イデアル格子を用いた完全準同型暗号について，Gentry による

On the fully homomorphic encryption using ideal lattices, after Gentry

数学専攻　田中清志
Kiyoshi TANAKA

はじめに

本論文は，完全準同型暗号に関する Craig Gentry の論文 [1] の数学的な部分について，Alice Silverberg の論説 [2] を参考にしてまとめた総合報告である．論文は 4 節からなっていて，第 1 節では準同型暗号や完全準同型暗号について [4] を参考に概略をまとめた．第 2 節では整数を成分に持つ正方行列の Hermite 正規形について，第 3 節では円分体の整数環におけるイデアル格子について，第 4 節では Gentry の方式について，数学の記述としてして厳密に，他の文献を参照しなくても読めるようにまとめた．

1　準同型暗号

用語 1.1. 公開鍵暗号は以下の 3 つの多項式時間アルゴリズムからなっている．
(1) 鍵生成 KeyGen: 1^k (k はセキュリティパラメータ) を入力して，公開鍵と秘密鍵の対 $(\mathrm{pk}, \mathrm{sk})$ を出力するアルゴリズム．システムの上の平文空間 $\mathcal{M}_{\mathrm{pk}}$ は pk に含まれる．特に $\mathcal{M}_{\mathrm{pk}}$ の指定がない場合は $\mathcal{M}_{\mathrm{pk}} = \{0,1\}^k$ と設定する．
(2) 暗号化 Encrypt: 公開鍵 pk および平文 $m \in \mathcal{M}_{\mathrm{pk}}$ を入力して暗号文 c を出力するアルゴリズム．
(3) 復号化 Decrypt: 公開鍵 pk，秘密鍵 sk および暗号文 c を入力し，平文 m あるいは復号不可を意味する特別な記号を出力するアルゴリズム．

用語 1.2. 以下が成立するとき，公開鍵暗号方式 $(\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ は準同型性を持つという．
任意の k および $(\mathrm{pk}, \mathrm{sk}) \xleftarrow{\mathrm{R}} \mathsf{KeyGen}(1^k)$ に対して
(1) 平文空間 $\mathcal{M}_{\mathrm{pk}}$ と暗号文空間 $\mathcal{C}$ が群の構造を持つ．
(2) 任意の $m \in \mathcal{M}_{\mathrm{pk}}$ に対して $\mathsf{Encrypt}(\mathrm{pk}, m) \in \mathcal{C}$．
(3) 任意の $m_1, m_2 \in \mathcal{M}_{\mathrm{pk}}$ に対して

$$\mathsf{Encrypt}(\mathrm{pk}, m_1 m_2) = \mathsf{Encrypt}(\mathrm{pk}, m_1)\mathsf{Encrypt}(\mathrm{pk}, m_2)$$

が成立する．

準同型性を持つ公開鍵暗号を準同型暗号とよぶ．例えば，RSA 暗号，ElGamal 暗号，Paillier 暗号は準同型暗号である．

用語 1.3. 公開鍵暗号方式 $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ に，アルゴリズム Evaluate「公開鍵 pk，回路 f および暗号文の組 $\boldsymbol{c} = (c_1, \ldots, c_l)$ を入力として，暗号文 $c' \xleftarrow{\mathrm{R}} \mathsf{Evaluate}(\mathrm{pk}, f, \boldsymbol{c})$ を出力する」を追加する．$m_1, m_2, \ldots$ を平文の列とし，各 i に対して $c_i \xleftarrow{\mathrm{R}} \mathsf{Encrypt}(\mathrm{pk}, m_i)$ とおく．任意の回路 f に対して

$$\mathsf{Decrypt}(\mathrm{sk}, \mathsf{Evaluate}(\mathrm{pk}, f, \boldsymbol{c})) = f(m_1, \ldots, m_l)$$

が成立するとき，公開鍵暗号方式 $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt}, \mathsf{Evaluate})$ は完全準同型性を持つという．

2 Hermite の正規形

定義 2.1. (整数成分の行列に対する基本変形) 整数を成分に持つ行列に対する以下の操作を行に関する基本変形という.
(1) ある行に他の行の整数倍を加える.
(2) ある行を ± 1 倍する.
(3) ある行と他の行を入れ換える.
また，以下の操作を列に関する基本変形という.
(4) ある列他の列の整数倍を加える.
(5) ある列を ± 1 倍する.
(6) ある列と他の列を入れ換える.

定理 2.2. $A \in M(n,\mathbb{Z})$ とし，$\det A \neq 0$ と仮定する．このとき，A に対して列に関する基本変形を繰り返し施すことによって下三角行列

$$(\sharp) \quad \begin{pmatrix} a'_{11} & 0 & \dots & 0 \\ a'_{21} & a'_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a'_{n1} & a'_{n2} & \dots & a'_{nn} \end{pmatrix} \quad (\text{各 } j \geq 1 \text{ に対して } a'_{jj} > 0,\ i > j \text{ なら } 0 \leq a'_{ij} < a'_{jj})$$

の形に変形できる．また，下三角行列 $(\sharp)$ は A に対して一意的に定まる．$(\sharp)$ を A の Hermite の正規形 normal form とよぶ.

