部分復号可能な格子ベース暗号の提案*

安田貴徳† 穴田啓晃† 櫻井幸一†‡

†九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22
{yasuda,anada}@isit.or.jp

‡九州大学大学院システム情報科学研究院
819-0395 福岡市西区元岡 744

あらまし 一つの平文を多数の受信者に対し暗号化し送付する状況において，暗号文の復号部分を受信者に応じ指定可能な公開鍵暗号方式が部分復号方式として知られている．本稿では，部分復号方式であって，暗号化は 1 個の公開鍵で行い，復号は公開鍵に紐付けられた複数の秘密鍵でそれぞれ部分復号を行う方式を提案する．本提案方式は，複数の暗号の組み合わせでなく，多変数 NTRU 暗号を用いた単一の暗号スキームによりこの機能を実現することを特徴とする．本提案方式により，受信者が購入する秘密鍵に応じコンテンツの開示部分を指定できるコンテンツ配信を実現できる．特徴として，コンテンツの暗号化処理は 1 回のみでよい．

A Lattice-based Encryption Allowing Partial-Decryption

Takanori Yasuda† Hiroaki Anada† Kouichi Sakurai†‡

†Institute of Systems, Information Technologies and Nanotechonologies.
2-1-22 Fukuoka SRP Center Building 7F, Momochihama, Sawara-ku, Fukuoka 814-0001, JAPAN

‡Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395 , JAPAN

Abstract In the case that one message is encrypted and sended to several receivers, there already exist techniques that designated recievers can decrypt only partial information of the message. In this paper, we propose a scheme which has one time encryption process (for both whole and partial message) and easy key management.

1 はじめに

部分復号方式 (Partial Decryption) [2, 6, 10] は，一つの暗号文を復号できるユーザを指定可能な公開鍵暗号の方式の一つであり，暗号文の復号可能部分を受信者ごとに設定可能であることを特徴とする．つまり，権限の異なる受信者が多数いる状況を想定し，一つのコンテンツを権限の異なる複数の利用者が閲覧できるようにする方法である．このような部分復号方式が必要とされる背景として，例えば有償の文献や動画配信サービスにおいて，コンテンツへの閲覧許可にレベルが設定され，閲覧権限に応じて開示を制御するケースが考えられる．

1.1 平文分割暗号化による部分復号方式

部分復号を実現する方式として，想定される複数の受信者に応じ一つの平文を予め分割し，各々の平文の断片を各受信者の公開鍵で暗号化する方式がある．また，別の方式として，送信

*この研究は総務省戦略的情報通信研究開発推進事業（SCOPE）平成 27 年度イノベーション創出型研究開発フェーズ II（no. 0159-0016）の委託の一環である．

者が秘密鍵と公開鍵のペアを複数生成し，予め分割した平文の各々の断片を各々の公開鍵で暗号化する方式がある．上記二つの方式に工夫を加えたものとして，処理効率を追求した研究がある [2].

1.2 多重暗号化による部分復号方式

部分復号方式を実現する別の方針として，複数の公開鍵を利用する多重暗号化がある [6]．すなわち，復号可能なメッセージの部分情報が n 通りある場合, 暗号送信者は n 個の公開鍵を使って暗号文を作る．部分復号を行う受信者は事前に教えられた複数の秘密鍵を用いて，暗号文の部分情報を手に入れることができる．知っている秘密鍵の個数が多いほどより完全に近いメッセージを手に入れることができる．この方法は共通鍵暗号でも用いることができ，公開鍵暗号を用いた部分復号方式は，共通鍵を用いた部分復号方式の一時的な鍵（セッション鍵）の生成に用いるという方法もある．なお，共通鍵暗号を用い，第三者向けにはマスク処理を行い参照不可情報を作り込む方式も知られている [8, 10]. 共通鍵暗号であるため，適用には前提があるものの，処理効率は良い.

