イデアル格子暗号入門

有田正剛 †

1　はじめに

イデアル格子暗号とは円分整数の作り出す暗号である。円分整数とは、1 のべき乗根が作り出す、一般化された整数であり、数であると同時に多次元ベクトルでもある。円分整数を仲立ちとして代数的な世界 (イデアル) と幾何的な世界 (格子) が交錯し、豊かな数学的状況 (イデアル格子) が現れる。そのような円分整数の特性が作り出すイデアル格子暗号は、RSA 暗号や楕円曲線暗号といった、従来の数論的な公開鍵暗号とは異なる原理で動作し、それら従来の公開鍵暗号よりも一般に高機能であり、かつ高い並列処理性をもつ。そのため、クラウド環境においてビッグデータを処理するための切り札として期待されている。

本解説では、そのようなイデアル格子暗号の代表例として、最短円分整数問題の困難性に基づく衝突困難ハッシュ関数 [4] と Ring-LWE 問題に基づく準同型暗号 [1, 2] について紹介する。（小さなパラメータの）計算例を多く用意した。理論の理解よりも計算感覚を重視して説明する。

2　円分整数

円分整数について紹介する。詳細は [3] 等を参照されたい。

2.1　円の 3 分整数

高校数学でもお馴染みの複素数

$$\zeta = (-1 + \sqrt{-3})/2$$

から始める。三角関数を思い出すと、$-1/2 = \cos(2\pi/3)$, $\sqrt{3}/2 = \sin(2\pi/3)$ なので、ζ は

$$\zeta = \cos(2\pi/3) + \sqrt{-1}\sin(2\pi/3) = \mathrm{e}^{2\pi\sqrt{-1}/3}$$

ともかけ、複素平面で図示すると図 1 のようになる。

†情報セキュリティ研究科 教授

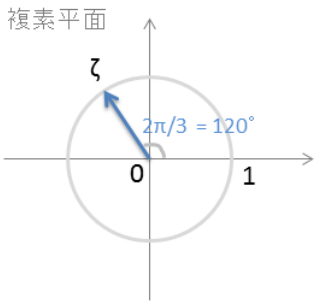

図 1: 1 の 3 乗根

つまり、ζ は円を 3 つに分ける (絶対値 1 の) 複素数であり、代数的にも 3 乗すると 1 に等しい:

$$\zeta^3 - 1 = 0.$$

ここで、左辺は $\zeta - 1$ で割りきれるので、

$$\zeta^2 + \zeta + 1 = 0$$

となり、

$$\begin{aligned}
\zeta^2 &= -1 - \zeta, \\
\zeta^3 &= \zeta^2\zeta = (-1-\zeta)\zeta = -\zeta - (-1-\zeta) = 1 \\
\zeta^4 &= (\zeta^2)^2 = (-1-\zeta)^2 = 1 + 2\zeta + \zeta^2 = 1 + 2\zeta + (-1-\zeta) = \zeta
\end{aligned}$$

といった具合に、ζ の (一般次数) 多項式 $f(\zeta)$ は、$\zeta^2 = -\zeta - 1$ であることを利用すれば、必ず ζ の一次式 $a_0 + a_1\zeta$ に変形することができる。多項式 $f(\zeta)$ に対し、2 次式 $\zeta^2 + \zeta + 1$ でわった余りをとると一次式 $a_0 + a_1\zeta$ が得られるということである。

定義 1 a_0, a_1 を整数とするとき

$$a_0 + a_1\zeta$$

の形の複素数を円の *3* 分整数という。

円の 3 分整数どうしは足したり、掛けたりすることができる:

$$\begin{aligned}
(a_0 + a_1\zeta) + (b_0 + b_1\zeta) &= (a_0 + b_0) + (a_1 + b_1)\zeta, \\
(a_0 + a_1\zeta) \cdot (b_0 + b_1\zeta) &= (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0 - a_1b_1)\zeta.
\end{aligned}$$

このように、足し算は ζ の係数どうしを単に足すだけで、掛け算はそれよりも少し複雑である。この、ころよい複雑さが円分整数が暗号に役立つことのはじまりのように思う。

円の 3 分整数全体を $\mathbb{Z}[\zeta]$ とかく:

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta \mid a_0, a_1\text{は整数}\}.$$

上に見たように、$\mathbb{Z}[\zeta]$ は足し算と掛け算をもつ。

2.2 円 (の m) 分整数

一般に、正の整数 m について

$$\zeta = \cos(2\pi/m) + \sqrt{-1}\sin(2\pi/m) = \mathrm{e}^{2\pi\sqrt{-1}/m}$$

とする。ζ は m 乗すると 1 に等しい: $\zeta^m = 1$. ζ(とその共役) を根とする多項式

$$\Phi_m(X) = \prod_{0\le k<m,\ \gcd(k,m)=1} (X - \zeta^k) \tag{1}$$

を考える。ここで、k は、0 以上 (m-1) 以下の整数のうち、m とは互いに素 (すなわち最大公約数 $\gcd(k,m) = 1$) である、すべての k を走る。そのような k の個数を $\phi(m)$ とおくと、$\Phi_m(X)$ は $\phi(m)$ 次の多項式ということになるが、$\Phi_m(X)$ の定義式 (1) は ζ^k たちについて対称であるため、(その定義式を展開すると) 係数はすべて (通常の) 整数となることが知られている。

定義 2 (円分整数) $n = \phi(m)$ 個の整数 $a_0, a_1, \ldots, a_{n-1}$ について

$$a_0 + a_1\zeta + \cdots a_{n-1}\zeta^{n-1}$$

の形の複素数を円 *(の m)* 分整数という。

円の m 分整数全体を $\mathbb{Z}[\zeta]$ とかく:

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots a_{n-1}\zeta^{n-1} \ \mid \ a_0, a_1, \ldots, a_{n-1}\text{は整数}\}.$$

円の 3 分整数の場合と同様、$\mathbb{Z}[\zeta]$ は足し算と掛け算をもち、通常の整数の一般化と考えられる。

円分整数はベクトルあるいは格子点と見なすこともできる (図 2)。実際、円分整数 $h = a_0 + a_1\zeta + \cdots a_{n-1}\zeta^{n-1}$ に対してその ζ に関する係数をならべると、格子点 $(a_0, a_1, \ldots, a_{n-1})$ を得る。整数 a_i は規則正しく離散的に現れるので、点 $(a_0, a_1, \ldots, a_{n-1})$ は格子上に並ぶ。円分整数 h に対し、このように格子点 $(a_0, a_1, \ldots, a_{n-1})$ を対応させることで、その大きさを考えることができる:

$$||h|| = (a_0^2 + a_1^2 + \cdot + a_{n-1}^2)^{1/2}.$$

この大きさ $||h||$ は、円分整数 h の複素数としての絶対値とは異なることに注意する。

2.3 イデアル

円分整数 $g = g_0 + g_1\zeta + \cdots + g_{n-1}\zeta^{n-1}$ の ‘倍数 ’全体の集合 I_g を (円分整数 g が生成する) イデアルという [1]:

$$I_g = \{a_0 g + a_1\zeta g + \cdots + a_{n-1}\zeta^{n-1} g \mid a_0, a_1, \ldots, a_{n-1} : \text{整数}\}.$$

