Vol.2019-DPS-178 No.25
Vol.2019-CSEC-84 No.25
2019/3/5

Preimage Sampleable Functionで用いられる格子上のサンプリングに対する考察

太中 裕貴[1,2,a)]　宇野 隼平[2,3]　鈴木 洋一[2]

概要：格子を用いた暗号技術は, 耐量子計算暗号の候補として近年注目をあびている. 格子暗号の応用のうち, 電子署名や ID ベース暗号等の主要な応用では主に Preimage Samplable Function というアルゴリズムを用いている. 一方で, Preimage Samplable Function で使用される離散ガウス分布の生成法は, 既存の研究では任意の分散値に対してサンプリングする一般的な方法が知られていない. そこで, 本稿では, MP12(Micciancio and Peikert, CRYPTO 2012) で提案された手法で用いられるような型の離散ガウス分布に対し, 格子の特徴を利用することで, 任意の分散値に対してサンプリングを行う手法について考察を与える. 任意の分散値に対して, サンプリングすることにより, 秘密鍵の長さを削減できることが期待できる.

キーワード：格子暗号, 離散ガウス分布, サンプリング手法

Investigatig Lattice Sampling Inspired by the Closest Vector Problem for Discrete Gaussian Sampling

Yuki Tanaka[1,2,a)]　Shumpei Uno[2,3]　Yohichi Suzuki[2]

Abstract: Lattice-based cryptographic systems have recently attracted as a candidate of post-quantum cryptography. In several known lattice-based algorithms, discrete Gaussian sampling is used. In this paper, we show one-dimensional reduction of the multi-dimensional discrete Gaussian distribution under the lattice proposed in MP12(Micciancio and Peikert, CRYPTO 2012).

Keywords: Lattice-based cryptography, Discrete Gaussian distribution, Sampling method

1. はじめに

現在用いられている RSA 暗号は, Shor[1] による量子アルゴリズムによって, 理論上多項式時間で解読できるという発見がなされた. それ以来, RSA 暗号に替わる暗号の開発が喫緊の課題になっている [2]. 特に, 安全性が重視される金融機関において, 量子コンピュータに対して耐性のある暗号への変更は必須となる. システム移行の期間を踏まえると現時点において研究・開発に取り組むべきだとの報告もなされている [3], [4]. このように, 耐量子暗号の研究開発が重要視されている中で, 耐量子暗号の候補として, 格子暗号 [5] , [6], [7] が有力視されている. 格子暗号は 耐量子性の他に暗号文のままで計算できる準同型暗号といった豊かな応用性に対しても注目を浴びている [8], [9], [10]. 本稿は, 耐量子性と応用性を有する格子暗号について, 暗号応用技術として用いる際の最も重要な要素技術の一つである Preimage Sampleable Fucntion に関する研究である. 特に Preimage Sampleable Fucntion の構成として, 有力とされる MP12[5] に着目する. 格子暗号や署名, その他の暗号応用技術において, 離散ガウス分布に従う乱数生成は重要な

[1] 三菱 UFJ トラスト投資工学研究所
Mitsubishi UFJ Trust Investment Technology Institute Co., Ltd.
[2] 慶應義塾大学 量子コンピューティングセンター
Keio University, Quantum Computing Center
[3] みずほ情報総研株式会社 サイエンスソリューション部
Mizuho Information & Research Institute department of Science Solution
[a)] ytanaka@mtec-institute.co.jp

役割を果たす [11].

MP12[5] における Preimage sampleable Function においては, 格子上の離散ガウス分布に従う乱数生成が使用されている. 一般の格子上で, 離散ガウス分布を分散値の制限なしににサンプリングすることは困難である. 既存研究 [11] の手法では, 格子の基底を $\mathbf{B}$ とセキュリティパラメータ n とした時, 分散値が $\omega(\sqrt{\log n})\|\tilde{\mathbf{B}}\|$ 以上のものに限りサンプリングできる. ただし, $\|\tilde{\mathbf{B}}\|$ は行列 $\mathbf{B}$ に対してグラムシュミット直交基底を取った場合の行列ノルムを表す. 他にも, 一般次元におけるサンプリング法として, [12] や [13] が挙げられる.

MP12[5] では, 署名や暗号を構成する度に, 次で表される格子上の離散ガウス分布に従う乱数を必要とする.

$$S_p = \begin{bmatrix} p & 0 & 0 & \cdots & 0 \\ -1 & p & 0 & \cdots & 0 \\ 0 & -1 & p & & 0 \\ \vdots & \vdots & \vdots & p & \vdots \\ 0 & 0 & \cdots & -1 & p \end{bmatrix}$$

ここで p は任意の整数である. 格子基底を S_p とするサンプリングは “G-sampling” と呼ばれる. “G-sampling” は, 様々な場面で用いられる重要なサンプリングであり [14], サンプリングを効率化する方法が研究されている [15]. 既存研究 [15] よると, 任意の modulous に対して, 分散値に制約 $\omega(\sqrt{\log n})|\tilde{S_p}|$ をつけて効率化する手法がのべられている.

本研究では, 上に示した格子基底 S_p の基底の等長性に注目し, 任意の分散値に対してサンプリングする方法を提案する.

2. 格子と離散ガウス分布の定義

以下で, 格子と離散ガウス分布の定義を与える.

定義 1. $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$ を基底にもつ格子を

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_i a_i \mathbf{b}_i \,\middle|\, \text{ここで } a_i \in \mathbb{Z} \right\}$$

で定める. 行列 $\mathbf{B}$ を格子基底, $\mathbf{b}_i$ を基底ベクトルと呼ぶ.