1.3 墨塗り署名 [1]

暗号化とは異なるが，データを部分的に秘匿する方法として墨塗り署名が盛んに研究されてきた [1, 4, 3, 11]．墨塗り署名は，通常のデジタル署名の機能（真正性の証明）と両立する形で，秘匿すべき情報の削除（墨塗り）を，署名後に（改ざんとみなされずに）行う機能を併せ持つ．しかしながら墨塗り箇所の復元ができないので，部分復号（及び部分暗号化）とは異なる．

1.4 秘密分散法と電子割符 [13, 9]

部分復号と類似の趣旨の技術として，秘密分散法 [13] とこれを用いた電子割符 [9] がある．すなわち，分配したシェアを集めて初めて全体の（意味ある）データが復元される点である．しかしながら，部分復号では復号した各部分が元のデータの部分をなしている．これに対し，秘密分散法では各シェアから元のデータの部分が得られるわけではない．この点，部分復号と秘密分散法（及び電子割符）は異なる．

1.5 提案方式

本稿では，どのような部分復号に対する暗号文も 1 つの公開鍵のみで構成できる暗号スキームを提案する．提案方式は代数的構造を積極的に活用することで，より柔軟な使用法を可能とする．例えば，分権譲渡された 2 つの異なる秘密鍵（復号権限）があるとし，それらの情報を両方入手できたとする．そのとき，それらの結合あるいは共通部分にあたる秘密鍵を新たに生成できる場合があり，それらの鍵も譲渡することができる．結合に関しては 4.2 節で，共通部分に関しては 4.1 節で，具体的な場合を用いて活用方法を説明する.

このような公開鍵暗号を実現する方法として，格子ベース暗号 NTRU とさらにそれを拡張した多変数版の NTRU を利用する．具体的には多変数 NTRU の鍵や暗号文から（1 変数）NTRU の鍵や暗号文などを対応させる．このとき，移される情報は限定的となるため，部分的な情報だけが復号可能となる．この方法は変数を増やすことで柔軟な部分情報の暗号化が可能となる．例えば，部分情報とさらにその部分情報を暗号化したり，異なる複数部分の情報を暗号化するなどができる.

2 NTRU

2.1 1 変数 NTRU [7]

N を素数とする．また，p, q をそれぞれ正の整数とする．環 $R = \mathbb{Z}[x]/(x^N - 1)$ の任意の元 f は $f = \sum_{i=0}^{N-1} a_i x^i$ $(a_i \in \mathbb{Z})$ と一意的に表すことができる．R の部分集合 $\mathcal{L}_{\mathbf{f}}, \mathcal{L}_{\xi}, \mathcal{L}_{\mathbf{r}}, \mathcal{L}_{\mathbf{m}}$ を定義する．まず,

$$\mathcal{L}_{\mathbf{m}} = \left\{ \sum a_i x^i \in R \;\middle|\; |a_i| < \frac{p-1}{2},\ \forall i \right\}$$

とおく．正整数 d, d' に対して，

$$\mathcal{L}(d,d') = \left\{ \sum a_i x^i \in R \;\middle|\; \begin{array}{l} d \text{ 個の } a_i \text{ は } 1, \\ d' \text{個の } a_i \text{ は } -1, \\ \text{残りは全て } 0. \end{array} \right\}$$

3 つの正整数 d_1, d_2, d_3 を選び，

$$\mathcal{L}_{\mathbf{f}} = \mathcal{L}(d_1, d_1 - 1),\ \mathcal{L}_{\xi} = \mathcal{L}(d_2, d_2),$$
$$\mathcal{L}_{\mathbf{r}} = \mathcal{L}(d_3, d_3).$$

2.1.1 鍵生成

$\mathbf{f} \in \mathcal{L}_{\mathbf{f}}$, $\xi \in \mathcal{L}_{\xi}$ をランダムに選ぶ．但し，$\mathbf{f}$ はさらに以下を満たさなければならない．(もし満たさない場合は，満たすまで $\mathbf{f}$ を選び直す．失敗する確率は N/q より小さく，数回の探索で条件を満たす $\mathbf{f}$ を見つけ出すことが可能である．)

条件　$1 + p \cdot \mathbf{f} \bmod q$ は可逆である．

このとき，以下のような $\mathbf{F}_q \in R$ が存在する：

$$\mathbf{F}_q \cdot (1 + p \cdot \mathbf{f}) \equiv 1 \bmod q$$

このとき，$\mathbf{h} \equiv \mathbf{F}_q \cdot p\xi \bmod q$ なる $\mathbf{h} \in R$ を公開鍵とし，$\mathbf{f}$ を秘密鍵とする．

2.1.2 暗号化

メッセージ m は $\mathcal{L}_{\mathbf{m}}$ の元と対応しているものとする．m を暗号化するには，まず $\mathbf{r} \in \mathcal{L}_{\mathbf{r}}$ をランダムに選ぶ．次に $e \equiv \mathbf{h} \cdot \mathbf{r} + m \bmod q$ を計算する．e が暗号文となる．