[1] 主イデアルというべきだがここでは簡単にイデアルという。

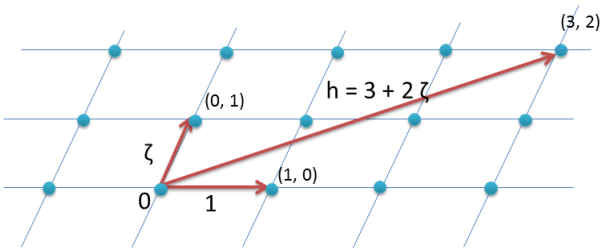

図 2: 円分整数は格子点でもある

イデアル I_g に含まれる円分整数どうしを足すと、またイデアル I_g に含まれる:

$$h_1, h_2 \in I_g \Rightarrow h_1 + h_2 \in I_g.$$

また、イデアル I_g に含まれる円分整数にどんな円分整数を掛けても、またイデアル I_g に含まれる:

$$a \in \mathbb{Z}[\zeta], h \in I_g \Rightarrow ah \in I_g.$$

イデアル I_g に含まれる円分整数 $h = a_0 g + a_1 \zeta g + \cdots + a_{n-1}\zeta^{n-1} g$ の全体は n 個のベクトル $g, \zeta g, \ldots, \zeta^{n-1} g$ が張る部分格子をなし、h はその格子点と考えることができる (図 3)。

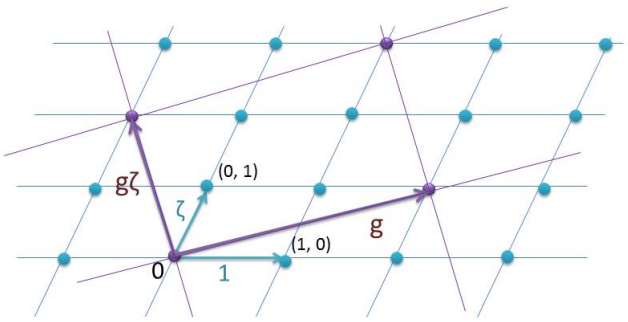

図 3: イデアル I_g は部分格子をなす

ここまでのまとめ：円分整数の性質

- 円分整数は代数構造をもつ。

$$(a_0 + a_1\zeta) + (b_0 + b_1\zeta) = (a_0 + b_0) + (a_1 + b_1)\zeta$$

$$(a_0 + a_1\zeta) \cdot (b_0 + b_1\zeta) = (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0 - a_1 b_1)\zeta$$

- 円分整数は格子をなす:

$$h = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \Leftrightarrow \text{格子点 } (a_0, a_1, \ldots, a_{n-1}).$$

大きさ $||h|| = (a_0^2 + a_1^2 + \cdots + a_{n-1}^2)^{1/2}$ をもつ。

- 円分整数 g が生成するイデアル I_g に含まれる円分整数の全体を考えると、それは n 個のベクトル $g, \zeta g, \ldots, \zeta^{n-1} g$ が張る部分格子をなす。足し算も掛け算ももつ。

例 1 円の 3 分整数の場合 ($m = 3, n = 2, \zeta = (-1 + \sqrt{-3})/2$) の計算例を示す。

$$
\begin{aligned}
(2 + 5\zeta) + (1 - 7\zeta) &= 3 - 2\zeta \\
(2 + 5\zeta) \cdot (1 - 7\zeta) &= 2 - 9\zeta - 35\zeta^2 = 2 - 9\zeta - 35(-1 - \zeta) = 37 + 26\zeta \\
||2 + 5\zeta|| &= \sqrt{4 + 25} = \sqrt{29} \\
||1 - 7\zeta|| &= \sqrt{1 + 49} = \sqrt{50} \\
||37 + 26\zeta|| &= \sqrt{37^2 + 26^2} = \sqrt{2045} \\
g = 3 + 4\zeta \quad \text{とすると} \quad \zeta g &= -4 - \zeta \quad \therefore\ I_g = \mathbb{Z}(3 + 4\zeta) + \mathbb{Z}(-4 - \zeta)
\end{aligned}
$$

記号

ここで、以降、本解説で用いる記号をまとめておく。

- $[a..b]$
  a 以上 b 以下の実数からなる区間を表す。

- $(a..b]$
  a より大きく b 以下の実数からなる区間を表す。

- $a \equiv b \pmod{n}$
  $a - b$ が n で割り切れることを表す。例: $8 \equiv 3 \pmod{5}$.

- $a \bmod n$
  a を n でわった余りを表す。余りは $\{0, 1, \ldots, n-1\}$ の範囲にとる。a が円分整数の場合には ζ の各係数について上記の余りをとる。例: $8 \bmod 5 = 3$, $[12 + 8\zeta - 9\zeta^2]_5 = 2 + 3\zeta + \zeta^2$.

- $[a]_n$
  a を n でわった余りを表す。余りは区間 $(-n/2, n/2]$ にとる。a が円分整数の場合には ζ^i の各係数について上記の余りをとる。例: $[8]_5 = -2$, $[12 + 8\zeta - 9\zeta^2]_5 = 2 - 2\zeta + \zeta^2$.

- $\mathbb{Z} = \{$ 整数全体 $\}$
  a が整数であることを $a \in \mathbb{Z}$ とかく。

- $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$, $\mathbb{Z}^{(p)} = (-p/2, p/2] \cap \mathbb{Z}$
  例: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, $\mathbb{Z}^{(5)} = \{-2, -1, 0, 1, 2\}$.

- $\mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{n-1} = \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}\}$
  円分整数全体を表す。

- $\mathbb{Z}_p[\zeta] = \mathbb{Z}_p + \mathbb{Z}_p\zeta + \cdots + \mathbb{Z}_p\zeta^{n-1}$
  $\mathbb{Z}_p$ の要素を ζ の各係数にもつ円分整数全体を表す。

- $\mathbb{Z}^{(p)}[\zeta] = \mathbb{Z}^{(p)} + \mathbb{Z}^{(p)}\zeta + \cdots + \mathbb{Z}^{(p)}\zeta^{n-1}$
  $\mathbb{Z}^{(p)}$ の要素を ζ の各係数にもつ円分整数全体を表す。

- $I_g = \mathbb{Z}g + \mathbb{Z}g\zeta + \cdots + \mathbb{Z}g\zeta^{n-1}$
  円分整数 g の倍数全体のなすイデアルを表す。

3 円分整数を用いた衝突困難関数の構成

本節では、最短円分整数問題の困難性に基づく衝突困難ハッシュ関数 [4] を紹介する。

3.1 衝突困難関数

有限集合 V から有限集合 W への関数 $H : V \to W$ を考える。ただし、V の要素数 $>$ W の要素数とする。このとき、必ず、V の異なる 2 要素 $v_1 \neq v_2$ があって、それらの H による像は等しい: $f(v_1) = f(v_2)$.

