格子暗号

廣政 良（三菱電機）

耐量子計算機暗号と量子情報の数理（’22/08/01-04）

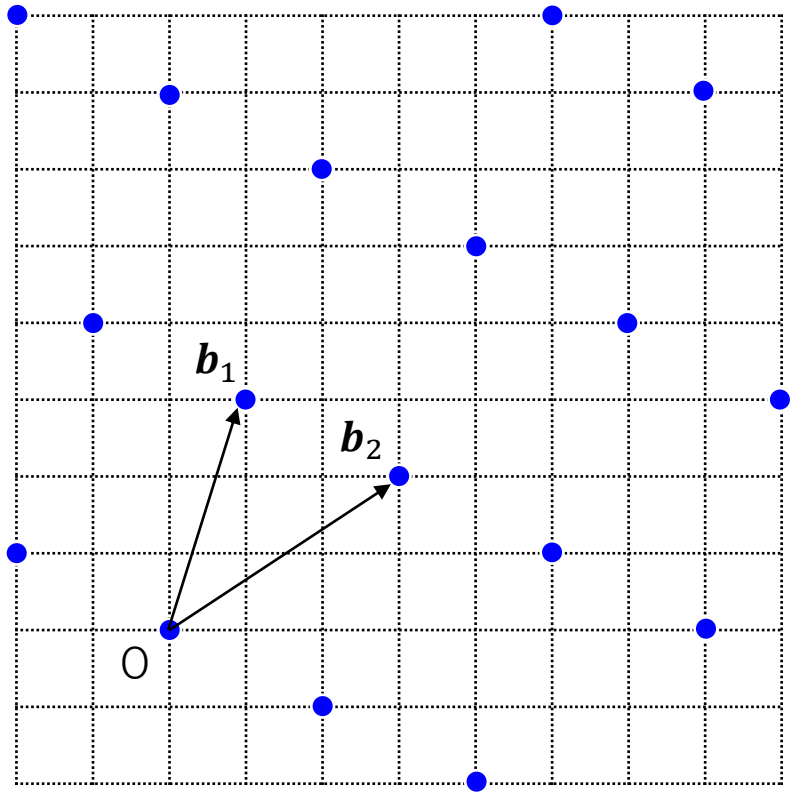
話すこと

- 格子，格子暗号，公開鍵暗号
- 格子ベース公開鍵暗号（LWE，Regev暗号）
- 完全準同型暗号（Gentry-Sahai-Waters完全準同型暗号）
- 量子性検証プロトコル（Noisy Trapdoor Claw-free関数）

格子

- 線型独立なベクトルの集合（基底）で表されるベクトルの集合
  - 基底：$\boldsymbol{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$
  - 格子：$L(\boldsymbol{B}) = \left\{\sum_{i\in[n]} z_i \cdot \boldsymbol{b}_i : z_i \in \mathbb{Z}\right\}$

- 格子問題（最短ベクトル問題）
  - 任意の基底$\boldsymbol{B}$が与えられたとき，
    格子$L(\boldsymbol{B})$の短い格子ベクトルを
    計算する or 存在を検知する問題
  - 量子コンピュータでも（現状は）解読困難



格子暗号

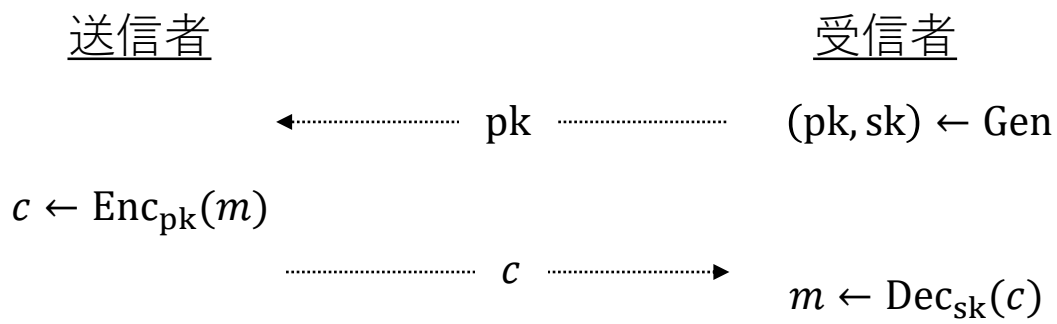
- 格子暗号
  - 格子問題の困難性を安全性の根拠とする暗号方式
  - 実際に方式を構成する際はlearning with errors (LWE) 問題（後述）等を利用