2.1.3 復号化

e を復号するには，$a \equiv (1 + p \cdot \mathbf{f}) \cdot e \bmod q$ を計算する．このとき，a の係数を $-q/2$ から $q/2$ の間に入るように取ると，これは m に一致する．

上のように構成された方式を NTRU(d_1, d_2, d_3) と表すことにする．

2.2 多変数 NTRU [5, 12]

1 変数 NTRU の類似で多変数の NTRU も構成できる．l を正整数，$N_1, \ldots, N_l$ を素数とする．また，p, q をそれぞれ正の整数とする．環 $R = \mathbb{Z}[x_1, x_2, \ldots, x_l]/(x^{N_1} - 1, \ldots, x^{N_l} - 1)$ の任意の元 f は $f = \sum_{i_1,\ldots,i_l} a_{i_1,\ldots,i_l} x_1^{i_1} \cdots x_l^{i_l}$ $(a_{i_1,\ldots,i_l} \in \mathbb{Z})$ と一意的に表すことができる．R の部分集合 $\mathcal{L}_{\mathbf{f}}^{(l)}, \mathcal{L}_{\xi}^{(l)}, \mathcal{L}_{\mathbf{r}}^{(l)}, \mathcal{L}_{\mathbf{m}}^{(l)}$ を定義する．まず，

$$\mathcal{L}_{\mathbf{m}}^{(l)} = \left\{ \sum a_{i_1,\ldots,i_l} x_1^{i_1} \cdots x_l^{i_l} \in R \;\middle|\; |a_{i_1,\ldots,i_l}| < \frac{p-1}{2},\ \forall i \right\}$$

とおく．正整数 d, d' に対して，

$$\mathcal{L}^{(l)}(d,d') = \left\{ \sum a_{i_1,\ldots,i_l} x_1^{i_1} \cdots x_l^{i_l} \in R \;\middle|\; \begin{array}{l} d \text{ 個の } a_{i_1,\ldots} \text{ は } 1, \\ d' \text{個の } a_{i_1,\ldots} \text{ は } -1, \\ \text{残りは全て } 0. \end{array} \right\}$$

3 つの正整数 d_1, d_2, d_3 を選び，

$$\mathcal{L}_{\mathbf{f}}^{(l)} = \mathcal{L}^{(l)}(d_1, d_1 - 1),\ \mathcal{L}_{\xi}^{(l)} = \mathcal{L}^{(l)}(d_2, d_2),$$
$$\mathcal{L}_{\mathbf{r}}^{(l)} = \mathcal{L}^{(l)}(d_3, d_3).$$

2.2.1 鍵生成

上記の設定の下，多変数 NTRU の鍵生成，暗号化，復号化は 1 変数 NTRU と同様に実行される．$\mathbf{f} \in \mathcal{L}_{\mathbf{f}}^{(l)}$, $\xi \in \mathcal{L}_{\xi}^{(l)}$ をランダムに選ぶ．但し，$\mathbf{f}$ はさらに以下を満たさなければならない．(もし満たさない場合は，満たすまで $\mathbf{f}$ を選び直す．失敗する確率は N/q より小さく，数回の探索で条件を満たす $\mathbf{f}$ を見つけ出すことが可能である．)

条件　$1 + p \cdot \mathbf{f} \bmod q$ は可逆である．

このとき，以下のような $\mathbf{F}_q \in R$ が存在する：

$$\mathbf{F}_q \cdot (1 + p \cdot \mathbf{f}) \equiv 1 \bmod q$$

このとき，$\mathbf{h} \equiv \mathbf{F}_q \cdot p\xi \bmod q$ なる $\mathbf{h} \in R$ を公開鍵とし，$\mathbf{f}$ を秘密鍵とする．

注意 1 オリジナルの *NTRU* の場合，上の条件を満たす $\mathbf{f}$ の探索はユークリッド互除法を用いて行うことができる．しかし，多変数 *NTRU* の場合，ユークリッド互除法が使えないため，別

の方法で条件を満たすか調べる必要がある．文献 *[12]* では，グレブナー基底計算を利用して探索する方法を提案している．我々の実装ではグレブナー基底計算は用いず，以下のような手順で探索を行った．