定義 2. 格子 $\mathcal{L}(\mathbf{B})$ 上の標準偏差が $\sigma \in \mathbb{R}$, 中心が $\mathbf{c} \in \mathbb{R}^n$ の n 次元離散ガウス分布を,

$$D_{\mathcal{L}(\mathbf{B}),\sigma,\mathbf{c}}(\mathbf{x}) = \frac{\exp\left(-\frac{1}{\sigma^2}\|\mathbf{B}\mathbf{x}-\mathbf{c}\|^2\right)}{\sum_{\mathbf{x}\in\mathbb{Z}^n}\exp\left(-\frac{1}{\sigma^2}\|\mathbf{B}\mathbf{x}-\mathbf{c}\|^2\right)} \quad (1)$$

と定義する. ここで, 確率変数 $\mathbf{x} \in \mathbb{Z}^n$ であり, $\mathbf{B}\mathbf{x} \in \mathcal{L}(\mathbf{B})$ である. また, $\|\mathbf{v}\|$ はベクトル $\mathbf{v}$ の L^2 ノルムを表す.

3. 提案アルゴリズム

本節では, MP12[5] において用いられている離散ガウス分布

$$\begin{aligned}\Pr(\mathbf{x}) &= \frac{\exp\left(-\frac{1}{\sigma^2}\|S_2\mathbf{x}-\mathbf{c}\|^2\right)}{\sum_{\mathbf{x}\in\mathbb{Z}^{3n}}\exp\left(-\frac{1}{\sigma^2}\|S_2\mathbf{x}-\mathbf{c}\|^2\right)} \\ &= D_{\mathcal{L}(S_2),\sigma,\mathbf{c}}(\mathbf{x})\end{aligned} \quad (2)$$

に従って, 離散確率変数 $\mathbf{x} \in \mathbb{Z}^{3n}$ をサンプリングする手法を提案する. ここで, 格子基底 S_2 は $\mathbb{Z}^{3n\times 3n}$ の下 2 重対角行列

$$S_2 = \begin{bmatrix} 2 & 0 & 0 & \cdots & 0 \\ -1 & 2 & 0 & \cdots & 0 \\ 0 & -1 & 2 & & 0 \\ \vdots & \vdots & \vdots & 2 & \vdots \\ 0 & 0 & \cdots & -1 & 2 \end{bmatrix} \quad (3)$$

であり, $\sigma \in \mathbb{R}$ は分布の標準偏差, $\mathbf{c} \in \mathbb{R}^{3n}$ は分布の中心である. ここでは, 一例として, 格子基底 S_2 を考えるが, 一般の S_p への拡張は容易であると考えられる.

本節で提案するアルゴリズムでは, 3.1 節で説明するような格子基底 S_2 の性質を利用することで, 確率変数 $\mathbf{x} = (x_1, x_2, \cdots, x_{3n})$ を

$$\begin{aligned} x_{3i-2} &= \alpha_1^i + \alpha_2^i + \delta^i \\ x_{3i-1} &= \alpha_1^i - \alpha_2^i \\ x_{3i} &= 21\cdot 8^{n-i}\alpha_3^i + \beta^i \\ &\quad \text{where } \alpha_1^i, \alpha_2^i, \alpha_3^i \in \mathbb{Z} \\ &\quad \delta^i \in \{0,1\}, \beta^i \in \mathbb{Z} \cap \{0 \le x \le 8^{n-i}-1\} \end{aligned} \quad (4)$$

と変数変換を行うことで, 式 (2) の同時確率分布が

$$\begin{aligned}\Pr(\mathbf{x}) = \Pr(\boldsymbol{\beta},\boldsymbol{\delta}) &\prod_{i=1}^{n}\Pr(\alpha_3^i \mid \alpha_3^{i-1}, \beta^i, \beta^{i-1}) \\ &\times \Pr(\alpha_{3i-2} \mid \alpha_3^i, \alpha_3^{i-1}, \beta^i, \beta^{i-1}, \delta^i) \\ &\times \Pr(\alpha_{3i-1} \mid \alpha_3^i, \alpha_3^{i-1}, \beta^i, \beta^{i-1}, \delta^i)\end{aligned} \quad (5)$$

と置き換えられることを利用してサンプリングを行う. ここで, 式 (5) の確率の表式では, 付録 A.1 節で定義される周辺確率分布及び条件付き確率分布の定義を用いている. また, $\boldsymbol{\delta} = (\delta^1, \delta^2, \cdots, \delta^n), \boldsymbol{\beta} = (\beta^1, \beta^2, \cdots, \beta^n)$ とし, 表式を簡単にするため $\beta^0 = \alpha_3^0 = 0$ とした.

以下, まず 3.1 節で格子基底 S_2 の性質及びその性質を利用するための変数変換について説明する. 次に 3.2 節で, 3.1 節の格子の性質を用いて, 式 (2) の一部を分解する方法について示す. その後, 3.3 節において, 付録 A.3 で説明する格子の並進対称性を用いて, 更に, 式 (2) を分解する方法を示す. 最後に, 3.4 節において, 式 (5) の分解を利用したサンプリングアルゴリズムを提案する.