- 様々な格子暗号：
  - 公開鍵暗号
  - ディジタル署名
  - IDベース，属性ベース暗号
  - （量子）完全準同型暗号
  - 量子性検証，量子計算検証プロトコル

公開鍵暗号

- 暗号化するための鍵（公開鍵）と復号するための鍵（秘密鍵）が異なる暗号方式

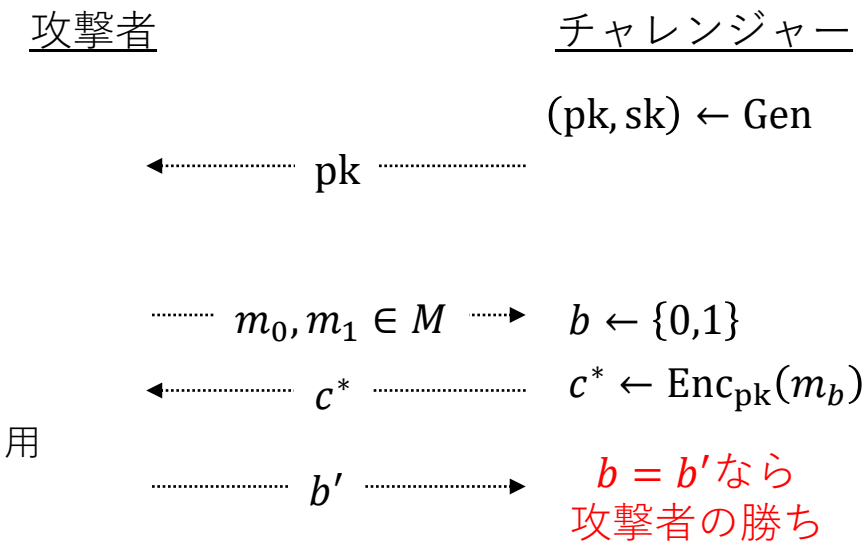
- 公開鍵暗号は三つのアルゴリズムからなる
  - Gen：公開鍵pk，秘密鍵skを生成
  - Enc：pkと平文mを用いて暗号文cを生成
  - Dec：skとcから平文を復号



- 公開鍵暗号の性質（正当性）
  - $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}, c \leftarrow \mathrm{Enc}_{\mathrm{pk}}(m)$に対して，高い確率で$\mathrm{Dec}_{\mathrm{sk}}(c) = m$が成り立つ