Step 1 $1+p\cdot\mathbf{f} \bmod q$ の $R_q = R \bmod q$ 上の積作用を行列で表示.（それを M とおく.）

Step 2 M^{-1} を計算する.（なかったら $\mathbf{f}$ を取り換え，*Step 1* に戻る.）

Step 3 M^{-1} が積作用として対応する R_q の元を計算.（それが $\mathbf{F}_q$）

2.2.2 暗号化

メッセージ m は $\mathcal{L}_{\mathbf{m}}^{(l)}$ の元と対応しているものとする．m を暗号化するには，まず $\mathbf{r}\in\mathcal{L}_{\mathbf{r}}^{(l)}$ をランダムに選ぶ．次に $e\equiv \mathbf{h}\cdot\mathbf{r}+m \bmod q$ を計算する．e が暗号文となる．

2.2.3 復号化

e を復号するには，$a\equiv(1+p\cdot\mathbf{f})\cdot e \bmod q$ を計算する．このとき，a の係数を $-q/2$ から $q/2$ の間に入るように取ると，これは m に一致する．

上のように構成された方式を $\mathrm{MTRU}_l(d_1,d_2,d_3)$ と表すことにする．

3 部分復号の方法

簡単のため，2 変数 NTRU と 1 変数 NTRU を用いた場合に，部分復号と全復号の方法を，アリスが全復号を，ボブが部分復号を行う場合で説明する．部分復号可能な暗号化は，基本的には 2 変数 NTRU と方式は同じである．但し，いくつか秘密鍵や平文の取り方に条件が加わる．まず，$R_1=\mathbb{Z}[x_1]/(x_1^{N_1}-1)$，$R_2=\mathbb{Z}[x_1,x_2]/(x_1^{N_1}-1,x_2^{N_2}-1)$ とし，次のような写像を定義する．

$$\begin{array}{ccccc}\phi_{\mathbb{Z}}: & R_2 & \to & R_1 & \\ & \cup & & \cup & \\ & f(x_1,x_2) & \mapsto & f(x_1,1). & \end{array} \tag{1}$$

3.1 鍵生成

アリスは R_2 上で $\mathrm{MTRU}_2(d_1,d_2,d_3)$ の秘密鍵 $\mathbf{f}_2\in\mathcal{L}_{\mathbf{f}}^{(2)}$ を生成する．但し，以下を満たすものとする．

$$\phi_{\mathbb{Z}}(\mathbf{f}_2)\in\mathcal{L}_{\mathbf{f}}. \tag{2}$$

ここで，$\mathcal{L}_{\mathbf{f}}$ は 1 変数の $\mathrm{NTRU}(d_1',d_2',d_3')$ から 2.1 節のように定まる R_1 の部分集合である．次に $\mathbf{f}_2$ から $\mathrm{MTRU}(d_1,d_2,d_3)$ の公開鍵 $\mathbf{h}_2\in\mathbb{Z}[G]$ を構成する．この $\mathbf{h}_2$ がアリスの公開鍵である．アリスの秘密鍵は $\mathbf{f}_2$ であり，ボブの秘密鍵は $\mathbf{f}_1:=\phi_{\mathbb{Z}}(\mathbf{f}_2)$ である．

3.2 アリスの暗号化

メッセージ m は $\mathcal{L}_m^{(2)}$ の元と対応しているものとする．但し，$\phi_{\mathbb{Z}}(m)\in\mathcal{L}_m$ を満たすと仮定する．m を暗号化するには，まず $\mathbf{r}\in\mathcal{L}_{\mathbf{r}}^{G}$ を $\phi_{\mathbb{Z}}(\mathbf{r})\in\mathcal{L}_{\mathbf{r}}^{H}$ となる範囲でランダムに選ぶ．次に $e\equiv p\mathbf{r}\cdot\zeta+m \bmod q$ を計算する．e が暗号文となる．

3.3 アリスの復号化

e を復号するには，$a\equiv(1+p\mathbf{f})\cdot e \bmod q$ を計算する．このとき，a の係数を $-q/2$ から $q/2$ の間に入るように取る．そして，$\mathbf{f}_p\cdot a \bmod p$ を計算することにより m を得る．

3.4 ボブの復号化

まず，$e'=\phi_{\mathbb{Z}}(e)$ を計算する．次に $a\equiv(1+p\mathbf{f}')\cdot e' \bmod q$ を計算する．このとき，a の係数を $-q/2$ から $q/2$ の間に入るように取る．そして，$\mathbf{f}_p\cdot a \bmod p$ を計算することにより $m'=\phi_{\mathbb{Z}}(m)$ を得る．