3.1 格子の性質:基底ベクトルの等長性

ここでは, MP12[5] で用いられる格子基底 S_2 の性質について説明を行う. 格子基底 S_2 は, 隣り合う基底ベクトルのノルムが等しいという性質を有する. ノルムが等しい基

Vol.2019-DPS-178 No.25
Vol.2019-CSEC-84 No.25
2019/3/5

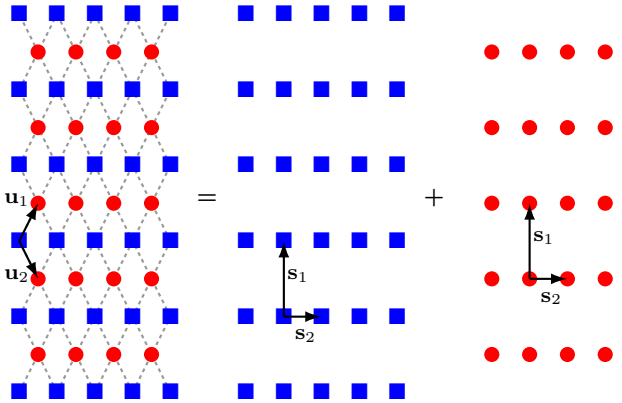

図 1　格子の分解の模式図

底によって張られる格子は, 図 1 に示すように, 直交する 2 つの格子に分解することが可能である.

例えば, 式 (3) の格子基底を

$$S_2 = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{3n}) \tag{6}$$

と書いたときの隣合う 2 つの基底ベクトル $\mathbf{v}_1, \mathbf{v}_2$ を考える. ここでは簡単のため, $\mathbf{v}_1, \mathbf{v}_2$ の最初の 3 成分を

$$\mathbf{u}_1 = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \mathbf{u}_2 = \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix}, \tag{7}$$

とおく. このベクトル $\mathbf{u}_1, \mathbf{u}_2$ により張られる格子

$$\mathcal{L}(\mathbf{u}_1, \mathbf{u_2}) = \mathcal{L}\begin{pmatrix} 2 & 0 \\ -1 & 2 \\ 0 & -1 \end{pmatrix} \tag{8}$$

は, 図 1 に示すように, 直交基底により張られる格子

$$\mathcal{L}(\mathbf{s}_1, \mathbf{s_2}) = \mathcal{L}\begin{pmatrix} 2 & 2 \\ 1 & -3 \\ -1 & 1 \end{pmatrix} \tag{9}$$

と, 式 (9) を平行移動させた

$$\mathcal{L}(\mathbf{s}_1, \mathbf{s_2}) + \mathbf{u}_1 = \mathcal{L}\begin{pmatrix} 2 & 2 \\ 1 & -3 \\ -1 & 1 \end{pmatrix} + \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} \tag{10}$$

に分離することが可能である.

以下, 式 (9) 及び式 (10) の基底ベクトル

$$\mathbf{s}_1 = \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}, \mathbf{s}_2 = \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix}, \tag{11}$$

及び, これらに対して直交する基底

$$\mathbf{s}_3 = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} \tag{12}$$

を用いて, 式 (3) に現れる格子点 $S_2\mathbf{x}$ を表現することを考えていく.

格子点 $S_2\mathbf{x}$ を直交基底で表すことができれば, 付録 A.2 で示すように, 多次元の離散ガウス分布を 1 次元離散ガウス分布の積で記述することが可能であるため, 既存のサンプリング方法 [16], [17] を適用することが出来ると考えられる.

$3n$ 次元上の格子点 $S_2\mathbf{x}$ を表現するために, 以下のように記号を導入する.

$$\begin{aligned}
\mathbf{s}_1^i &= 2\mathbf{e}_{3i-2} + \mathbf{e}_{3i-1} - \mathbf{e}_{3i} = (\underbrace{0, \cdots, 0}_{3i-3\text{ 個}}, \mathbf{s}_1^T, 0, \cdots, 0)^T \\
\mathbf{s}_2^i &= 2\mathbf{e}_{3i-2} - 3\mathbf{e}_{3i-1} + \mathbf{e}_{3i} = (\underbrace{0, \cdots, 0}_{3i-3\text{ 個}}, \mathbf{s}_2^T, 0, \cdots, 0)^T \\
\mathbf{s}_3^i &= \mathbf{e}_{3i-2} + 2\mathbf{e}_{3i-1} + 4\mathbf{e}_{3i} = (\underbrace{0, \cdots, 0}_{3i-3\text{ 個}}, \mathbf{s}_3^T, 0, \cdots, 0)^T
\end{aligned}$$

ここで, $\mathbf{e}_i$ は, 第 i 成分が 1 である単位ベクトルであり, また, 上付きの添字 T は転置を表す. この $\{\mathbf{s}_i^j\}$ を用いて, $3n$ 次元の格子点 $S_2\mathbf{x}$ は, 次のように表すことができる.

$$\begin{aligned}
S_2\mathbf{x} &= \sum_{i=1}^{n} x_i \mathbf{v}_i \\
&= \sum_{i=1}^{n} \left(\alpha_1^i + \frac{\delta^i}{2} - \frac{1}{3}x_{3i} - \frac{1}{3}x_{3i-3} \right) \mathbf{s}_1^i \\
&+ \sum_{i=1}^{n} \left(\alpha_2^i + \frac{\delta^i}{2} + \frac{1}{7}x_{3i} - \frac{1}{7}x_{3i-3} \right) \mathbf{s}_2^i \\
&+ \sum_{i=1}^{n} \left(\frac{8}{21}x_{3i} - \frac{1}{21}x_{3i-3} \right) \mathbf{s}_3^i
\end{aligned} \tag{13}$$

となる. ここで,

$$\begin{aligned}
x_{3i-2} &= \alpha_1^i + \alpha_2^i + \delta^i \\
x_{3i-1} &= \alpha_1^i - \alpha_2^i \\
&\text{where } \alpha_1^i, \alpha_2^i \in \mathbb{Z}, \delta^i \in \{0, 1\}
\end{aligned} \tag{14}$$

であり, また, 表記の簡単のため $\alpha_{3i-2}^0 = \alpha_{3i-1}^0 = 0$ とした. この表式から, 任意の格子点を直交する基底を用いて表現できていることがわかる.