数学的に存在するものであっても、実際に計算できるかどうかは別である。このような関数 $H : V \to W$ に対して、$H(v_1) = H(v_2)$ となるペア $v_1 \neq v_2$ を求めることが計算量的には困難である (すなわち計算は数学的には可能だが人間的な時間内には終わらない) とき、関数 H は**衝突困難**であるという。衝突困難関数は暗号ツールとしてとても強力なものであり、その構成は容易ではない。

衝突困難ハッシュ関数 [4] は、以下の問題の困難性に基づく。

定義 3 (最短円分整数問題) 与えられたイデアル $I_f = \mathbb{Z}f + \mathbb{Z}\zeta f + \cdots + \mathbb{Z}\zeta^{n-1}f$ について、それに含まれる *0* とは異なる円分整数 $g = a_0 f + a_1\zeta f + \cdots + a_{n-1}\zeta^{n-1}f = c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1}$ $(a_0, \ldots, a_{n-1} \in \mathbb{Z}, c_0, \ldots, c_{n-1} \in \mathbb{Z})$ のうち、その大きさ $||g|| = (c_0^2 + c_1^2 + \cdots + c_{n-1}^2)^{1/2}$ が最少であるものを求める問題を**最短円分整数問題**とよぶ。

n が十分大きいとき (数百以上)、最短円分整数問題は (量子計算機を用いても) 難問と考えられている。

例 2 円の 3 分整数の場合 $(m = 3, n = 2, \zeta = (-1 + \sqrt{-3})/2)$ に、イデアルとそれに属する円分整数の大きさを観察する。($n = 2$ では小さすぎて最短円分整数問題は難しくない。この例の目的は計算のイメージを示すことである)

円分整数として $f = 3 + 4\zeta$ をとる。$\zeta f = -4 - \zeta$ であるので、f が生成するイデアル I_f は $I_f = \mathbb{Z}(3 + 4\zeta) + \mathbb{Z}(-4 - \zeta)$ となる。イデアル I_f に属する円分整数 $I_f \ni h = (3 + 4\zeta) - 2(-4 - \zeta) = 11 + 6\zeta$ はその大きさとして $||h|| = \sqrt{11^2 + 6^2} = \sqrt{157}$ をもつ。イデアル I_f に属する円分整数 $I_f \ni g = 2(3 + 4\zeta) + (-4 - \zeta) = 2 + 7\zeta$ は、大きさ $||g|| = \sqrt{2^2 + 7^2} = \sqrt{53}$ をもつ。

3.2 衝突困難関数の構成

係数が 0 または 1 である円分整数全体の集合を B とする: $B = \mathbb{Z}_2[\zeta] \subset \mathbb{Z}[\zeta]$. m 個の円分整数 $a_1, \ldots, a_m$ を $\mathbb{Z}_p[\zeta]$ から独立に一様ランダムに選んでおく。B の m 個の直積 B^m から $\mathbb{Z}_p$ 係数の円分整数の集合 $\mathbb{Z}_p[\zeta]$ への写像

$$H : B^m \to \mathbb{Z}_p[\zeta]$$

を以下のように定義する:

$$H(z_1, \ldots, z_m) = (a_1 z_1 + a_2 z_2 + \ldots + a_m z_m) \bmod p.$$

このように、関数 H は入力された円分整数 z_i に予め選んでおいた円分整数 a_i を掛け合わせ、そのようにしてできる m 個の円分整数の総和を計算し p でわった余りを求めているだけである。ただし、ここで、掛け算や足し算は円分整数としてのそれであり、また、各円分整数 z_i は B に属しているのでその (ζ に関する) 各係数は 0 か 1 であることに注意する。とても単純な関数だが、驚くべきことに、

定理 1 関数 H は、最短円分整数問題の困難性のもとで衝突困難である。

パラメータの具体的な値としては $n = 64, m = 16, p = 257$ が推奨されている。このとき、B^m の要素は $1024 (= nm)$ ビット、$\mathbb{Z}_p[\zeta]$ の要素は約 $512 (= n \log(p))$ ビットとなる。

例 3 円の 3 分整数の場合 ($n = 2, \zeta = (-1 + \sqrt{-3})/2$) に関数 H の計算例を示す。($n = 2$ では小さすぎて衝突困難ではないが。) $m = 6, p = 5$ とする。

まず、$m = 6$ 個の、$\mathbb{Z}_5$ に係数をもつランダムな円分整数を選んでおく:

$$\begin{aligned} a_1 &= 2 + 3\zeta, a_2 = 4 + \zeta, a_3 = 1 + 3\zeta \\ a_4 &= 1 + 0\zeta, a_5 = 3 + 2\zeta, a_6 = 2 + 2\zeta \end{aligned}$$

入力

$$\begin{aligned} z_1 = 0 + \zeta, z_2 = 1 + 0\zeta, z_3 = 0 + 0\zeta \\ z_4 = 1 + \zeta, z_5 = 0 + \zeta, z_6 = 1 + \zeta \end{aligned}$$

における関数 H の値を計算する。(この入力 $(z_1, \ldots, z_6)$ はビット列としては $z = 011000110111$ と表される。)

$$\begin{aligned} w &= H(z_1, z_2, z_3, z_4, z_5, z_6) \\ &= a_1 z_1 + a_2 z_2 + a_3 z_3 + a_4 z_4 + a_5 z_5 + a_6 z_6 \\ &= (2 + 3\zeta)(\zeta) + (4 + \zeta)(1) + (1 + 3\zeta)(0) + (1)(1 + \zeta) + (3 + 2\zeta)(\zeta) + (2 + 2\zeta)(1 + \zeta) \\ &= -3 - \zeta + 4 + \zeta + 0 + 1 + \zeta - 2 + \zeta + 2\zeta \\ &\equiv 0 + 4\zeta \pmod 5 \end{aligned}$$

以上より、w の係数に現れた 0 を 000、4 を 100 とビット表示すると、圧縮関数 H はバイナリ文字列 $z = 011000110111$ をバイナリ文字列 $w = 000100$ に圧縮することがわかる。

証明のアイデア　定理 1 の証明についてそのアイデアを説明する。(あくまでアイデアの説明であって細部にはこだわらない。) 背理法を用いて、関数

$$H(z_1, \ldots, z_m) = a_1 z_1 + a_2 z_2 + \cdots + a_m z_m \bmod p$$

が衝突困難でないと仮定すると、$H(x_1, \ldots, x_m) = H(y_1, \ldots, y_m)$ となる、異なる $x = (x_1, \ldots, x_m) \in B$ と $y = (y_1, \ldots, y_m) \in B$ を求められることになる。$z = (z_1, \ldots, z_m) = (x_1 - y_1, \ldots, x_m - y_m)$ とすると

$$\begin{aligned} H(z_1, \ldots, z_m) &= a_1 z_1 + a_2 z_2 + \cdots + a_m z_m \\ &= a_1(x_1 - y_1) + a_2(x_2 - y_2) + \cdots + a_m(x_m - y_m) \\ &= (a_1 x_1 + a_2 x_2 + \cdots + a_m x_m) - (a_1 y_1 + a_2 y_2 + \cdots + a_m y_m) \\ &\equiv 0 \pmod{p} \end{aligned}$$

となる。よって、関数 H が衝突困難でないとの仮定のもとでは、我々は $H(z_1, \ldots, z_m) = 0$ となる (0 ではない) 短いベクトル $(z_1, z_2, \ldots, z_m)$ を求めることができる。(x も y も B に属しているので、その差 z は小さい。) このことを利用すると、どんなイデアル I_f についても、下記のように、その最短円分整数問題を解くことができることとなってしまい、最短円分整数問題は困難であるとの仮定に反する。

$H(z_1, \ldots, z_m) = 0$ となる (0 ではない) 短いベクトル $(z_1, z_2, \ldots, z_m)$ を求めることができることを仮定して、与えられたイデアル I_f について、最短円分整数問題を解く。方針として、円分整数 $g \in I_f$ が与えられると、それよりも短い I_f に属する円分整数 h を新たに求めることができることを示す。これを繰り返せば最短円分整数に辿り着く。

与えられた円分整数 $g \ (\in I_f)$ が生成する基本領域、すなわち、n 個のベクトル $g, g\zeta, ..., g\zeta^{n-1}$ を辺とする基本平行体 (平行四辺形の多次元版) を $U(g, g\zeta, ..., g\zeta^{n-1})$ とする (図 4 参照)。$i = 1, 2, \ldots, m$ について以下を繰り返す。