補足 2.3. $A \in M(n,\mathbb{Z})$ とし，$\det A \neq 0$ と仮定する．このとき，A に列に関する基本変形を繰り返し施すことによって下三角行列

$$(\sharp)' \quad \begin{pmatrix} a'_{11} & 0 & \dots & 0 \\ a'_{21} & a'_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a'_{n1} & a'_{n2} & \dots & a'_{nn} \end{pmatrix} \quad (\text{各 } j \geq 1 \text{ に対して } a'_{jj} > 0,\ i > j \text{ なら } -\frac{a'_{jj}}{2} \leq a'_{ij} < \frac{a'_{jj}}{2})$$

の形に一意的に変形できる．$(\sharp)'$ も A の Hermite の正規形とよぶことにする.

命題 2.4. $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n, \boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n \in \mathbb{Z}^n$ とし，$A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n)$, $B = (\boldsymbol{b}_1\ \boldsymbol{b}_2\ \dots\ \boldsymbol{b}_n)$ とおく．さらに，$\det A \neq 0$ と仮定する．このとき，$\mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \cdots + \mathbb{Z}\boldsymbol{a}_n = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2 + \cdots + \mathbb{Z}\boldsymbol{b}_n \Leftrightarrow P \in GL(n,\mathbb{Z})$ が存在して $B = AP$ となる.

系 2.5. $\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n \in \mathbb{Z}^n$ とし，$A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n) \in M(n,\mathbb{Z})$ とおく．さらに，$\det A \neq 0$ と仮定する．このとき，$\boldsymbol{a}'_1, \boldsymbol{a}'_2, \dots, \boldsymbol{a}'_n \in \mathbb{Z}^n$ が唯一組存在して，(1) $\mathbb{Z}\boldsymbol{a}'_1 + \mathbb{Z}\boldsymbol{a}'_2 + \cdots + \mathbb{Z}\boldsymbol{a}'_n = \mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \cdots + \mathbb{Z}\boldsymbol{a}_n$, (2) $(\boldsymbol{a}'_1\ \boldsymbol{a}'_2\ \dots\ \boldsymbol{a}'_n)$ が Hermite の正規形，となる.

3 イデアル格子

記号 3.1. n を整数 ≥ 3 とし，$\zeta = e^{2\pi i/n}$, $K = \mathbb{Q}(\zeta)$, $\mathcal{O}_K = \mathbb{Z}[\zeta]$, $N = \varphi(n)$ とおく．このとき，対応 $t \mapsto \zeta$ によって環の準同型 $\xi : \mathbb{Z}[t] \to \mathbb{C}$ を定義すれば，ξ は剰余環の同型 $\tilde{\xi} : \mathbb{Z}[t]/(\Phi_n(t)) \xrightarrow{\sim} \mathcal{O}_K$ を誘導する．した

がって，$\{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\}$ は $\mathcal{O}_K$ の $\mathbb{Z}$ の上の基底.

$\alpha \in \mathcal{O}_K$ とする．このとき，$a(t) \in \mathbb{Z}[t]$ が唯一つ存在して $a(\zeta) = \alpha$, $\deg a(t) < N$ となる．さらに，環の同型 $\tilde{\xi} : \mathbb{Z}[t]/(\Phi_n(t)) \xrightarrow{\sim} \mathcal{O}_K$ は環の同型 $\tilde{\xi} : \mathbb{Z}[t]/(\Phi_n(t), a(t)) \xrightarrow{\sim} \mathcal{O}_K/(\alpha)$ を誘導する．

$\alpha \in \mathcal{O}_K$ とする．このとき，$a(t) \in \mathbb{Z}[t]$ が唯一つ存在して $a(\zeta) = \alpha$, $\deg a(t) < N$ となる．さらに，環の同型 $\tilde{\xi} : \mathbb{Z}[t]/(\Phi_n(t)) \xrightarrow{\sim} \mathcal{O}_K$ は環の同型 $\tilde{\xi} : \mathbb{Z}[t]/(\Phi_n(t), a(t)) \xrightarrow{\sim} \mathcal{O}_K/(\alpha)$ を誘導する．

補題 3.2. $\alpha \in \mathcal{O}_K$, $d = \mathrm{Nr}_{K/\mathbb{Q}}\alpha$ とし，d が平方因子を持たないと仮定する．このとき，剰余環 $\mathcal{O}_K/(\alpha)$ は $\mathbb{Z}/d\mathbb{Z}$ に同型．さらに，$r \in \mathbb{Z}$ が存在して $\Phi_n(r) \equiv 0 \mod d$, $a(r) \equiv 0 \mod d$ が成立する．r は d を法として一意的に定まる．