以下, 3.2 節では, 格子の直交性を用いて, 式 (2) の同時確率分布 $\Pr(\mathbf{x})$ の分解を行っていく.

3.2　格子の直交性を用いた同時確率分布の分解

ここでは, 3.1 節において導入した直交基底を用いて, 式 (2) の同時確率分布 $\Pr(\mathbf{x})$ を, 条件付き確率分布 (1 次元離散ガウス分布) の積として表現できることを示す. 同時確率分布 $\Pr(\mathbf{x})$ の確率変数 $\mathbf{x}$ は, 変数変換に伴い, $\boldsymbol{\alpha}_1 = (\alpha_1^1, \alpha_1^2, \cdots, \alpha_1^n)$, $\boldsymbol{\alpha}_2 = (\alpha_2^1, \alpha_2^2, \cdots \alpha_2^n)$, $\mathbf{x}_3 = (x_3, x_6, \cdots x_{3n})$, $\boldsymbol{\delta} = (\delta^1, \delta^2, \cdots, \delta^n)$ の関数と見な

すことができる. ここで, 同時確率分布を $\Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \mathbf{x}_3, \boldsymbol{\delta})$ と書いた場合,

$$\Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \mathbf{x}_3, \boldsymbol{\delta}) = \Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 | \mathbf{x}_3, \boldsymbol{\delta}) \cdot \Pr(\mathbf{x}_3, \boldsymbol{\delta}) \quad (15)$$

が成立する. ここで, $\Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 | \mathbf{x}_3, \boldsymbol{\delta})$ は, 条件付き確率を表し, ベクトル $\mathbf{s}_1^i$, $\mathbf{s}_2^i$, $\mathbf{s}_3^i$ の直交性から,

$$\begin{aligned}\Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 | \mathbf{x}_3, \boldsymbol{\delta}) = & \prod_{i=1}^{n} \Pr(\alpha_1^i | x_{3i}, x_{3i-3}, \delta^i) \\ & \times \Pr(\alpha_2^i | x_{3i}, x_{3i-3}, \delta^i) \end{aligned} \quad (16)$$

が成立する. ここで, 表式を簡単にするため $x_0 = 0$ を導入した. 式 (16) について, 簡単のため, $n = 2$ の場合について付録 A.2 に記述するが, 一般的の n に対する導出も容易である. なお, 式 (16) に現れる条件付き確率は, 1 次元離散ガウス分布

$$\begin{aligned}\mathcal{D}^1_{\sigma,c}(x) = \frac{\exp\left(-\frac{1}{\sigma^2}(x-c)^2\right)}{\sum_{x \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}(x-c)^2\right)}, \\ \sigma, c \in \mathbb{R}, \quad x \in \mathbb{Z}\end{aligned} \quad (17)$$

を用いて,

$$\begin{aligned}\Pr(\alpha_1^i | x_{3i}, x_{3i-3}, \delta^i) &= D^1_{\frac{\sigma}{\|\mathbf{s}_1\|}, \frac{x_3^i}{3} + \frac{x_3^{i-1}}{3} - \frac{\delta^i}{2} + C_1^i}(\alpha_1^i) \\ \Pr(\alpha_2^i | x_{3i}, x_{3i-3}, \delta^i) &= D^1_{\frac{\sigma}{\|\mathbf{s}_1\|}, -\frac{x_3^i}{7} + \frac{x_3^{i-1}}{7} - \frac{\delta^i}{2} + C_2^i}(\alpha_2^i)\end{aligned} \quad (18)$$

と具体的に 書き下すことが出来る. ここで, 式 (18) の C_1^i 及び C_2^i は, 式 (2) の分布の中心 $\mathbf{c} = (c_1, c_2, \cdots, c_{3n})$ を用いて

$$\begin{aligned}C_1^i &= \frac{2c_{3i-2} + c_{3i-1} + c_{3i}}{6} \\ C_2^i &= \frac{2c_{3i-2} - 3c_{3i-1} + c_{3i}}{14}\end{aligned} \quad (19)$$

と定義した.

以上より, 同時確率分布は

$$\begin{aligned}\Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \mathbf{x}_3, \boldsymbol{\delta}) = & \Pr(\mathbf{x}_3, \boldsymbol{\delta}) \prod_{i=1}^{n} \Pr(\alpha_1^i | x_{3i}, x_{3i-3}, \delta^i) \\ & \times \Pr(\alpha_2^i | x_{3i}, x_{3i-3}, \delta^i) \end{aligned} \quad (20)$$

となり, 一部を条件付き確率 (1 次元離散ガウス分布) の積の形に分解できることを示した. 以下, 式 (20) の 1 次元離散ガウス分布以外の部分 ($\Pr(\mathbf{x}_3, \boldsymbol{\delta})$) について更に分解を行うことを考えていく.

3.3 格子の並進対称性を用いた同時確率分布の分解

ここでは式 (20) の周辺確率分布 $\Pr(\mathbf{x}_3, \boldsymbol{\delta})$ について, 付録 A.3 に示した格子の並進対称性を用いて, 分解を行った結果を示す.