- 基本領域 $U(g, g\zeta, ..., g\zeta^{n-1})$ から一様ランダムにベクトル y_i を選択する。y_i は円分整数とはならない、円分 “実数”。
- 円分実数 $w_i = py_i/g$ にもっとも近い円分整数 $a_i \in \mathbb{Z}_p[\zeta]$ を求める (図 4)。この円分整数 a_i は、基本領域 $U(g, g\zeta, ..., g\zeta^{n-1})$ を $p \times p$ の p^2 個のタイルに分割したとき、ランダムに選択しておいたベクトル y_i がそれら p^2 個のタイルのうち、どのタイルに属しているかを表す。

以上によって得られた m 個の a_i (ベクトル y_i の一様性により、a_i も $\mathbb{Z}_p[\zeta]$ 上に一様分布する) が定義する関数 H に対して、$a_1 z_1 + \cdots + a_m z_m \equiv 0 \pmod{p}$ となる短いベクトル $z = (z_1, \ldots, z_m)$ を求め (背理法の仮定)、

$$h = (g(w_1 - a_1)/p - y_1)z_1 + \cdots + (g(w_m - a_m)/p - y_m)z_m$$

を計算すると、h は g より短い、イデアル I_f に属する円分整数となる。z が短いこと、g を p で割っていることより、h は g よりも短くなる。また、p で割っているために、h は f の円

分整数倍ではないように見え、イデアル I_f の外に出てしまいそうだが、$a_1 z_1 + \cdots + a_m z_m$ が p の倍数であることから、h が分数であるのは見かけだけで、実際には f の円分整数倍となり、イデアル I_f に属すことがわかる。

上記の証明のアイデアでは、ひとつ本質的に重要な点が欠落している。「基本領域 $U(g, g\zeta, ..., g\zeta^{n-1})$ から一様ランダムにベクトル y_i を選択する」としているが、ベクトル y_i は円分整数ではなく、円分 “実数” である。効率的なアルゴリズムには、このような一様な円分実数をサンプリングすることは不可能である (基本領域 $U(g, g\zeta, ..., g\zeta^{n-1})$ には無限の円分実数がつまっている)。そこで、実際の証明では、一様分布のかわりに適度な分散をもつガウス分布を用い、ベクトル y_i のサンプリングを可能としつつ、上記 m 個の a_i の分布が $\mathbb{Z}_p[\zeta]$ 上の一様分布に十分近くなるよう工夫しなければならない。

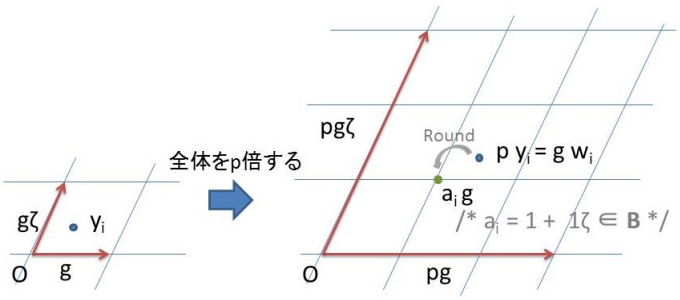

図 4: 基本領域 $U(g, g\zeta, ..., g\zeta^{n-1})$ を $p \times p$ の p^2 個のタイルに分割する

4 円分整数を用いた準同型暗号の構成

準同型暗号とは、暗号化したままで足し算・掛け算ができる暗号のことをいう。その構成は長い間未解決だった。

鍵生成 公開鍵 pk と秘密鍵 sk を生成する。

暗号化 公開鍵 pk を用いて平文 m を暗号化する:

$$\mathsf{c} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m})$$

復号 秘密鍵 sk を用いて暗号文 c を復号する:

$$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{c})$$

足し算・掛け算 $\mathsf{c}_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}_1)$, $\mathsf{c}_2 \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}_2)$ のとき、和 $\mathsf{c}_1 + \mathsf{c}_2$ や積 $\mathsf{c}_1 \dot{\mathsf{c}}_2$ を計算することができ、

$$\begin{aligned} \mathsf{Dec}(\mathsf{sk}, \mathsf{c}_1 + \mathsf{c}_2) &= \mathsf{m}_1 + \mathsf{m}_2 \\ \mathsf{Dec}(\mathsf{sk}, \mathsf{c}_1 \cdot \mathsf{c}_2) &= \mathsf{m}_1 \cdot \mathsf{m}_2 \end{aligned}$$

となる。

4.1 Ring-LWE 問題

正の整数 m を選択する。以下、$n = \phi(m)$ とし、円分整数とは円の m 分整数を意味するものとする。正の整数であるモジュラス q を選択する。(ζ に関する) 各係数が 0 か 1 である円分整数 s および各係数が $(-q/2, q/2]$ の範囲の円分整数 a をそれぞれ一様ランダムに選ぶ:

$$s \leftarrow \mathbb{Z}^{(2)}[\zeta], \quad a \leftarrow \mathbb{Z}^{(q)}[\zeta].$$

さらに、ある $\sigma > 0$ について、平均 0、分散 σ^2 のガウス分布 $\mathrm{N}(0, \sigma^2)$ から実数をサンプルし (図 5 参照)、もっとも近い整数に丸め込んだものを (ζ の) 各係数にもつ、円分整数 e を生成する:

$$e \leftarrow \mathrm{Round}(\mathrm{N}(0, \sigma^2)) + \mathrm{Round}(\mathrm{N}(0, \sigma^2))\zeta + \cdots + \mathrm{Round}(\mathrm{N}(0, \sigma^2))\zeta^{n-1}.$$

円分整数 a を s 倍し、ノイズ e を加えて、各係数についてモジュラス q でわった余りをとって b を得る (余りは $(-q/2, q/2]$ の範囲にとる):

$$b = [as + e]_q.$$

このとき、円分整数 a と b を与えられて、円分整数 s を求める問題を **Ring-LWE 問題**という。(ノイズ e と s は、求まるときは同時に求まるので、ノイズ e を求めることも暗黙の内に問題の一部となっている。) 方程式として書けば、未知数 S と E について円分整数上の一次方程式

$$b \equiv aS + E \pmod{q}$$

を解けということである。

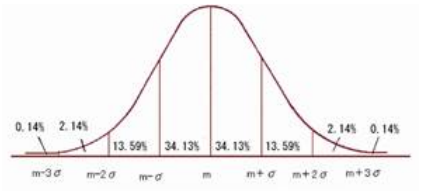

図 5: ガウス分布 $N(m, \sigma^2)$

n が十分大きいとき (数百以上)、ノイズレベル σ をうまく選ぶと Ring-LWE 問題は (量子計算機を用いても) 難問と考えられている。

もしもノイズレベル σ が余りに大きいと、Ring-LWE 問題における e について、$[e]_q$ が $\mathbb{Z}^{(q)}[\zeta]$ 上の一様分布に統計的に極めて近くなってしまう。そうすると問題の a と b が統計的に独立になってしまうため、Ring-LWE 問題は無限の計算能力があっても解けない、つまり問題として意味がないことになる。一方、ノイズレベル σ が余りに小さいと、極端に 0 であったとすると、Ring-LWE 問題はやさしい問題となってしまう。b を a で割れば s が (そして e が) 求まる。

このように、Ring-LWE 問題が意味のある難問であるには、よいノイズレベル σ を選ぶ必要があるが、幸いなことにそのようなよいノイズレベル σ をモジュラス q にくらべて十分小さい範囲にとれることが知られている。このとき、ノイズ e の各係数は $(-q/2, q/2]$ の範囲に余裕をもって収まることになる。