4 部分復号法の一般化

3 節で説明した部分復号法はさらに一般化することができる．$R_k=\mathbb{Z}[x_1,x_2,\ldots,x_k]/(x^{N_1}-1,\ldots,x^{N_k}-1)$ とおき，$\phi_i: R_{k_i}\to R_{k_{i+1}}(i=$

$1, 2, \ldots, s)$ を (1) と同様に定義される準同型写像の列とする．このとき，3 節で説明した部分復号法は（全体の場合も含めた）s 種類の部分復号法に拡張することができる．さらに一般に，上記の ϕ_i 達が木グラフを構成する場合も，部分復号法を拡張することができる．

4.1 2 種類の部分情報を持つ場合

3 節の一般化の例として，平文の 2 つの部分情報があり，それぞれをボブ，チャーリーが部分的に復号する場合を考える．2 つの部分情報は排他的である必要はない．以下では，共通情報とそれ以外（それぞれだけが復号できる情報）が存在する場合を説明する．共通情報部分を使用しなければ，排他的な部分情報をそれぞれが復号できることになる．

また前節同様，アリスは強い権限を持ち，全文を復号を復号可能であるとする．

N_1, N_2, N_3, N_4 を正の素数とし，

$$R_4 = \mathbb{Z}[x_1, x_2, x_3, x_4]/(x^{N_1} - 1, \cdots, x^{N_4} - 1),$$
$$R = \mathbb{Z}[x_1, x_2]/(x_1^{N_1} - 1, x_2^{N_2} - 1),$$
$$R' = \mathbb{Z}[x_1, x_3]/(x_1^{N_1} - 1, x_3^{N_3} - 1)$$

とする．また，

$$\begin{array}{lccc} \phi_{\mathbb{Z},1}: & R_4 & \to & R \\ & \cup & & \cup \\ & f(x_1, x_2, x_3, x_4) & \mapsto & f(x_1, x_2, 1, 1), \end{array} \tag{3}$$

$$\begin{array}{lccc} \phi_{\mathbb{Z},2}: & R_4 & \to & R' \\ & \cup & & \cup \\ & f(x_1, x_2, x_3, x_4) & \mapsto & f(x_1, 1, x_3, 1), \end{array} \tag{4}$$

を用意する．

4.1.1 ボブ，チャーリーの秘密鍵の配布

アリスは 4 変数 NTRU の鍵生成を行う．但し，$\phi_{\mathbb{Z},1}, \phi_{\mathbb{Z},2}$ に対し，(2) と同様の条件を満たすように鍵生成を行う．アリスは 4 変数 NTRU の秘密鍵 $\mathbf{f}_4$ からボブ，チャーリーの秘密鍵 $\mathbf{f}_1 = \phi_{\mathbb{Z},1}(\mathbf{f}_4)$，$\mathbf{f}_2 = \phi_{\mathbb{Z},2}(\mathbf{f}_4)$ を生成し，ボブ，チャーリーに配布する．

4.1.2 ボブ，チャーリーの部分復号法

アリスの公開鍵で生成された暗号文 e があるとする．ボブはまず，$e_1 = \phi_{\mathbb{Z},1}(e)$ を計算する．次に $a \equiv (1 + p\mathbf{f}_1) \cdot e_1 \bmod q$ を計算する．このとき，a の係数を $-q/2$ から $q/2$ の間に入るように取る．そして，$a \bmod p$ を計算することにより平文 m の部分情報 $m_1 = \phi_{\mathbb{Z},1}(m)$ を得る．

同様にして，チャーリーも平文 m の部分情報 $m_2 = \phi_{\mathbb{Z},2}(m)$ を得ることができる．定義から，m_1 は x_1, x_2 の多項式であり，m_2 は x_1, x_3 の多項式である．m_1, m_2 の構成法から，$m_1(x_1, 1) = m_2(x_1, 1) \in \mathbb{Z}[x_1]$ であり，この部分はボブとチャーリーの両方に共通の復元情報となる．

4.1.3 共通部分に対応する秘密鍵の生成

ボブとチャーリーは，互いに復元できる情報の共通部分を復元する秘密鍵を生成することができる．ボブは秘密鍵 $\mathbf{f}_1$ から $\mathbf{f}_1' = \mathbf{f}_1(x_1, 1)$ を作ることができ，チャーリーも秘密鍵 $\mathbf{f}_2$ から $\mathbf{f}_2' = \mathbf{f}_2(x_1, 1)$ を作ることができる．このとき，ボブとチャーリーの鍵の作り方から，$\mathbf{f}_1' = \mathbf{f}_2'$ となり，これが互いの共通情報を復元できる秘密鍵となる．