付録 A.3 の並進対称性を利用するため, $\mathbf{x}_3 = (x_3, x_6, \cdots, x_{3n})$ に関して, 以下の変数変換を行う.

$$\begin{aligned}x_{3i} &= 21 \cdot 8^{n-i} \alpha_3^i + \beta^i \\ \alpha_3^i &\in \mathbb{Z}, \quad \beta^i \in \{0, 1, \cdots, 21 \cdot 8^{n-i} - 1\}\end{aligned} \quad (21)$$

この時, 周辺確率分布 $\Pr(\mathbf{x}_3, \boldsymbol{\delta})$ は, $\boldsymbol{\alpha}_3 = (\alpha_3^1, \alpha_3^2, \cdots, \alpha_3^n)$ 及び $\boldsymbol{\beta} = (\beta^1, \beta^2, \cdots, \beta^n)$ の関数と見なすことが出来る. そこで, 周辺確率分布 $\Pr(\mathbf{x}_3, \boldsymbol{\delta})$ を $\Pr(\boldsymbol{\alpha}_3, \boldsymbol{\beta}, \boldsymbol{\delta})$ と書くと, 条件付き確率の定義から

$$\Pr(\boldsymbol{\alpha}_3, \boldsymbol{\beta}, \boldsymbol{\delta}) = \Pr(\boldsymbol{\beta}, \boldsymbol{\delta}) \Pr(\boldsymbol{\alpha}_3 \mid \boldsymbol{\beta}, \boldsymbol{\delta}) \quad (22)$$

が成立する.

式 (22) の右辺の $\Pr(\boldsymbol{\beta}, \boldsymbol{\delta})$ は, 付録 A.3 の並進対称性を考慮して, 以下のように式変形をすることが出来る (ここでは, 表記の簡単のため, 正規化をしていない相対確率を示す).

$$\begin{aligned}&\Pr(\boldsymbol{\beta}, \boldsymbol{\delta}) \\ &\propto \prod_{i=1}^{n} \mathcal{S}\left(\frac{\sigma}{\|\mathbf{s}_1\|}, -\frac{\delta^i}{2} + \frac{\beta^i}{3} + \frac{\beta^i}{3} + C_1^i\right) \\ &\times \mathcal{S}\left(\frac{\sigma}{\|\mathbf{s}_2\|}, -\frac{\delta^i}{2} - \frac{\beta^i}{7} + \frac{\beta^i}{7} + C_2^i\right) \\ &\times \mathcal{S}\left(\frac{\sigma}{8^{n-i+1}\|\mathbf{s}_3^i\|}, \frac{-1}{8^{n-i+1}}\left(\frac{8}{21}\beta^i - \frac{1}{21}\beta^{i-1} - C_3^i\right)\right)\end{aligned} \quad (23)$$

ここで, C_1^i 及び C_2^i は式 (19) であり, C_3^i は

$$C_3^i = \frac{c_{3i-2} + c_{3i-1} + 4c_{3i}}{21} \quad (24)$$

とした. また、$\mathcal{S}(\sigma, c)$ は、

$$\mathcal{S}(\sigma, c) = \sum_{x \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}(x-c)^2\right) \quad (25)$$

である。式 (25) の和は, 楕円シータ関数

$$\theta_3(u, q) = 1 + 2\sum_{i=1}^{\infty} q^{i^2} \cos(2iu) \quad (26)$$

を用いて,

$$\mathcal{S}(\sigma, c) = \sqrt{\pi\sigma^2}\theta_3\left(-c\pi, \exp(-\pi^2\sigma^2)\right) \quad (27)$$

と表すことが出来, 比較的容易に計算出来ることが知られている.

式 (22) の右辺の $\Pr(\boldsymbol{\alpha}_3 \mid \boldsymbol{\beta}, \boldsymbol{\delta})$ に対しては, 条件付き確率の定義に従い,

$$\Pr(\boldsymbol{\alpha}_3 \mid \boldsymbol{\beta}, \boldsymbol{\delta}) = \prod_{i=1}^{n} \Pr\left(\alpha_3^i, \mid \boldsymbol{\beta}, \boldsymbol{\delta}, \alpha_3^1, \alpha_3^2 \cdots, \alpha_3^{i-1}\right) \quad (28)$$

が成立する. ここで, 式 (28) の右辺は基底の直交性及び格子の並進対称性を考慮すると, 以下のように 1 次元離散ガ

ウス分布で表すことが出来る.

$$\begin{aligned}&\Pr\left(\alpha_3^i, \mid \boldsymbol{\beta}, \boldsymbol{\delta}, \alpha_3^1, \alpha_3^2 \cdots, \alpha_3^{i-1}\right)\\&= \mathcal{D}^1_{\frac{\sigma}{8^{n-i+1}\|\mathbf{s}_3\|}, \alpha_3^{i-1} - \frac{1}{21}\cdot\left(\beta^i - \frac{\beta^{i-1}}{8}\right)}\left(\alpha_3^i\right)\\&= \Pr\left(\alpha_3^i, \mid \beta^i, \beta^{i-1}, \alpha_3^{i-1}\right)\end{aligned} \tag{29}$$

以上をまとめると, $3n$ 次元離散ガウス分布 $\Pr(\mathbf{x})$ は, 式 (5) の積の形に分解することが出来る. 以下, 3.4 節では, この分解を利用したサンプリングアルゴリズムについて述べる.

3.4 サンプリングアルゴリズム

前節までで, MP12[5] で用いられている $3n$ 次元離散ガウス分布が

$$\begin{aligned}\Pr(\mathbf{x}) = \Pr(\boldsymbol{\beta}, \boldsymbol{\delta}) &\prod_{i=1}^{n} \Pr(\alpha_3^i \mid \alpha_3^{i-1}, \beta^i, \beta^{i-1})\\&\times \Pr(\alpha_1^i \mid \alpha_3^i, \alpha_3^{i-1}, \beta^i, \beta^{i-1}, \delta^i)\\&\times \Pr(\alpha_2^i \mid \alpha_3^i, \alpha_3^{i-1}, \beta^i, \beta^{i-1}, \delta^i)\end{aligned} \tag{30}$$

の積の形に分解出来ることを確認した. ここで, $\Pr(\boldsymbol{\beta}, \boldsymbol{\delta})$ は楕円シータ関数の積で表されており, 比較的容易に評価することが可能である. また, その他の条件付き確率は全て 1 次元の離散ガウス分布である. この分解を利用して, MP12[5] で用いられている $3n$ 次元離散ガウス分布のサンプリング手法を以下に示す.