公開鍵暗号の安全性

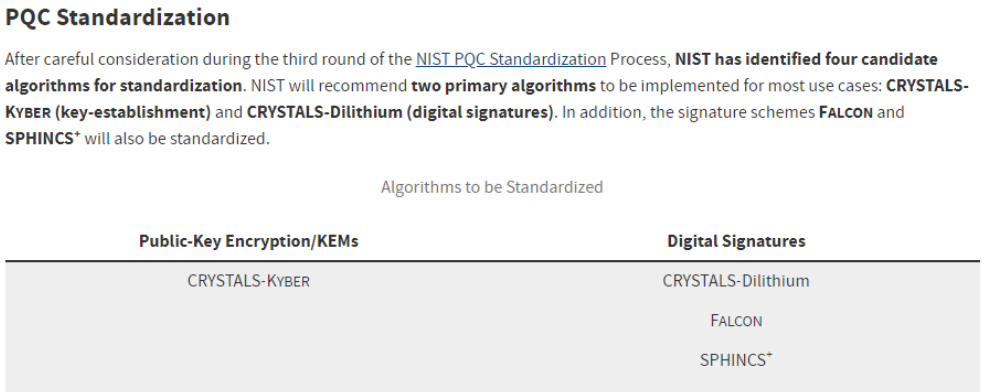
- 暗号方式の安全性
  - 暗号方式を利用するパーティや，安全性における攻撃者は（確率的多項式時間）チューリングマシンでモデル化
  - 安全性は攻撃者とチャレンジャーとの間のあるやり取り（ゲーム、実験）で定義される．
    任意の攻撃者がゲームに勝つ確率が無視できるほど小さければ，その暗号方式は安全
  - 「多項式時間」，「無視できるほど小さい」などは，セキュリティパラメータ（本発表ではλで表す）に対して考える．
    例：「確率が無視できるほど小さい」は，その確率が十分大きなλの任意の多項式の逆数より小さいことを表す（$\mathrm{negl}(\lambda)$と記載）
- 公開鍵暗号の安全性：選択平文攻撃に対する強秘匿性（IND-CPA安全性）
  - 攻撃者が選んだ二つの平文の内，どちらの平文が暗号化されたか推測するゲーム
- （一般的な）安全性証明でやりたいこと
  - ゲームを少しづつ変更していき，最終的に
    攻撃者が安全性を破る確率が小さい（と示せる）ゲームに変換する
  - 変換前後のゲームにおける攻撃者の勝つ確率が大きく変化しないことや，
    変換後ゲームでの攻撃者の勝つ確率が小さいことを示すために計算量的仮定を利用



格子ベース公開鍵暗号：Regev暗号[Reg05]

- 格子問題を安全性の根拠とする公開鍵暗号
  - learning with errors（LWE）問題の解読困難性を安全性の根拠として構成される
  - LWE問題の解読困難性は，格子問題の解読困難性で保証される

- NIST耐量子計算機暗号標準化方式[Nis22]であるCRYSTALS-KYBER方式の（かなり大雑把な意味で）ベースとなる暗号方式



PQC Standardization

After careful consideration during the third round of the NIST PQC Standardization Process, **NIST has identified four candidate algorithms for standardization**. NIST will recommend **two primary algorithms** to be implemented for most use cases: **CRYSTALS-KYBER (key-establishment)** and **CRYSTALS-Dilithium (digital signatures)**. In addition, the signature schemes **FALCON** and **SPHINCS+** will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS+

[Reg05] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In STOC, 2005.
[Nis22] NIST. Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC (nist.gov)

Learning with Errors (LWE) 問題

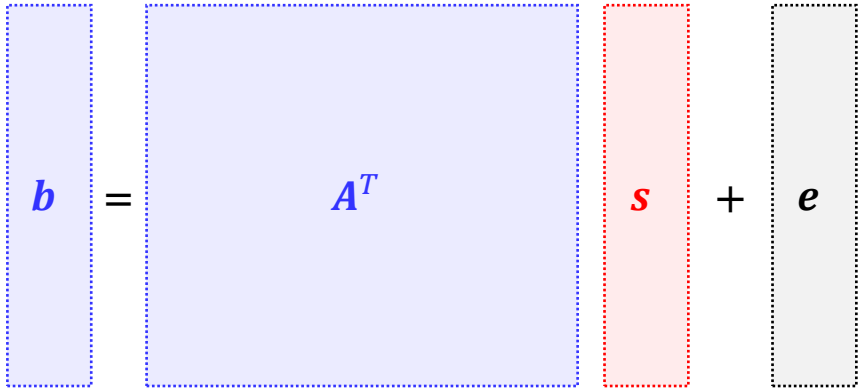
- 二つの行列を識別する問題（D_Bは分散B^2の$\mathbb{Z}$上の離散的な正規分布）
  - $\boldsymbol{B} = \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T \end{bmatrix} \in \mathbb{Z}_q^{(n+1)\times m}$ for $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n, \boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}, \boldsymbol{e} \leftarrow D_B^m$
  - $\boldsymbol{U} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$
- LWE仮定：どのような（確率的多項式時間）アルゴリズムDに対しても，