4.2 2 種類の部分情報の和

ボブとチャーリーがそれぞれ別の部分情報が復元できる場合，それらの情報を 2 人が持ち寄ると，より全体の情報に近い部分情報が得られるはずである．以下の場合はその典型的な例である．

N_1, N_3 を正の素数とし，$N_2 = 2$ とする．$R_3 = \mathbb{Z}[x_1, x_2, x_3]/\ (x^{N_1} - 1, x^{N_2} - 1, x^{N_3} - 1)$，$R_2 = \mathbb{Z}[x_1, x_2]/(x_1^{N_1} - 1, x_2^{N_2} - 1)$，$R_1 = \mathbb{Z}[x_1]/(x_1^{N_1} -$

1) とする．また，

$$\begin{array}{rccc} \phi_{\mathbb{Z},1}: & R_3 & \to & R_1 \\ & \cup & & \cup \\ & f(x_1,x_2,x_3) & \mapsto & f(x_1,1,0), \end{array} \tag{5}$$

$$\begin{array}{rccc} \phi_{\mathbb{Z},0}: & R_3 & \to & R_1 \\ & \cup & & \cup \\ & f(x_1,x_2,x_3) & \mapsto & f(x_1,0,0), \end{array} \tag{6}$$

$$\begin{array}{rccc} \phi_{\mathbb{Z},2}: & R_3 & \to & R_2 \\ & \cup & & \cup \\ & f(x_1,x_2,x_3) & \mapsto & f(x_1,x_2,0), \end{array} \tag{7}$$

を用意する．

4.2.1 ボブ，チャーリーの秘密鍵の配布

アリスは3変数 NTRU の鍵生成を行う．但し，$\phi_{\mathbb{Z},1}, \phi_{\mathbb{Z},2}$ に対し，(2) と同様の条件を満たすように鍵生成を行う．アリスは3変数 NTRU の秘密鍵 $\mathbf{f}_3$ からボブ，チャーリーの秘密鍵 $\mathbf{f}_1 = \phi_{\mathbb{Z},1}(\mathbf{f}_3)$，$\mathbf{f}_0 = \phi_{\mathbb{Z},0}(\mathbf{f}_3)$ を生成し，ボブ，チャーリーに配布する．チャーリーの鍵はボブが生成し，配布することもできる．

4.2.2 ボブ，チャーリーの部分復号法

アリスの公開鍵で生成された暗号文 e があるとする．ボブはまず，$e_1 = \phi_{\mathbb{Z},1}(e)$ を計算する．次に $a \equiv (1+p\mathbf{f}_1)\cdot e_1 \bmod q$ を計算する．このとき，a の係数を $-q/2$ から $q/2$ の間に入るように取る．そして，$a \bmod p$ を計算することにより平文 m の部分情報 $m_1 = \phi_{\mathbb{Z},1}(m)$ を得る．

チャーリーは暗号文 e から $e_0 = \phi_{\mathbb{Z},0}(\phi_{\mathbb{Z},1}(e))$ を計算する．あとはボブと同様にして，平文 m の部分情報 $m_0 = \phi_{\mathbb{Z},0}(\phi_{\mathbb{Z},0}(m))$ を得ることができる．

ボブとチャーリーがもし互いの復号情報を持ち寄った場合，合わせた情報は m_0, m_1 よりも大きくなる．実際，m_0, m_1 の情報から線形代数を解くことにより，$\phi_{\mathbb{Z},2}(m)$ の情報を得ることができ，これは m_0, m_1 の情報の和の情報と考えられる．

4.2.3 和に対応する秘密鍵の生成

ボブとチャーリーは互いに秘密鍵を持ち寄ることにより，互いに復元できる情報の和を復元する秘密鍵 $\mathbf{f} \in R_2$ を生成することができる．実際，$\mathbf{f}_1, \mathbf{f}_0$ から次を満たす $\mathbf{f} \in R_2$ が一意に存在し，それは線形代数を解くことにより得られる．

$$\begin{cases} \mathbf{f}_1(x_1) = \mathbf{f}(x_1,1), \\ \mathbf{f}_0(x_1) = \mathbf{f}(x_1,0). \end{cases}$$