Step 1: $\Pr(\boldsymbol{\beta}, \boldsymbol{\delta})$ を全ての $\boldsymbol{\beta}, \boldsymbol{\delta}$ に対し, 結果を保存しておく.

Step 2: 計算した $\Pr(\boldsymbol{\beta}, \boldsymbol{\delta})$ に従って,$\boldsymbol{\beta}, \boldsymbol{\delta}$ をサンプリングする.

Step 3: $\Pr(\alpha_3^i \mid \alpha_3^{i-1}, \beta^i, \beta^{i-1})$ に従って, α_3^i を $i = 1$ から順に n までサンプリングする.

Step 4: $\Pr(\alpha_1^i \mid \alpha_3^i, \alpha_3^{i-1}, \beta^i, \beta^{i-1}, \delta^i)$ 及び $\Pr(\alpha_2^i \mid \alpha_3^i, \alpha_3^{i-1}, \beta^i, \beta^{i-1}, \delta^i)$ に従って, 全ての $i = 1, \cdots, n$ に対して α_1^i 及び α_2^i をサンプリングする.

Step 5: 式 (4) を使って, $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_2, \boldsymbol{\beta}, \boldsymbol{\delta}$ を $\mathbf{x}$ に変換する.

ここで, 確率変数 $\mathbf{x}$ を繰り返しサンプリングする場合には, Step 1 は 1 度だけ計算すればよく, Step 2 から Step 5 のみを繰り返す. また, Step 4 は全ての i に関して, 並列でサンプリングすることが可能である.

4. まとめと今後の展望

本稿では, 格子暗号の重要な要素技術の一つである Preimage Sampleable Function で重要となる離散ガウス分布のサンプリングアルゴリズムの提案を行った. 提案したアルゴリズムは, 格子基底の等長性を利用した直交化及び格子の並進対称性を利用することで, $3n$ 次元離散ガウス分布を, 楕円シータ関数と 1 次元離散ガウス分布の積の形にかけるという事実に基づき, 構成されている.

今後, 提案したアルゴリズムの計算時間やメモリ使用量等を既存の研究と比較することで, 本アルゴリズムが優位性を持つパラメータ領域等について確認を行う必要がある. また, 本稿では, 格子基底について $3n$ 次元, 格子基底 S_p について $p = 2$ のみを考えたが, これらについて一般化することも重要であると考えられる.

謝辞 本研究の一部は, 文部科学省 光・量子飛躍フラッグシッププログラムの支援により行われた.

参考文献

[1] Shor, P. W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM review*, Vol. 41, No. 2, pp. 303–332 (1999).
[2] : NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.
[3] 伊藤忠彦: 量子コンピュータが公開鍵基盤に与える影響と対策」, 2018 年暗号と情報セキュリティシンポジウム予稿集, 電子情報通信学会 (2018).
[4] 清藤武暢: 量子コンピュータが金融サービスのセキュリティに与える影響とその対策, 日銀レビュー, 日本銀行 (2018).
[5] Micciancio, D. and Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller, *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 700–718 (2012).
[6] Regev, O.: The learning with errors problem, *Invited survey in CCC*, Vol. 7 (2010).
[7] Lindner, R. and Peikert, C.: Better key sizes (and attacks) for LWE-based encryption, Cryptographers' Track at the RSA Conference, Springer, pp. 319–339 (2011).
[8] Agrawal, S., Boneh, D. and Boyen, X.: Efficient lattice (H) IBE in the standard model, *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 553–572 (2010).
[9] Boyen, X.: Attribute-based functional encryption on lattices, *Theory of Cryptography*, Springer, pp. 122–142 (2013).
[10] Gentry, C. and Boneh, D.: *A fully homomorphic encryption scheme*, Vol. 20, No. 09, Stanford University Stanford (2009).
[11] Gentry, C., Peikert, C. and Vaikuntanathan, V.: Trapdoors for Hard Lattices and New Cryptographic Constructions, *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, New York, NY, USA, ACM, pp. 197–206 (online), DOI: 10.1145/1374376.1374407 (2008).
[12] Wang, Z., Ling, C. and Hanrot, G.: Markov chain Monte Carlo algorithms for lattice Gaussian sampling, *Information Theory (ISIT), 2014 IEEE International Symposium on*, IEEE, pp. 1489–1493 (2014).
[13] Wang, Z. and Ling, C.: Lattice Gaussian Sampling by Markov Chain Monte Carlo: Convergence Rate and Decoding Complexity, *CoRR*, Vol. abs/1704.02673 (online), available from ⟨http://arxiv.org/abs/1704.02673⟩ (2017).
[14] Boyen, X. and Li, Q.: Towards tightly secure lattice

short signature and id-based encryption, *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 404–434 (2016).
[15] Genise, N. and Micciancio, D.: Faster gaussian sampling for trapdoor lattices with arbitrary modulus, *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 174–203 (2018).
[16] Micciancio, D. and Walter, M.: Gaussian Sampling over the Integers: Efficient, Generic, Constant-Time, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, pp. 455–485 (online), DOI: 10.1007/978-3-319-63715-0_16 (2017).
[17] Dwarakanath, N. C. and Galbraith, S. D.: Sampling from discrete Gaussians for lattice-based cryptography on a constrained device, *Appl. Algebra Eng. Commun. Comput.*, Vol. 25, No. 3, pp. 159–180 (online), DOI: 10.1007/s00200-014-0218-3 (2014).