例 4 円の 3 分整数の場合 ($m = 3, n = 2, \zeta = (-1 + \sqrt{-3})/2$) に、Ring-LWE 問題の例を示す (このサイズではもちろん難問ではない)。モジュラスを $q = 65$ とし、ノイズレベルを $\sigma = 2$ とする。a を $\mathbb{Z}^{(65)}[\zeta]$ から一様ランダムに選ぶ (係数は-32 以上 32 以下):

$$a = -19 - 8\zeta.$$

s を $\mathbb{Z}^{(2)}[\zeta]$ から一様ランダムに選ぶ (係数は 0 か 1):

$$s = 1 + \zeta.$$

e(の各係数) をガウス分布 N(0,4) にしたがって生成する:

$$e = 1 - \zeta.$$

このとき、

$$as + e = (-19 - 8\zeta)(1 + \zeta) + 1 - \zeta = -10 - 20\zeta.$$

よって、

$$b = [as + e]_{65} = -10 - 20\zeta$$

となる。

この a と b について、LWE 問題

$$b \equiv aS + E \pmod{65}$$

は、$S = S_0 + S_1\zeta$, $E = E_0 + E_1\zeta$ として、

$$-10-20\zeta \equiv (-19-8\zeta)(S_0+S_1\zeta)+(E_0+E_1\zeta) \equiv (-19S_0+8S_1+E_0)+(-8S_0-11S_1+E_1)\zeta$$

となる。成分ごとに比較すると、結局、

$$\begin{aligned} -19S_0 + 8S_1 + E_0 &\equiv -10 \pmod{65} \\ -8S_0 - 11S_1 + E_1 &\equiv -20 \pmod{65} \end{aligned}$$

を解け、ということである。答えはもちろん上で生成したもので、$S_0 = 1, S_1 = 1, E_0 = 1, E_1 = -1$ である。ここで、もしもノイズ E_0, E_1 の項がなければ、これは通常の連立一次方程式の求解にすぎないこと、また、次元 n が十分大きくなると、ノイズ $E = E_0 + E_1\zeta + \cdots + E_{n-1}\zeta^{n-1}$ のとりうる値のパターン数は n について指数関数的に増加することに注意する。

4.2 準同型暗号の構成

文献 [1, 2] の準同型暗号を紹介する。

鍵生成アルゴリズム:

- 正の整数 m を選択する。以下、$n = \phi(m)$ とし、円分整数とは円の m 分整数を意味するものとする。さらに、暗号文モジュラスとして奇数 q を、ノイズレベルとして σ を選択する。σ は q にくらべて十分小さくとる。
- '小さな' 一様乱数 s と '大きな' 一様乱数 a を選ぶ: $s \leftarrow \mathbb{Z}^{(2)}[\zeta]$, $a \leftarrow \mathbb{Z}^{(q)}[\zeta]$.
- ノイズレベル σ のノイズ e を生成する: $e \leftarrow \mathrm{Round}(\mathrm{N}(0,\sigma^2)) + \mathrm{Round}(\mathrm{N}(0,\sigma^2))\zeta + \cdots + \mathrm{Round}(\mathrm{N}(0,\sigma^2))\zeta^{n-1}$.
- a を s 倍したものに 2 倍したノイズ$2e$ を加えて b とする: $b = [as + 2e]_q$.
- s を秘密鍵 sk とし、(a, b) を公開鍵 pk とする: $\mathsf{sk} = s$, $\mathsf{pk} = (a, b)$.

$\mathsf{sk} = s$ と $\mathsf{pk} = (a, b)$ は、その作り方から

$$b - as \equiv 2e \pmod{q}$$

を満たす。ここで、ノイズレベル σ の約束から、$2e$ の各係数は q にくらべて十分小さいので、それらはいずれも区間 $(-q/2, q/2]$ に入るとしてよい。したがって、

$$[b - as]_q = 2e \tag{2}$$

となることに注意する。

この鍵生成は、ノイズが 2 倍されることをのぞき、Ring-LWE 問題の生成と同じである。Ring-LWE 問題の困難性より、公開鍵 $\mathsf{pk} = (a, b)$ から秘密鍵 $\mathsf{sk} = s$ を求めることはできない。

例 5 円の 3 分整数の場合 $(m = 3, n = 2, \zeta = (-1 + \sqrt{-3})/2)$ を例に取り、鍵生成アルゴリズムの動作をトレースする。

- モジュラス $q = 65$ をとり, エラーレベルを $\sigma = 2$ とする。
- 乱数 s と乱数 a を生成する。$s = 1 + \zeta \leftarrow \mathbb{Z}^{(2)}[\zeta]$, $a = -19 - 8\zeta \leftarrow \mathbb{Z}^{(65)}[\zeta]$.
- ノイズレベル $\sigma = 2$ にしたがい、ノイズ e を生成する。$e = 1 - \zeta \leftarrow \mathrm{N}(0, 4)$.
- $as + 2e = (-19 - 8\zeta)(1 + \zeta) + 2(1 - \zeta) = -9 - 21\zeta$ より、$b = [as + 2e]_{65} = -9 - 21\zeta$ となるので、秘密鍵は $\mathsf{sk} = s = 1 + \zeta$, 公開鍵は $\mathsf{pk} = (a = -19 - 8\zeta, b = -9 - 21\zeta)$ となる。

このとき、

$$b - as = (-9 - 21\zeta) - (-19 - 8\zeta)(1 + \zeta) = 2 - 2\zeta$$

より、確かに、

$$[b - as]_{65} = 2 - 2\zeta = 2e$$

となっている。

暗号化アルゴリズム:

公開鍵 $\mathsf{pk} = (a, b)$ を用いて n ビット文字列である平文 $\mathsf{m} = (m_0, \ldots, m_{n-1})$ を以下のように暗号化する。(各 m_i は 0 か 1.)

- 平文 m を円分整数 $m \in Z^{(2)}[\zeta]$ に変換する:

$$m = m_0 + m_1\zeta + \cdots + m_{n-1}\zeta^{n-1}.$$

- '小さい' 乱数 v と 2 つのノイズ e_0, e_1 を生成する:

$$v \leftarrow \mathbb{Z}^{(2)}[\zeta], \;\; e_0, e_1 \leftarrow \mathrm{N}(0, \sigma^2).$$

- pk に含まれる b を v 倍したものにノイズ e_0 の 2 倍と平文 m を加えて (平文はノイズ扱い!)、暗号文の第 1 成分とする:

$$c_0 = [bv + 2e_0 + m]_q.$$

- pk に含まれる a を v 倍したものにノイズ e_1 の 2 倍を加えて、暗号文の第 2 成分とする:

$$c_1 = [av + 2e_1]_q.$$

- 暗号文 $\mathsf{c} = (c_0, c_1)$ を出力する。

暗号文 $\mathsf{c} = (c_0, c_1)$ を観察する。鍵生成の方法を思い出すと、公開鍵 pk に含まれる (a, b) は Ring-LWE 問題を表していて、b は a の秘密鍵 s 倍にノイズを加えた形になっていた。同様に、暗号文の第 1 成分 c_0 は、第 2 成分 c_1 の s 倍にノイズを加えた形となっている (c_0 と c_1 の計算において同じ乱数 v を用いていることに注意)。すなわち、暗号文 $\mathsf{c} = (c_0, c_1)$ もまた Ring-LWE 問題の問題文に他ならず、Ring-LWE 問題の困難性より、それからノイズの一部である平文 m を求めることはできない。逆の見方をすると、公開鍵 $\mathsf{pk} = (a, b)$ は平文 $m = 0$ の暗号文であるとも言える。

