価する．分散が影響を与えるのは，$\varepsilon^{\ell(NL-\tau_{\max})}_{\mathsf{RD}_a}$ の項である．

加法の場合　$L = 1, \tau_{\max} = N - 1$ より，

$$NL - \tau_{\max} = n \cdot 1 - (N - 1) = 1$$

したがって，$\mathcal{O}(1)$ となる．

複製の場合　$L = \binom{N-1}{t}, \tau_{\max} = (N - t)(\binom{N}{t} - 1)$ より，

$$NL - \tau_{\max} = N\binom{N-1}{t} - (N - t)(\binom{N}{t} - 1)$$

この式は，t の値が 1 に近づくほど，$\varepsilon_{\mathsf{RD}}$ の影響を大きくし，$N - 1$ に近づくほど，影響を小さくなる．例えば，$t = 1$ の場合，$NL - \tau_{\max} = N - 1$ となり，$\varepsilon_{\mathsf{RD}}^{\ell(N-1)}$ となる．$t = N - 1$ の場合，$NL - \tau_{\max} = 1$ となり，$\varepsilon_{\mathsf{RD}}^{\ell}$ となる．

つまり，復号に必要な人数（閾値）を下げるほど，現実のノイズとシミュレーションしたノイズの差 $\mathsf{RD}_a(D_{\mathsf{flood}} + B \| D_{\mathsf{sim}}$ （とその上限 $\varepsilon_{\mathsf{RD}}$）の影響が大きくなり，ThPKE の ℓ-OW-CPA ゲームへの優位性が無視できなくなる．統計距離でこれらのゲーム間の優位性を評価していた場合は，さらに大きな値となる．

第6章　おわりに

本研究では, Regev[?] によって提案された公開鍵暗号方式を, Boudgoust, Scholl[BS23] によって提案された技法によって閾値型暗号方式を構成した．[BS23] では，完全準同型暗号に対して Rényi Divergence を導入し，ノイズ評価を改善したが，その方式を通常の公開鍵暗号に適用した.

6.1　今後の展望

今後の展望として，以下のものが考えられる．
本研究では，Regev 暗合を使って ThPKE を構築したが,

- ThPKE の OW-CPA 安全性から IND-CPA 安全性への変換で，本研究はランダムオラクルモデル（ROM）を使った．しかし，ROM は理想的なハッシュ関数の存在という強い仮定を置く．したがって，ThPKE に特化した，標準モデルによる効率的な変換を構築することを目指す.

- 本研究での閾値型暗号方式(ThPKE, ThFHE)の構成いおいて, Rényi Divergence の上限値が安全性に大きな影響を与えた.

  1. より最適なノイズ分布を見つける
  2. 効率的分散方式（$\tau_{\max}$ を抑える）を見つける

  ことを目指す.

- Peikert, Vaikuntanathan, Waters による Regev 暗合の改良版 [PVW08] を使用し，より効率的かつ，平文空間を拡張した ThPKE を構築する.

- Gentry, Sahai, Water による完全準同型暗号方式 [GSW13] をしようし, ThFHE を構築する.

- Chillotti らによる [GSW13] を改良した FHE [CGGI16] によって，ThFHE を構築する.

謝辞

本研究を進めるにあたり，多大なるご指導とご助言を賜りました藤﨑英一郎教授に深く感謝申し上げます．常に的確なご指導をいただき，研究の方向性を見失うことなく進めることができました．

また，藤﨑研究室の皆様には，日々の議論や励ましを通じて多くの刺激をいただきました．貴重な意見や助言を共有してくださり，研究活動をより充実したものにすることができました．特に，川野さん，雨宮さんとは互いに生活リズムを整え，研究室通いを習慣を確立できたことで，途中で挫折することなく研究に専念できました．お二人の支えに深く感謝いたします．

最後に，これまで支えてくれた家族や友人に深く感謝いたします．皆様の支えがなければ，この研究を成し遂げることはできませんでした．

ここに感謝の意を表し，謝辞とさせていただきます．

参考文献

[BD10] Rikke Bendlin and Ivan Damgård. Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems. In *Proceedings of the 7th International Conference on Theory of Cryptography*, TCC'10, page 201–218, Berlin, Heidelberg, 2010. Springer-Verlag.

[BGG+18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. Threshold cryptosystems from threshold fully homomorphic encryption. In *Advances in Cryptology – CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I*, page 565–596, Berlin, Heidelberg, 2018. Springer-Verlag.

[Bla99] G. R. Blakley. Safeguarding cryptographic keys. *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1899.

[BLRL+15] Shi Bai, Tancrède Lepoint, Adeline Roux-Langlois, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the rényi divergence rather than the statistical distance. *Journal of Cryptology*, 31:610 – 640, 2015.

[BS23] Katharina Boudgoust and Peter Scholl. Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. Cryptology ePrint Archive, Paper 2023/016, 2023.

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. Cryptology ePrint Archive, Paper 2016/870, 2016.

[Des87] Yvo Desmedt. Society and group oriented cryptography: A new concept. In *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, CRYPTO '87, page 120–127, Berlin, Heidelberg, 1987. Springer-Verlag.

[DF89] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. In *Annual International Cryptology Conference*, 1989.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, January 2008.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. *IACR Cryptol. ePrint Arch.*, 2013:340, 2013.