付　　録

A.1 周辺確率分布と条件付き確率分布

本節では, 本文中で用いられる周辺確率分布及び条件付き確率分布の定義を示す.

確率変数 $X_1, X_2, \cdots, X_n$ に対して, ある値 $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ が観測される同時確率分布が

$$\Pr(\mathbf{x}) = \Pr(x_1, x_2, \cdots, x_n) \tag{A.1}$$

と与えられているとする. この時, $x_1, x_2, \cdots, x_m, (m < n)$ が観測される周辺確率分布を,

$$\Pr(x_1, x_2, \cdots, x_m) = \sum_{x_{m+1}, x_{m+2} \cdots, x_n} \Pr(x_1, x_2, \cdots, x_n) \tag{A.2}$$

と定義する. ここで, $\sum_{x_{m+1}, x_{m+2} \cdots, x_n}$ は, 同時確率分布 $\Pr(x_1, x_2, \cdots, x_n)$ の定義域全体に関して和をとることとする.

また, $x_{m+1}, x_{m+2}, \cdots x_n$ が与えられた条件の下で, $x_1, x_2, \cdots, x_m$ を得る条件付き確率 $\Pr(x_1, x_2, \cdots, x_m \mid x_{m+1}, x_{m+2}, \cdots x_n)$ を

$$\begin{aligned}
&\Pr(x_1, x_2, \cdots, x_m \mid x_{m+1}, x_{m+2}, \cdots, x_n) \\
&= \frac{\Pr(x_1, x_2, \cdots, x_n)}{\Pr(x_{m+1}, x_{m+2}, \cdots, x_n)} \\
&= \frac{\Pr(x_1, x_2, \cdots, x_n)}{\sum_{x_1, x_2 \cdots, x_m} \Pr(x_1, x_2, \cdots, x_m, \cdots, x_n)}
\end{aligned} \tag{A.3}$$

と定義する.

以上と同様にして, $l < m < n$ を満たす整数 l, m に対して, 条件付き周辺確率分布 $\Pr(x_1, x_2, \cdots, x_l \mid x_{l+1}, x_{l+2}, \cdots x_m)$ は,

$$\begin{aligned}
&\Pr(x_1, x_2, \cdots, x_l \mid x_{l+1}, x_{l+2}, \cdots, x_m) \\
&= \frac{\Pr(x_1, x_2, \cdots, x_m)}{\Pr(x_{l+1}, x_{l+2}, \cdots, x_m)} \\
&= \frac{\sum_{x_{m+1}, x_{m+2} \cdots, x_n} \Pr(x_1, \cdots, x_m, \cdots, x_n)}{\sum_{x_1, \cdots, x_l, x_{m+1}, x_{m+2}, \cdots, x_n} \Pr(x_1, \cdots, x_l, \cdots, x_m, \cdots, x_n)}
\end{aligned} \tag{A.4}$$

と定義される.

3 節では, 以上の定義を用いて, 同時確率分布 (2) から定義される周辺確率分布や条件付き確率分布を用いて, 記述を行っている.

A.2 基底の直交性と確率の分離

本節では, 基底が直交する場合に, 離散ガウス分布が基底毎に独立した 1 次元ガウス分布に分解可能であることを述べる. 3.2 節では, 本節の結果を用いて式変形を行っている.

まず, 簡単のため, 以下の 2 次元の同時確率分布を考える.

$$\begin{aligned}
&\Pr(x_1, x_2, c_1, c_2) \\
&= \frac{\exp\left(-\frac{1}{\sigma^2}\|x_1\mathbf{s}_1 + x_2\mathbf{s}_2 - c_1\mathbf{s}_1 - c_2\mathbf{s}_2\|^2\right)}{\sum_{x_1, x_2, c_1, c_2 \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}\|x_1\mathbf{s}_1 + x_2\mathbf{s}_2 - c_1\mathbf{s}_1 - c_2\mathbf{s}_2\|^2\right)}
\end{aligned} \tag{A.5}$$

ここで, $\mathbf{s}_1, \mathbf{s}_2$ は直交する基底ベクトルであり, σ は分布の標準偏差, c_1, $c_2 \in \mathbb{Z}$ は分布の中心とする. この時, c_1, c_2 が与えられた下での条件付き確率

$$\begin{aligned}
&\Pr(x_1, x_2 \mid c_1, c_2) \\
&= \frac{\exp\left(-\frac{1}{\sigma^2}\|x_1\mathbf{s}_1 + x_2\mathbf{s}_2 - c_1\mathbf{s}_1 - c_2\mathbf{s}_2\|^2\right)}{\sum_{x_1, x_2 \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}\|x_1\mathbf{s}_1 + x_2\mathbf{s}_2 - c_1\mathbf{s}_1 - c_2\mathbf{s}_2\|^2\right)}
\end{aligned} \tag{A.6}$$