復号アルゴリズム:

秘密鍵 $\mathsf{sk} = s$ を用いて暗号文 $\mathsf{c} = (c_0, c_1)$ を以下のように復号する。

- 暗号文の第 1 成分 c_0 から第 2 成分 c_1 の s 倍を引き、q でわった余りをとり、続いて 2 でわった余りをとる:

$$m = [[c_0 - sc_1]_q]_2$$

- m の各係数 (0 または 1) を連結して平文 m を得る。

復号アルゴリズムが、与えられた暗号文を正しい平文に復号することを見る。暗号文 $\mathsf{c} = (c_0, c_1)$ に対して、

$$\begin{aligned} c_0 - sc_1 &\equiv bv + 2e_0 + m - s(av + 2e_1) \\ &\equiv (b - as)v + 2e_0 - 2se_1 + m \\ &\equiv 2ev + 2e_0 - 2se_1 + m \\ &\equiv m + 2(ev + e_0 - se_1) \pmod{q} \end{aligned}$$

ここで q と比べて e, e_0, e_1, v や s は小さかった。よって、$2(ev + e_0 - se_1)$ も q にくらべて小さい。m もその各係数は 0 か 1 である。よって、それらの和である $m + 2(ev + e_0 - se_1)$ も q にくらべて小さく、その各係数は $(-q/2, q/2]$ の範囲に収まっているとしてよい。よって、

$$[c_0 - sc_1]_q = m + 2(ev + e_0 - se_1)$$

となり、mod2 をとって、

$$[[c_0 - sc_1]_q]_2 = m$$

となる。

例 6 円の 3 分整数の場合に暗号化アルゴリズムの動作をトレースする。例 5 で計算した、公開鍵 $\mathsf{pk} = (a = -19 - 8\zeta, b = -9 - 21\zeta)$ を用いて平文 $\mathsf{m} = 11$ を暗号化する。

- m を円分整数 m に変換する: $m = 1 + \zeta$.
- 小さな乱数 v を生成する: $v = 1 + \zeta \leftarrow \mathbb{Z}^{(2)}[\zeta]$.
- ノイズ e_0, e_1 を生成する: $e_0 = -1 + \zeta, e_1 = -\zeta \leftarrow \mathrm{N}(0, 4)$.
- 暗号文の第 1 成分 c_0 を計算する: $bv + 2e_0 + m = (-9 - 21\zeta)(1 + \zeta) + 2(-1 + \zeta) + (1 + \zeta) = 11 - 6\zeta$. よって、$c_0 = [11 - 6\zeta]_{65} = 11 - 6\zeta$.
- 暗号文の第 2 成分 c_1 を計算する: $av + 2e_1 = (-19 - 8\zeta)(1 + \zeta) + 2(-\zeta) = -11 - 21\zeta$. よって、$c_1 = [-11 - 21\zeta]_{65} = -11 - 21\zeta$.
- 暗号文 c を出力する: $\mathsf{c} = (c_0 = 11 - 6\zeta, c_1 = -11 - 21\zeta)$.

同様にして、平文 $\mathsf{m}' = 01$ を暗号化する。

- m' を円分整数 m' に変換する: $m' = \zeta$.
- 小さな乱数 v を生成する: $v = \zeta \leftarrow \mathbb{Z}^{(2)}[\zeta]$.
- ノイズ e_0, e_1 を生成する: $e_0 = \zeta, e_1 = 2 \leftarrow \mathrm{N}(0, 4)$.
- 暗号文の第 1 成分 c_0' を計算する: $bv + 2e_0 + m' = (-9 - 21\zeta)\zeta + 2\zeta + \zeta = 21 + 15\zeta$. よって、$c_0' = [21 + 15\zeta]_{65} = 21 + 15\zeta$.

- 暗号文の第 2 成分 c'_1 を計算する: $av + 2e_1 = (-19 - 8\zeta)\zeta + 2 \cdot 2 = 12 - 11\zeta$. よって、$c'_1 = [12 - 11\zeta]_{65} = 12 - 11\zeta$.
- 暗号文 c' を出力する: $\mathsf{c}' = (c'_0 = 21 + 15\zeta, c'_1 = 12 - 11\zeta)$.

つづいて、秘密鍵 $\mathsf{sk} = s = 1 + \zeta$ を用いて上で計算した暗号文 $\mathsf{c} = (c_0 = 11 - 6\zeta, c_1 = -11 - 21\zeta)$ を復号する。

- 暗号文の第 1 成分 c_0 から第 2 成分 c_1 の s 倍を引く: $c_0 - sc_1 = 11 - 6\zeta - (1+\zeta)(-11 - 21\zeta) = 11 - 6\zeta - (10 - 11\zeta) = 1 + 5\zeta$. よって、$[c_0 - sc_1]_{65} = 1 + 5\zeta$ となるので、$m = [[c_0 - sc_1]_{65}]_2 = 1 + \zeta$.
- 平文 $\mathsf{m} = 11$ を得る。

同様に、2 つ目の暗号文 $\mathsf{c}' = (c'_0 = 21 + 15\zeta, c'_1 = 12 - 11\zeta)$ を復号する。

- 暗号文の第 1 成分 c'_0 から第 2 成分 c'_1 の s 倍を引く: $c'_0 - sc'_1 = 21 + 15\zeta - (1 + \zeta)(12 - 11\zeta) = 21 + 15\zeta - (23 + 12\zeta) = -2 + 3\zeta$. よって、$[c'_0 - sc'_1]_{65} = -2 + 3\zeta$ となり、$m' = [[c'_0 - sc'_1]_{65}]_2 = \zeta$.
- 平文 $\mathsf{m}' = 01$ を得る。

暗号文どうしの加算

暗号文 $\mathsf{c} = (c_0, c_1)$ は平文 m を暗号化し、暗号文 $\mathsf{c}' = (c'_0, c'_1)$ は平文 m' を暗号化しているとする。このとき、小さな円分整数 e, e' があって、

$$\begin{aligned} c_0 - sc_1 &\equiv m + 2e \pmod q \\ c'_0 - sc'_1 &\equiv m' + 2e' \pmod q. \end{aligned}$$

となっていた。両辺を加えると、

$$(c_0 + c'_0) - s(c_1 + c'_1) \equiv (m + m') + 2(e + e') \pmod q$$

となる。これは、ノイズ $2(e + e')$ が小さいことに注意すると、$\mathsf{d} = (c_0 + c'_0, c_1 + c'_1)$ が $m + m'$ の暗号文であることを示す。以上より、

- 加算アルゴリズム: 入力暗号文 $\mathsf{c} = (c_0, c_1)$ と $\mathsf{c}' = (c'_0, c'_1)$ に対し、

  $$\mathsf{d} = ([c_0 + c'_0]_q, [c_1 + c'_1]_q)$$

  を出力する。

例 7 円の 3 分整数の場合に暗号文の加算アルゴリズムの動作をトレースする。例 6 で計算した、2 つの暗号文

$$\begin{aligned} \mathsf{c} &= (c_0 = 11 - 6\zeta, c_1 = -11 - 21\zeta) \\ \mathsf{c}' &= (c'_0 = 21 + 15\zeta, c'_1 = 12 - 11\zeta) \end{aligned}$$