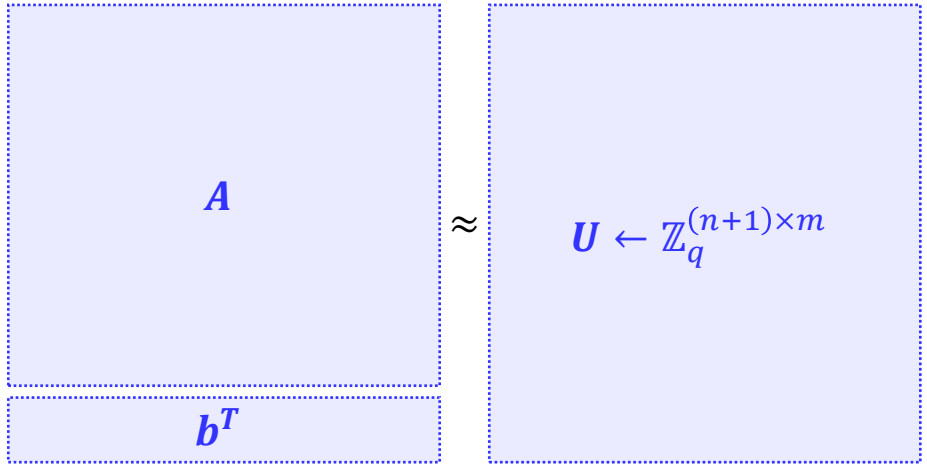
$$\left| \Pr\left[\begin{array}{c} D(\boldsymbol{B}) = 1: \\ \boldsymbol{s} \leftarrow \mathbb{Z}_q^n; \boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}; \\ \boldsymbol{e} \leftarrow D_B^m; \boldsymbol{B} = \begin{pmatrix} \boldsymbol{A} \\ \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T \end{pmatrix} \end{array} \right] - \Pr\left[\begin{array}{c} D(\boldsymbol{U}) = 1: \\ \boldsymbol{U} \leftarrow \mathbb{Z}_q^{(n+1)\times m} \end{array} \right] \right| = \mathrm{negl}(\lambda)$$

- LWE問題の困難性：
  $B \geq 2\sqrt{n}$に対して，格子問題の困難性の下でLWEは困難[Reg05]
- LWE仮定の下でランダム（に見える）行列が作れる

$$\boldsymbol{B} = \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T \end{bmatrix} \approx \boldsymbol{U} \leftarrow \mathbb{Z}_q^{(n+1)\times m},$$

$$(-\boldsymbol{s}^T, 1)\boldsymbol{B} = -\boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T = \boldsymbol{e}^T$$