この $\mathbf{f}$ は $\phi_{\mathbb{Z},2}(m)$ の情報を復元する秘密鍵となる．

5 パラメータの選択

提案方式の安全性を見積もる場合，使用する多変数（あるいは1変数）NTRU 全てが安全でなければならない．例えば，4.1 節の場合，ボブとチャーリーの共通部分鍵のために1変数 NTRU を用いている．このとき使用する環は $R_1 = \mathbb{Z}[x_1]/(x_1^{N_1}-1)$ である．よって，NTRU が安全となるように N_1 を選択する必要がある．同様に，4.2 節でも R_1 を使用するので，NTRU が安全となるように N_1 を選択する必要がある．

一方，方式としては使用しないが，

$$\begin{array}{rccc} \phi_{\mathbb{Z}}: & R_3 & \to & \mathbb{Z}[x_3]/(x_3^{N_3}-1) \\ & \cup & & \cup \\ & f(x_1,x_2,x_3) & \mapsto & f(0,1,x_3), \end{array}$$

などの写像を攻撃に利用される可能性がある．この場合，$\phi_{\mathbb{Z}}(\mathbf{f})$ が1変数 NTRU の鍵の条件を満たさないように選択することで攻撃を防ぐことができる．

6 秘密分散法との比較

上で説明した複数の部分情報の復元方法とは異なるが，環準同型写像として別のものを利用することで，同じように複数の部分情報の復元が可能となる．例えば，秘密分散にも応用できる．簡単な例では，2変数の場合で N_1 を素数，$N_2 = 3$ とする．$R_1 = \mathbb{Z}[x_1]/(x_1^{N_1}-1)$，$R_2 =$

$\mathbb{Z}[x_1, x_2]/(x_1^{N_1} - 1, x_2^{N_2} - 1)$ とし，次のような写像を定義する．

$$\begin{array}{rccc} \phi_{\mathbb{Z},1}: & R_2 & \to & R_1 \\ & \cup & & \cup \\ & f(x_1, x_2) & \mapsto & f(x_1, 1), \end{array} \tag{8}$$

$$\begin{array}{rccc} \phi_{\mathbb{Z},0}: & R_2 & \to & R_1 \\ & \cup & & \cup \\ & f(x_1, x_2) & \mapsto & f(x_1, 0). \end{array} \tag{9}$$

$$\begin{array}{rccc} \phi_{\mathbb{Z},-1}: & R_2 & \to & R_1 \\ & \cup & & \cup \\ & f(x_1, x_2) & \mapsto & f(x_1, -1), \end{array} \tag{10}$$

ボブ，チャーリー，デイブはそれぞれ $\phi_{\mathbb{Z},1}$, $\phi_{\mathbb{Z},0}$, $\phi_{\mathbb{Z},-1}$ に対応する部分秘密鍵をアリスから受け取っているとする．すると，暗号文 c から，2変数 NTRU の平文 m の部分情報 $m_1 = \phi_{\mathbb{Z},1}(m)$, $m_0 = \phi_{\mathbb{Z},0}(m)$, $m_{-1} = \phi_{\mathbb{Z},-1}(m)$ をボブ，チャーリー，デイブはそれぞれ復元することが可能である．

一方，3人が m_1, m_0, m_{-1} の情報を持ち寄ると，線形代数を解くことにより，元の平文 m を復元することが可能である．すなわち，閾値3の秘密分散が可能となる．

7 具体例

7.1 Toy Example 1

2変数NTRUの具体例を見よう．$N_1 = 6$, $N_2 = 3$, $p = 3$, $q = 1024$ とする．2変数多項式 $\sum_{i,j} a_{ij} x^i y^j$ は行列 $(a_{ij})_{ij}$ と対応させることができる．よって以下，2変数多項式を行列の形で表すことにする．$\mathcal{S}_G$ での秘密鍵を

$$\mathbf{f}_G = \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & -1 & -1 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \end{array}\right)$$

と表すことができる．$\mathbf{f}_G$ と対応する $\mathcal{S}_H$ の秘密鍵 $\mathbf{f}_H$ は $\mathbf{f}_G$ の最後の列の，

$$\mathbf{f}_H = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}$$

となる．これから計算される公開鍵はそれぞれ，

$$\mathbf{h}_G = \left(\begin{array}{ccc} 280 & 365 & 626 \\ 71 & 969 & 494 \\ 376 & 986 & 455 \\ 225 & 236 & 22 \\ 495 & 667 & 961 \\ 601 & 11 & 514 \end{array}\right), \quad \mathbf{h}_H = \begin{pmatrix} 626 \\ 494 \\ 455 \\ 22 \\ 961 \\ 514 \end{pmatrix}$$