は, 基底ベクトル $\mathbf{s}_1$ と $\mathbf{s}_2$ の直交性により, 1 次元離散ガウス分布の積に分解することが出来る:

$$\begin{aligned}
&\Pr(x_1, x_2 \mid c_1, c_2) \\
&= \frac{\exp\left(-\frac{1}{\sigma^2}\|x_1\mathbf{s}_1 - c_1\mathbf{s}_1\|^2\right)}{\sum_{x_1 \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}\|x_1\mathbf{s}_1 - c_1\mathbf{s}_1\|^2\right)} \\
&\times \frac{\exp\left(-\frac{1}{\sigma^2}\|x_2\mathbf{s}_2 - c_2\mathbf{s}_2\|^2\right)}{\sum_{x_2 \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}\|x_2\mathbf{s}_2 - c_2\mathbf{s}_2\|^2\right)} \\
&= D^1_{\frac{\sigma}{\|\mathbf{s}_1\|}, c_1}(x_1) \cdot D^1_{\frac{\sigma}{\|\mathbf{s}_2\|}, c_2}(x_2)
\end{aligned} \tag{A.7}$$

ここで, 1 次元離散ガウス分布を

$$\begin{aligned}
\mathcal{D}^1_{\sigma,c}(x) &= \frac{\exp\left(-\frac{1}{\sigma^2}(x-c)^2\right)}{\sum_{x \in \mathbb{Z}} \exp\left(-\frac{1}{\sigma^2}(x-c)^2\right)}, \\
\sigma, c &\in \mathbb{R}, \quad x \in \mathbb{Z}
\end{aligned} \tag{A.8}$$

と表した.(A.5) の同時確率分布から求められる条件付き周

辺確率分布が

$$\begin{aligned}\Pr(x_i \mid c_i) &= \frac{\exp\left(-\frac{1}{\sigma^2}\|x_i\mathbf{s}_i - c_i\mathbf{s}_i\|^2\right)}{\sum_{x_i\in\mathbb{Z}}\exp\left(-\frac{1}{\sigma^2}\|x_i\mathbf{s}_1 - c_i\mathbf{s}_i\|^2\right)} \\ &= D^i{}_{\frac{\sigma}{\|\mathbf{s}_i\|},c_i}(x_i)\end{aligned} \tag{A.9}$$

と与えられることを考慮すると, 式 (A.6) の条件付き確率は

$$\Pr(x_1, x_2 \mid c_1, c_2) = \Pr(x_1 \mid c_1)\Pr(x_2 \mid c_2) \tag{A.10}$$

と表すことが出来る.

同様にして, 同時確率分布が直交した基底ベクトルを持つ n 次元離散ガウス分布

$$\begin{aligned}&\Pr(x_1, x_2, \cdots, x_n, c_1, c_2, \cdots, c_n) \\ =&\frac{\exp\left(-\frac{1}{\sigma^2}\left\|\sum_{i=1}^n x_i\mathbf{s}_i - c_i\mathbf{s}_i\right\|^2\right)}{\sum_{x_1,\cdots,x_n,c_1,\cdots,c_n\in\mathbb{Z}}\exp\left(-\frac{1}{\sigma^2}\left\|\sum_{i=1}^n x_i\mathbf{s}_i - c_i\mathbf{s}_i\right\|^2\right)}\end{aligned} \tag{A.11}$$

で表される時, n 個の 1 次元離散ガウス分布の積に分解することが可能である.

$$\Pr(x_1, x_2, \cdots, x_n \mid c_1, c_2, \cdots, c_n) = \prod_{i=1}^n \Pr(x_i \mid c_i) \tag{A.12}$$

3.2 節では, 式 (A.12) の分解を用いることにより, 条件付き確率の各直交基底毎の 1 次元離散ガウス分布への分解

$$\begin{aligned}&\Pr(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \mid \mathbf{x}_3, \boldsymbol{\delta}) \\ &= \prod_{i=1}^n \Pr(\alpha_1^i \mid x_{3i}, x_{3i-3}, \delta^i)\Pr(\alpha_2^i \mid x_{3i}, x_{3i-3}, \delta^i)\end{aligned} \tag{A.13}$$

を行っている.

A.3 1 次元離散ガウス分布の和の離散並進対称性

本節では, 3.3 節で用いた 1 次元離散ガウス分布の和の離散並進対称性について述べる.

1 次元離散ガウス分布

$$\begin{aligned}\mathcal{D}^1_{\sigma,c}(x) &= \frac{\exp\left(-\frac{1}{\sigma^2}(x-c)^2\right)}{\sum_{x\in\mathbb{Z}}\exp\left(-\frac{1}{\sigma^2}(x-c)^2\right)}, \\ &\sigma, c \in \mathbb{R}, \quad x \in \mathbb{Z}\end{aligned} \tag{A.14}$$

の確率変数 x を整数全体 $\mathbb{Z}$ について和を取った量

$$\mathcal{S}(\sigma, c) = \sum_{x\in\mathbf{Z}} \mathcal{D}^1_{\sigma,c}(x) \tag{A.15}$$

は以下の離散並進対称性を有する.

$$\mathcal{S}(\sigma, c+k) = \mathcal{S}(\sigma, c), \quad k \in \mathcal{Z} \tag{A.16}$$

このため, 例えば

$$\begin{aligned}&\sum_{x_1,x_2\in\mathbb{Z}} \mathcal{D}^1_{\sigma_1,c_1}(x_1+x_2)\mathcal{D}^1_{\sigma_2,c_2}(x_2) \\ &= \sum_{x_1,x_2\in\mathbb{Z}} \mathcal{D}^1_{\sigma_1,c_1}(x_1)\mathcal{D}^1_{\sigma_2,c_2}(x_2) \\ &= \sum_{x_1\in\mathbb{Z}} \mathcal{D}^1_{\sigma_1,c_1}(x_1) \sum_{x_2\in\mathbb{Z}} \mathcal{D}^1_{\sigma_2,c_2}(x_2) \\ &= 1\end{aligned} \tag{A.17}$$

のような演算が可能となる.3.3 節では, (A.16) 及び (A.17) の離散並進対称性を用いて, 確率の分解を行っている.