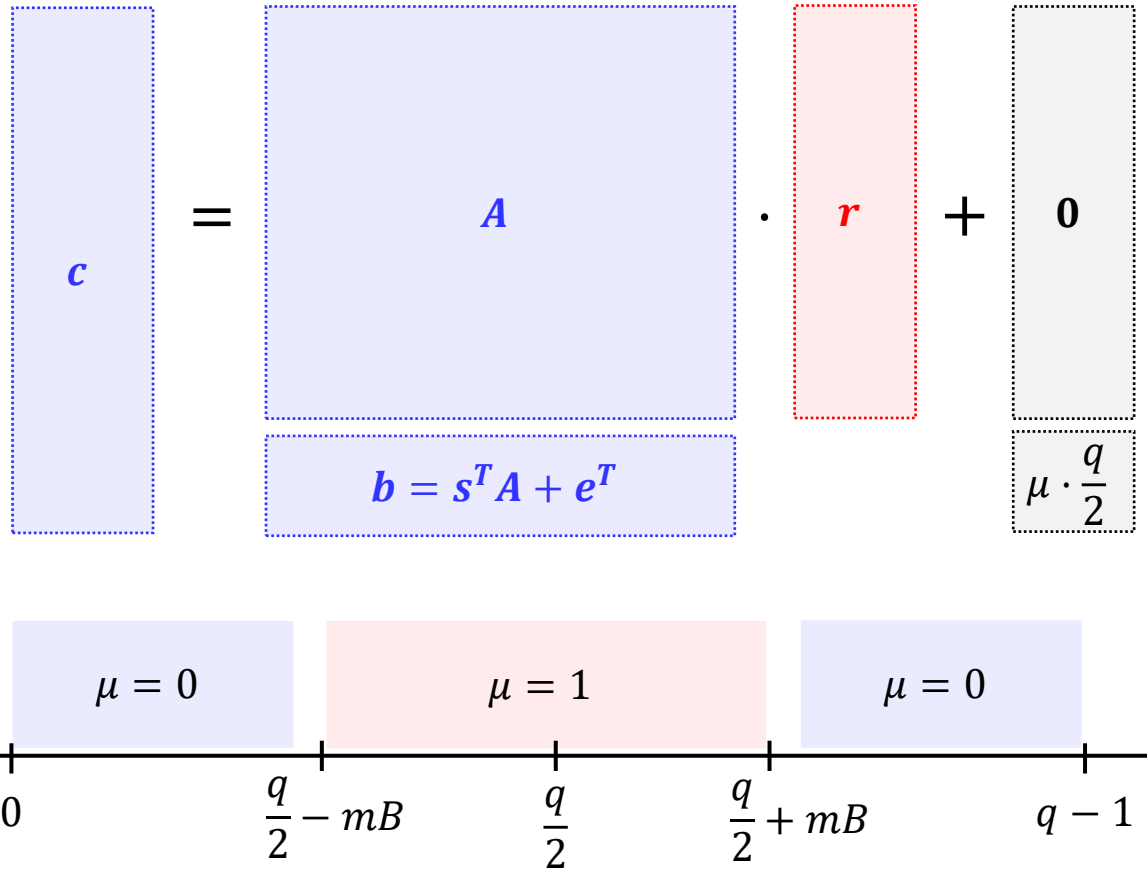




[Reg05] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In STOC, 2005.

Regev暗号：構成

- Gen
  - $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{m\times n}, \boldsymbol{s} \leftarrow \mathbb{Z}_q^n, \boldsymbol{e} \leftarrow D_B^m$
  - $\boldsymbol{B} = \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T \end{bmatrix} \in \mathbb{Z}_q^{(n+1)\times m}$
  - $\mathrm{pk} = \boldsymbol{B}$, $\mathrm{sk} = \boldsymbol{t} = (-\boldsymbol{s}^T, 1) \in \mathbb{Z}^{(n+1)}$
- $\mathrm{Enc}_{\mathrm{pk}}(\mu \in \{0,1\})$
  - $r \leftarrow \{0,1\}^m$
  - $\mathrm{ct} = \boldsymbol{c} = \boldsymbol{B}\boldsymbol{r} + \mu \cdot \begin{bmatrix} \boldsymbol{0} \\ q/2 \end{bmatrix} \in \mathbb{Z}_q^{(n+1)}$
- $\mathrm{Dec}_{\mathrm{sk}}(\mathrm{ct})$
  - Output 1 if $\boldsymbol{t}^T\boldsymbol{c} \approx q/2$, and 0 otherwise.
  - 正当性：$\boldsymbol{t}^T\boldsymbol{c} = \boldsymbol{t}^T\boldsymbol{B}\boldsymbol{r} + \mu \cdot \frac{q}{2} = \boldsymbol{e}^T\boldsymbol{r} + \mu \cdot \frac{q}{2}$ $(|e^T r| < mB < q/4)$



Regev暗号：IND-CPA安全性

Game_0

攻撃者A　　チャレンジャー

$(\boldsymbol{B}, \boldsymbol{t}) \leftarrow \mathrm{Gen}(1^\lambda)$
$b_0 \leftarrow \{0,1\}$
$\boldsymbol{r} \leftarrow \{0,1\}^m$
$\boldsymbol{c}^* = \boldsymbol{B}\boldsymbol{r} + b_0 \cdot \begin{bmatrix} \boldsymbol{0} \\ \frac{q}{2} \end{bmatrix} \in \mathbb{Z}_q^{n+1}$