となる．$\mathbf{h}_H$ は $\mathbf{h}_G$ から誰でも計算可能なので，公開鍵は $\mathbf{h}_G$ のみで十分である．平文をそれぞれ，

$$m_G = \left(\begin{array}{cc|c} 0 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \\ -1 & 1 & 1 \\ 0 & -1 & -1 \\ 1 & -1 & 1 \end{array}\right), \quad m_H = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

とする（m_H は m_G から定まることに注意）と，暗号文はそれぞれ，

$$e_G = \left(\begin{array}{ccc} 584 & 420 & 30 \\ 207 & 561 & 120 \\ 56 & 630 & 974 \\ 66 & 932 & 133 \\ 109 & 304 & 1013 \\ 325 & 762 & 803 \end{array}\right), \quad e_H = \begin{pmatrix} 30 \\ 120 \\ 974 \\ 133 \\ 1013 \\ 803 \end{pmatrix}$$

となる．e_H は e_G から誰でも計算可能なので，暗号文は e_G のみで十分である．

8 まとめと今後の課題

暗号化を1個の公開鍵で行い，復号は公開鍵に紐付けられた複数の秘密鍵でそれぞれ部分復号

を行う部分復号方式を提案した．本提案方式は，複数の暗号の組み合わせでなく，多変数NTRU暗号を用いた単一の暗号スキームによりこの機能を実現することを特徴とするものである．

本提案方式の設計指針は群環を用いたNTRU暗号の拡張版に対しても適用することが可能である．この場合は安全な設計が課題であり，今後の課題としたい．

参考文献

[1] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik. Sanitizable signatures. In *Computer Security - ESORICS 2005, 10th European Symposium on Research in Computer Security, Milan, Italy, September 12-14, 2005, Proceedings*, pages 159–177, 2005.

[2] M. Bellare, A. Boldyreva, and J. Staddon. Randomness re-use in multi-recipient encryption schemeas. In *Public Key Cryptography - PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, January 6-8, 2003, Proceedings*, pages 85–99, 2003.

[3] C. Brzuska, M. Fischlin, T. Freudenreich, A. Lehmann, M. Page, J. Schelbert, D. Schröder, and F. Volk. Security of sanitizable signatures revisited. In *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, pages 317–336, 2009.

[4] C. Brzuska, M. Fischlin, A. Lehmann, and D. Schröder. Santizable signatures: How to partially delegate control for authenticated data. In *BIOSIG 2009 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 17.-18. September 2009 in Darmstadt, Germany*, pages 117–128, 2009.

[5] M. Caboara, F. Caruso, and C. Traverso. Gröbner bases for public key cryptography. In *Symbolic and Algebraic Computation, International Symposium, ISSAC 2008, Linz/Hagenberg, Austria, July 20-23, 2008, Proceedings*, pages 315–324, 2008.

[6] Y. Hatano and K. Miyazaki. 権限の異なる多重受信者のための暗号化方式 (an encryption method for multiple receivers with different roles). **電子情報通信学会技術研究報告**. *ISEC,* **情報セキュリティ**, 105(664):91–96, 2006.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, pages 267–288, 1998.

[8] S. Idani, K. Aburu, T. Izu, K. Itoh, M. Ushida, T. Ogura, M. Takenaka, and H. Tsuda. センサデータの利活用に適したプライバシ保護付き暗号化システム. In **コンピュータセキュリティシンポジウム** *2012* **論文集**, pages 1D2–1, 2012.

[9] G. F. Inc. 秘密分散技術 gfi 電子割符, 1999.

[10] T. Izu, K. Ito, H. Tsuda, K. Abiru, and T. Ogura. Privacy-protection technologies for secure utilization of sensor data. *Fujitsu Sci. Tech. J.*, 50(1):30–33, 2014.

[11] T. Izu, N. Kunihiro, K. Ohta, M. Sano, and M. Takenaka. Yet another sanitizable signature from bilinear maps. In *Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES 2009, March 16-19, 2009, Fukuoka, Japan*, pages 941–946, 2009.

[12] M. Koshiba, S. Inoue, M. Wada, and M. Morita. 多変数多項式環を用いた ntru 暗号の拡張. In **数理解析研究所講究録 第** *1815* **巻**, pages 79–89, 2012.

[13] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.