を加える。対応する平文はそれぞれ、$\mathsf{m}=11$ と $\mathsf{m}'=01$ であり、円分整数としては $m=1+\zeta$ と $m'=\zeta$ と表されていた。

2 つの暗号文 c, c' を円分整数として加え、係数ごとにモジュラス $q=65$ でわった余りをとれば、暗号文 $\mathsf{d}=c+c'=([11-6\zeta+21+15\zeta]_{65}, [-11-21\zeta+12-11\zeta]_{65})=(32+9\zeta, 1-32\zeta)$ が得られる。

暗号文 d を秘密鍵 s を使って復号すると、$d_0-sd_1 = 32+9\zeta-(1+\zeta)(1-32\zeta) = 32+9\zeta-(33+\zeta) = -1+8\zeta$. よって、$[d_0-sd_1]_{65}=-1+8\zeta$ となるので、復号結果は $[[d_0-sd_1]_{65}]_2=1$. これは確かに、$m'+m''=(1+\zeta)+\zeta\equiv 1 \pmod 2$ に等しい。

暗号文どうしの掛け算

暗号文 $\mathsf{c}=(c_0,c_1)$ は平文 m を暗号化し、暗号文 $\mathsf{c}'=(c_0',c_1')$ は平文 m' を暗号化しているとする。このとき、小さな円分整数 e, e' があって、

$$\begin{aligned} c_0-sc_1 &\equiv m+2e \pmod q \\ c_0'-sc_1' &\equiv m'+2e' \pmod q. \end{aligned}$$

となっていた。辺々を掛けると、

$$\begin{aligned} (c_0-sc_1)\cdot(c_0'-sc_1') &\equiv (m+2e)(m'+2e') \pmod q \\ c_0c_0'-s(c_1c_0'+c_0c_1')+s^2c_1c_1' &\equiv mm'+2(em'+e'm+2ee') \pmod q. \end{aligned}$$

となる。よって、

$$d_0=c_0c_0',\ \ d_1=c_1c_0'+c_0c_1',\ \ d_2=-c_1c_1'$$

とおけば、(d_0,d_1,d_2) は「秘密鍵 (s,s^2) に関する積 mm' の暗号文」となっていることが観察される:

$$d_0-sd_1-s^2d_2\equiv mm'+2e'' \pmod q.$$

ここで、$e''=em'+e'm+2ee'$ とした。この新たな暗号文 (d_0,d_1,d_2) は、入力暗号文 c と c' のみから計算できることに注意する。しかし、肝心の s^2 は秘密鍵に入っていないので、このままでは復号者が困ってしまう。そこで、$-s^2$ の暗号文 (A,B) を用意して、公開鍵にいれておこう。A を $\mathbb{Z}^{(q)}[\zeta]$ からランダムに選び、ガウスノイズ $e(\leftarrow \mathrm{N}(0,\sigma^2))$ を用いて、

$$B=As-s^2+2e \pmod q$$

とする。このようにして得られる、$-s^2$ の暗号文 (A,B) は**スイッチ鍵**と呼ばれる。

しかし、このままでは、2 成分の暗号文 (c_0,c_1) と (c_0',c_1') どうしを掛けると 3 成分 (d_0,d_1,d_2) の暗号文となってしまう。すると、この 3 成分 (d_0,d_1,d_2) の暗号文と通常の 2 成分の暗号文 (c_0,c_1) の積を考え、さらにその結果生じる 5 成分の暗号文と $\cdots$、という具合に収拾がつかなくなってくる。3 成分 (d_0,d_1,d_2) の暗号文を通常の 2 成分の暗号文に変換する方法はないものか。

次のように d_2 成分を d_0,d_1 に重ね合わせてみてはどうだろうか?

$$d_0':=d_0+Bd_2,\ \ d_1':=d_1+Ad_2.$$

これを秘密鍵 s で復号すると、

$$\begin{aligned} d'_0 - sd'_1 &= (d_0 + Bd_2) - s(d_1 + Ad_2) = (d_0 - sd_1) + (B - As)d_2 \\ &\equiv (d_0 - sd_1) + (-s^2 + 2e)d_2 \pmod{q} \\ &\equiv (d_0 - sd_1 - s^2 d_2) + 2ed_2 \pmod{q} \\ &\equiv mm' + 2e'' + 2ed_2 \pmod{q}. \end{aligned}$$

一見、うまくいったように見えるが、よく見ると ed_2 は小さくはない! そのため、$mm' + 2e'' + 2ed_2$ はモジュラス q より大きくなり、復号に失敗してしまう:

$$[d'_0 - sd'_1]_q \neq mm' + 2e'' + 2ed_2.$$

モジュラスブースト

この困難はモジュラスブーストと呼ばれる手法で回避することができる。エラーが大きくなってしまうのなら、その分モジュラスも一時的に大きくすればよい、という発想である。

まず、モジュラス q と同程度の大きさの奇数 P を用意する。そして、以下を満たす、$-Ps^2$ の暗号文 (A, B) を計算しておく:

$$B - As \equiv -Ps^2 + 2e \pmod{Pq}.$$

(つまり、mod$P$ で 0 になるようにしてスイッチ鍵 (A, B) を modPq に引き上げた。) さらに、

$$d'_0 = Pd_0 + Bd_2, \;\; d'_1 = Pd_1 + Ad_2$$

とおく。(d_0, d_1 も Pd_0, Pd_1 にブーストしている。) すると、これを秘密鍵 s で復号すると

$$\begin{aligned} d'_0 - sd'_1 &= (Pd_0 + Bd_2) - s(Pd_1 + Ad_2) \\ &= (Pd_0 - sPd_1) + (B - As)d_2 \\ &\equiv (Pd_0 - sPd_1) + (-Ps^2 + 2e)d_2 \pmod{Pq} \\ &\equiv P(d_0 - sd_1 - s^2 d_2) + 2ed_2 \pmod{Pq} \\ &\equiv P(mm' + 2e'') + 2ed_2 \pmod{Pq} \end{aligned}$$

よって、

$$d'_0/P - sd'_1/P \equiv mm' + 2e'' + (2ed_2)/P \pmod{q}.$$

今度は、$2e'' + (2ed_2)/P$ は q にくらべて十分小さいので

$$[d'_0/P - sd'_1/P]_q = mm' + 2e'' + (2ed_2)/P$$

となり、無事に積 mm' に復号される。

以上より、下記の暗号文の乗算アルゴリズムが得られる。

- 乗算アルゴリズム: スイッチ鍵 (A,B) を用いて、入力暗号文 (c_0,c_1) と (c'_0,c'_1) の積 (d''_0,d''_1) を以下のように計算する。(スイッチ鍵 (A,B) はブースト用の奇数 P について、$B-As\equiv -Ps^2+2e \pmod{Pq}$ を満たすのだった。)

  1. 3 成分暗号文 (d_0,d_1,d_2) を計算する:
  $$d_0=[c_0c'_0]_q,\ \ d_1=[c_1c'_0+c_0c'_1]_q,\ \ d_2=[-c_1c'_1]_q.$$
  2. スイッチ鍵 (A,B) を用いて、モジュラス Pq にブーストしながら、3 成分暗号文 (d_0,d_1,d_2) を 2 成分暗号文 (d'_0,d'_1) に変換する:
  $$d'_0=[Pd_0+Bd_2]_{Pq},\ \ d'_1=[Pd_1+Ad_2]_{Pq}$$
  3. ブースト用奇数 P で割ることで、2 成分暗号文 (d'_0,d'_1) のモジュラスを元の q に戻す:
  $$d''_0=[(d'_0-\delta_0)/P]_q,\ \ d''_1=[(d'_1-\delta_1)/P]_q$$
  ここで δ_i は以下を満たすようになるべく小さくとる (i=0,1):
  $$d'_i-\delta_i\equiv 0 \pmod P,\ \ \delta_i\equiv 0 \pmod 2.$$