命題 3.3. ν を整数 ≥ 1 とし，$n = 2^{\nu+1}$, $N = 2^\nu$, $\zeta = e^{2\pi i/n}$, $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{N-1}\zeta^{N-1}$ $(a_0, a_1, a_2, \ldots, a_{N-1} \in \mathbb{Z})$ とおく．$\alpha \neq 0$ なら，整数環 $\mathbb{Z}[\zeta]$ のイデアル (α) の基底 $\{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\}$ に関するイデアル格子としての表現行列は

$$A = \begin{pmatrix} a_0 & -a_{N-1} & -a_{N-2} & \ldots & -a_1 \\ a_1 & a_0 & -a_{N-1} & \ldots & -a_2 \\ a_2 & a_1 & a_0 & \ldots & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{N-1} & a_{N-2} & a_{N-3} & \ldots & a_0 \end{pmatrix}$$

で与えられる．さらに，$d = \det A$, $a(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_{N-1}t^{N-1}$ とおく．d が平方因子を持たなければ,

(1) $r \in \mathbb{Z}$ が存在して $r^N + 1 \equiv 0 \mod d$, $a(r) \equiv 0 \mod d$ となる．さらに，r は d を法として一意的に定まる．

(2) A に対して列に関する基本変形を繰り返し施すことによって下三角行列

$$\begin{pmatrix} d & -r & -r^2 & \ldots & -r^{N-2} & -r^{N-1} \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

の形に変形できる．

4 Gentry の完全準同型暗号

定義 4.1. $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n \in \mathbb{R}^n$ とし，$A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \ldots\ \boldsymbol{a}_n)$, $\Lambda = \boldsymbol{a}_1\mathbb{Z} + \boldsymbol{a}_2\mathbb{Z} + \cdots + \boldsymbol{a}_n\mathbb{Z}$ とおく．さらに，$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n \in \mathbb{R}^n$ が一次独立であると仮定する．このとき，Λ は $\mathbb{R}^n$ の格子．また，剰余群 $\mathbb{R}^n/\Lambda$ の完全代表系として

$$\Pi_A = \left\{ r_1\boldsymbol{a}_1 + r_2\boldsymbol{a}_2 + \ldots + r_n\boldsymbol{a}_n\ ;\ r_i \in \left[-\frac{1}{2}, \frac{1}{2}\right) \right\}$$

が取れる．Π_A を $A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \ldots\ \boldsymbol{a}_n)$ に伴う基本平行体 fundamental parallelepiped とよぶ.

定義 4.2. $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ とする．このとき，

$$\begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} = A^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

とおけば，

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \dots\ \boldsymbol{a}_n) \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} = x'_1\boldsymbol{a}_1 + x'_2\boldsymbol{a}_2 + \cdots + x'_n\boldsymbol{a}_n$$

さらに，各 i に対して $r_i \in \left[-\frac{1}{2}, \frac{1}{2}\right)$ が唯一つ存在して $r'_i \equiv x'_i \mod \mathbb{Z}$ となる．このとき，

$$A \begin{pmatrix} r'_1 \\ r'_2 \\ \vdots \\ r'_n \end{pmatrix} = r'_1\boldsymbol{a}_1 + r'_2\boldsymbol{a}_2 + \cdots + r'_n\boldsymbol{a}_n \in \mathit{\Pi}_A,\ A \begin{pmatrix} r'_1 \\ r'_2 \\ \vdots \\ r'_n \end{pmatrix} \equiv \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mod \mathit{\Lambda}$$

対応

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = A \begin{pmatrix} r'_1 \\ r'_2 \\ \vdots \\ r'_n \end{pmatrix}$$

によって写像 $\pi_A : \mathbb{R}^n \to \mathit{\Pi}_A$ を定義する．

B を A の Hermite 正規形とする．$\boldsymbol{a} \in \mathit{\Pi}_A$ なら，$\pi_A(\pi_B(\boldsymbol{a}) = \boldsymbol{a}$.

参考文献

[1] Craig Gentry, Fully Homomorphic Encryption Using Ideal Lattices, in Proceedings of the 41st ACM Symposium on Theory of Computing – STOC 2009, ACM, New York (2009), 169–178.

[2] Alice Silverberg, Fully homomorphic encryption for mathematicians, IACR Cryptology ePrint Archive http://eprint.jacr.org/2013/250

[3] 笠原正雄，境隆一，暗号–ネットワーク社会の安全を守る鍵，共立出版 (2002)

[4] 森山大輔，西巻陵，岡本龍明，公開鍵暗号の数理，共立出版 (2011)