$(\boldsymbol{B}, \boldsymbol{c}^*)$

b_0'

変換

Game_1

攻撃者A　　チャレンジャー

$\boldsymbol{B} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$
$b_1 \leftarrow \{0,1\}$
$\boldsymbol{r} \leftarrow \{0,1\}^m$
$\boldsymbol{c}^* = \boldsymbol{B}\boldsymbol{r} + b_1 \cdot \begin{bmatrix} \boldsymbol{0} \\ \frac{q}{2} \end{bmatrix} \in \mathbb{Z}_q^{n+1}$

$(\boldsymbol{B}, \boldsymbol{c}^*)$

b_1'

攻撃者Aを用いて，LWE問題の識別者Dを構成

A　　D

LWE or ランダム
$\boldsymbol{B}$

$b \leftarrow \{0,1\}$
$\boldsymbol{r} \leftarrow \{0,1\}^m$
$\boldsymbol{c}^* := \boldsymbol{B}\boldsymbol{r} + b \cdot \begin{bmatrix} \boldsymbol{0} \\ q/2 \end{bmatrix}$

$(\boldsymbol{B}, \boldsymbol{c}^*)$

b'

1 if $b = b'$
0 otherwise

$$
\begin{aligned}
&|\Pr[b_0 = b_0'] - \Pr[b_1 = b_1']| \\
&= \left| \Pr\left[\begin{matrix} D(\boldsymbol{B}) = 1: \\ \boldsymbol{B}\text{がLWE行列} \end{matrix} \right] - \Pr\left[\begin{matrix} D(\boldsymbol{B}) = 1: \\ \boldsymbol{B}\text{がランダム行列} \end{matrix} \right] \right| \\
&= \mathrm{negl}(\lambda) \ (\because \text{LWE仮定})
\end{aligned}
$$

Regev暗号：IND-CPA安全性

Game_1

攻撃者A　　チャレンジャー

$\boldsymbol{B} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$

$b_1 \leftarrow \{0,1\}$

$\boldsymbol{r} \leftarrow \{0,1\}^m$

$\boldsymbol{c}^* = \boldsymbol{B}\boldsymbol{r} + b_1 \cdot \begin{bmatrix} 0 \\ \underline{q} \\ 2 \end{bmatrix} \in \mathbb{Z}_q^{n+1}$

$(\boldsymbol{B}, \boldsymbol{c}^*)$

b_1'

変換

Game_2

攻撃者A　　チャレンジャー

$\boldsymbol{B} \leftarrow \mathbb{Z}_q^{(n+1)\times m}$

$b_2 \leftarrow \{0,1\}$

$\boldsymbol{c}^* \leftarrow \mathbb{Z}_q^{n+1}$

$(\boldsymbol{B}, \boldsymbol{c}^*)$

b_2'

暗号文が平文に依存しないので，
AがGame_2に勝つ確率は高々1/2

Regularity Lemma (or Leftover Hash Lemma)[GKPV10]

$m \approx 2n\log q$であれば，　（無制限の計算能力を持つ）
どのようなアルゴリズムAに対しても，

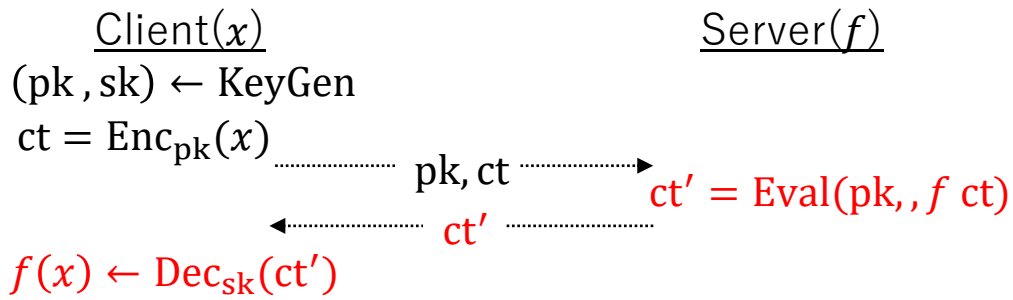
$$\left|\Pr\left[\begin{matrix} A(\boldsymbol{B}, \boldsymbol{B}\boldsymbol{r} \in \mathbb{Z}_q^n) = 1: \\ \boldsymbol{B} \leftarrow \mathbb{Z}_q^{n\times m}; \boldsymbol{r} \leftarrow \{0,1\}^m \end{matrix}\right] - \Pr\left[\begin{matrix} A(\boldsymbol{B}, \boldsymbol{u}) = 1: \\ \boldsymbol{B} \leftarrow \mathbb{Z}_q^{n\times m}; \boldsymbol{u} \leftarrow \mathbb{Z}_q^n \end{matrix}\right]\right| = \mathrm{negl}(\lambda)$$