上記ステップ 3 では、P で割る際に分数が出て来ないよう $\delta_i(\equiv d'_i \bmod P)$ を d'_i から引いてから P で割っている。このようにしても、δ_i を偶数にとっているので復号結果には影響しない。

例 8 円の 3 分整数の場合に暗号文の乗算アルゴリズムの動作をトレースする。

ブースト用の奇数として $P=67$ を選ぶ。(モジュラスは $q=65$ だった。)

まず、スイッチ鍵 ($=-Ps^2$ の暗号文) を計算する。$s=1+\zeta$ なので、$-Ps^2=-67(1+\zeta)^2=-67\zeta$. これををモジュラス $qP=65\cdot 67=4355$ で暗号化する。乱数 $A=2116+1119\zeta\leftarrow\mathbb{Z}^{(4355)}[\zeta]$ とガウスノイズ $e=1-\zeta\leftarrow \mathrm{N}(0,4)$ を用いて、

$$As-Ps^2+2e=(2116+1119\zeta)(1+\zeta)-67\zeta+2(1-\zeta)=999+2047\zeta.$$

よって、$B=[999+2047\zeta]_{4355}=999+2047\zeta$ となり、スイッチ鍵 $(A,B)=(2116+1119\zeta,999+2047\zeta)$ を得る。

このスイッチ鍵 (A,B) を用いて、例 6 で計算した、2 つの暗号文

$$\begin{aligned}\mathsf{c} &= (c_0=11-6\zeta,c_1=-11-21\zeta)\\ \mathsf{c}' &= (c'_0=21+15\zeta,c'_1=12-11\zeta)\end{aligned}$$

の積を計算する。対応する平文はそれぞれ、$\mathsf{m}=11$ と $\mathsf{m}'=01$ であり、円分整数としては $m=1+\zeta$ と $m'=\zeta$ と表されていた。

1. 3 成分暗号文 (d_0,d_1,d_2) を計算する。$c_0c'_0=(11-6\zeta)(21+15\zeta)=321+129\zeta$ より、$d_0=[321+129\zeta]_{65}=-4-\zeta$ となる。また、$c_1c'_0+c_0c'_1=(-11-21\zeta)(21+15\zeta)+(11-6\zeta)(12-11\zeta)=84-291\zeta+66-259\zeta=150-550\zeta$ より $d_1=[150-550\zeta]_{65}=$

$20-30\zeta$ を得る。さらに、$-c_1c_1' = -(-11-21\zeta)(12-11\zeta) = 363+362\zeta$ なので、$d_2 = [363+362\zeta]_{65} = -27-28\zeta$ となる。

今、仮に秘密鍵として s に加えて s^2 も持っていたとして、この 3 成分暗号文 (d_0, d_1, d_2) を復号してみると、$d_0 - sd_1 - s^2d_2 = -4-\zeta-(1+\zeta)(20-30\zeta)-(1+\zeta)^2(-27-28\zeta) = -4-\zeta-50-20\zeta-28-\zeta = -82-22\zeta$. よって、復号結果は、$[d_0 - sd_1 - s^2d_2]_{65} = -17-22\zeta \equiv 1 \pmod 2$ となるが、確かに $m \cdot m' = (1+\zeta)\zeta \equiv 1 \pmod 2$ なので、正しく復号されていることが確認できる。

2. スイッチ鍵 (A, B) を用いて、モジュラス $Pq = 67 \cdot 65 = 4355$ にブーストしながら 3 成分暗号文 (d_0, d_1, d_2) を 2 成分暗号文 (d_0', d_1') に変換する。

$$\begin{aligned} Pd_0 + Bd_2 &= 67 \cdot (-4-\zeta) + (999+2047\zeta)(-27-28\zeta) \\ &= -268 - 67\zeta + 30343 - 25925\zeta = 30075 - 25992\zeta. \end{aligned}$$

よって、$d_0' = [30075 - 25992\zeta]_{4355} = -410 + 138\zeta$ を得る。また、

$$\begin{aligned} Pd_1 + Ad_2 &= 67 \cdot (20-30\zeta) + (2116+1119\zeta)(-27-28\zeta) \\ &= 1340 - 2010\zeta - 25800 - 58129\zeta = -24460 - 60139\zeta. \end{aligned}$$

よって、$d_1' = [-24460 - 60139\zeta]_{4355} = 1670 + 831\zeta$ となる。

3. 2 成分暗号文 (d_0', d_1') を $P = 67$ でわってそのモジュラスを $q = 65$ に戻す。$\delta_0 = (d_0' \bmod 67) = -8+4\zeta$ となるが、これは係数がすでにすべて偶数なので、$d_0'' = [((-410+8)+(138-4)\zeta)/67]_{65} = -6+2\zeta$ を得る。同様に、$\delta_1 = (d_1' \bmod 67) = -5+27\zeta$ となるが、これは係数が偶数でないので $P \cdot (1-\zeta)$ を加えて、$\delta_1 = \delta_1 + 67 - 67\zeta = 62 - 40\zeta$ とし、$d_1'' = [((1670-62)+(831+40)\zeta)/67]_{65} = 24+13\zeta$ を得る。

以上より、2 つの暗号文 $\mathsf{c} = (c_0 = 11-6\zeta, c_1 = -11-21\zeta)$ と $\mathsf{c}' = (c_0' = 21+15\zeta, c_1' = 12-11\zeta)$ を掛けて、暗号文

$$\mathsf{d}'' = (-6+2\zeta, 24+13\zeta)$$

を得た。これを秘密鍵 $s = 1+\zeta$ で復号すると、

$$[(-6+2\zeta) - (24+13\zeta)(1+\zeta)]_{65} = [-17-22\zeta]_{65} = -17-22\zeta \equiv 1 \pmod 2$$

を得るが、確かに、 $mm' = (1+\zeta)\zeta \equiv 1 \pmod 2$ だった。

5 おわりに

円分整数の代数的性質 (足し算、掛け算) と格子としての幾何的性質がイデアル格子暗号を作り出すことを見た。そのようなイデアル格子暗号の例として、衝突困難圧縮関数と準

同型暗号をみた。他にも、プログラムコードの暗号理論的難読化や準同型署名など新しい暗号技術が続々と発明されている。従来、暗号技術とはシステムを守るための技術だったが、今や、安全な情報処理プラットフォームを実現するための基本演算機能となりつつある。すべてのデータが暗号化されて蓄積され、暗号化されたままで難読化されたプログラムによって演算処理され、知るべき存在 (人、サーバ等) だけその暗号化された演算結果を復号して知ることができる、そういうプラットフォームが可能と成りつつあるのである。

参考文献

[1] Z. Brakerski, C. Gentry, V. Vaikuntanathan, Fully homomorphic encryption without bootstrapping, ITCS ’12, 2012.
[2] Craig Gentry, Shai Halevi, and Nigel P. Smart, Homomorphic Evaluation of the AES Circuit, CRYPTO 2012, LNCS 7417, pp. 850–867, 2012.
[3] 石田信, 代数的整数論, 森北出版; POD 版 (2003/9/15).
[4] V. Lyubashevsky, D. Micciancio, Generalized Compact Knapsacks are Collision Resistant, ICALP 2006, LNCS 4052, pp. 144-155, 2006.