[ISN89] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan Part Iii-fundamental Electronic Science*, 72:56–64, 1989.

[LSS14] Adeline Langlois, Damien Stehle, and Ron Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. Cryptology ePrint Archive, Paper 2014/487, 2014.

[NIS22] NIST. PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates. `https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4#fourth-round`, 2022.

[NIS24a] NIST. Multi-Party Threshold Cryptography. `https://csrc.nist.rip/Projects/threshold-cryptography`, 2024.

[NIS24b] NIST. NIST Releafses First 3 Finalized Post-Quantum Encryption Standards. `https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards`, 2024.

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *Proceedings of the 28th Annual Conference on Cryptology: Advances in Cryptology*, CRYPTO 2008, page 554–571, Berlin, Heidelberg, 2008. Springer-Verlag.

[RD78] Ronald L. Rivest and Michael L. Dertouzos. On data banks and privacy homomorphisms. 1978.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery.

[SE94] C. P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Math. Program.*, 66(2):181–199, September 1994.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[vEH14] Tim van Erven and Peter Harremos. Rényi divergence and kullback-leibler divergence. *IEEE Transactions on Information Theory*, 60(7):3797–3820, 2014.

[青安 19] 青野良範 and 安田雅哉. 格子暗号解読のための数学的基礎, 2019.

[敦剛 19] 高安 敦 and 高木 剛. 格子簡約アルゴリズムを用いた公開鍵暗号の安全性評価. **応用数理**, 29(1):12–19, 2019.

付 録A

A.1　復号の正当性

図 (5.1) の構成は，復号の正当性を満たす．

証明. $S \subset [N]$ を $|S| > t$ を満たす集合とし，正しく生成された暗号文 ct を入力する．$i \in S$ に対し，$\mathbf{d}_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$ とする．ただし，$(\mathsf{sk}_1, \ldots, \mathsf{sk}_N) = \mathsf{Share}(\mathsf{sk})$ である．

LSS の strong $\{0,1\}$-reconstruction property と，有効集合 S に対し，

$$\mathsf{Rec}_S\big((\mathsf{sk}_i)_{i\in S}\big) = \sum_{(i,j)\in T} \mathsf{sk}_{i,j} = \mathsf{sk}$$

となる最小有効シェア $T \subseteq S \times [L]$ が存在する．

これにより，

$$\begin{aligned}
\mathsf{Combine}(d_{i\in S}\}, \mathsf{ct}) &= \left\lfloor (p/q) \cdot (\langle \mathsf{ct}, \mathsf{sk}\rangle + \sum_{(i,j)\in T} \mathbf{e}_{i,j}) \right\rceil \\
&= \left\lfloor (p/q) \cdot \Big(\lfloor (q/p)m \rceil + e_{\mathsf{ct}} + \sum_{(i,j)\in T} \mathbf{e}_{i,j}) \right\rceil \\
&= \left\lfloor (p/q) \cdot \Big((q/p)m + e_{\mathsf{rnd}} + e_{\mathsf{ct}} + \sum_{(i,j)\in T} \mathbf{e}_{i,j} \Big) \right\rceil \\
&= m + \left\lfloor (p/q) \cdot \big(e_{\mathsf{rnd}} + e_{\mathsf{ct}} + \sum_{(i,j)\in T} \mathbf{e}_{i,j} \big) \right\rceil .
\end{aligned}$$

が得られる．ここで，e_{ct} を暗号文誤差，e_{rnd} は係数が $1/2$ 以下の丸め込み誤差多項式である．$e = e_{\mathsf{rnd}} + e_{\mathsf{ct}} + \sum_{(i,j)\in T} \mathbf{e}_{i,j}$ とすると，PKE の $(\beta_{\mathsf{pke}}, \varepsilon)$-線形復号性により，確率 ε を除き，

$$\|e\| \le 1/2 + \beta_{\mathsf{pke}} + |T| \cdot \beta_{\mathsf{flood}}$$

が成り立つ．

ここで， $\beta_{\mathsf{fhe}} \leq q/(2p) - \tau_{\min}\beta_{\mathsf{flood}} - 1$ かつ，T が最小有効集合である，すなわち，$|T| \leq \tau_{\min}$ より，

$$\begin{aligned}\beta_{\mathsf{fhe}} &\leq q/(2p) - \tau_{\min}\beta_{\mathsf{flood}} - 1 \\ &= q/(2p) - |T|\beta_{\mathsf{flood}} - 1\end{aligned}$$

すなわち，

$$\begin{aligned}||e||_\infty &\leq 1/2 + \beta_{\mathsf{pke}} + |T| \cdot \beta_{\mathsf{flood}}, \\ &\leq 1/2 + q/(2p) - |T|\beta_{\mathsf{flood}} - 1 + |T|\beta_{\mathsf{flood}} \\ &\leq -1/2 + q/(2p) \\ &< q/(2p)\end{aligned}$$

が成り立つ.

$\|e\|_\infty < q/(2p)$ のとき，

$$\lfloor (p/q)e \rceil < \lfloor (p/q)(q/(2p)) \rceil = \lfloor 1/2 \rceil = 0.$$

より，誤差項 e は 0 に丸め込まれ，正しいメッセージ m が得られる. □