$$\begin{aligned} &|\Pr[b_1 = b_1'] - \Pr[b_2 = b_2']| \\ &= \left| \begin{pmatrix} \Pr[b_1 = 0] \cdot \Pr[b_1' = 0 | b_1 = 0] \\ +\Pr[b_1 = 1] \cdot \Pr[b_1' = 1 | b_1 = 1] \end{pmatrix} - \begin{pmatrix} \Pr[b_2 = 0] \cdot \Pr[b_2' = 0 | b_2 = 0] \\ +\Pr[b_2 = 1] \cdot \Pr[b_2 = 1 | b_2 = 1] \end{pmatrix} \right| \\ &= \frac{1}{2}\left| \begin{pmatrix} \Pr[b_1' = 0 | b_1 = 0] \\ -\Pr[b_2' = 0 | b_2 = 0] \end{pmatrix} + \begin{pmatrix} \Pr[b_1' = 1 | b_1 = 1] \\ -\Pr[b_2 = 1 | b_2 = 1] \end{pmatrix} \right| \\ &= \mathrm{negl}(\lambda) \end{aligned}$$

[GKPV10] Shafi Goldwasser, Yael Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the Learning with Errors Assumption. In ICS, 2010.

完全準同型暗号（Fully Homomorphic Encryption, FHE）

- 暗号化したまま計算できる公開鍵暗号方式
  - KeyGen, Enc, Dec, に加えてEval の4つのアルゴリズムからなる
  - 安全性は（主に）格子問題の解読困難性で保証される



- 2009年に初めて方式が構成されてから多くの方式が提案されている[Vai]
  - Gen I: **[Gentry, STOC'09]**, [Dijk, Gentry, Halevi, Vaikuntanathan, EUROCRYPT'10], [Smart, Vercauteren, PKC'10], [Gentry, CRYPTO'10], [Halevi, Gentry, FOCS'11]
  - Gen II: **[Brakerski, Vaikuntanathan, FOCS'11], [Brakerski, Gentry, Vaikuntanathan, ITCS'12],** [Brakerski, CRYPTO'12], [Gentry, Halevi, Smart, EUROCRYPT'12], [Gentry, Halevi, Smart, CRYPTO'12]
  - Gen III: **[Gentry, Sahai, Waters, CRYPTO'13]**, [Brakerski, Vaikuntanathan, ITCS' 14], [Alperin-Sheriff, Peikert, CRYPTO'14], [Ducas, Micciancio, EUROCRYPT'15], [Hiromasa, Abe, Okamoto, PKC'15], [Chillotti, Gama, Georgieva, Izabachene, ASIACRYPT'16]

- Gentry-Sahai-Waters FHE (GSW FHE)
  - 構成がかなりシンプル（行列の足し算・掛け算の知識だけで理解できる）
  - 安全性はLWE仮定の下で保証される

The 2022 Gödel Prize

The 2022 Gödel Prize is awarded to the following papers

- Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106. SIAM Journal of Computing 43(2): 831-871 (2014)
- Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012: 309-325. ACM Transactions on Computation Theory 6(3): 13:1-13:36 (2014)

The above papers made transformative contributions to cryptography by constructing efficient fully homomorphic encryption (FHE) schemes.

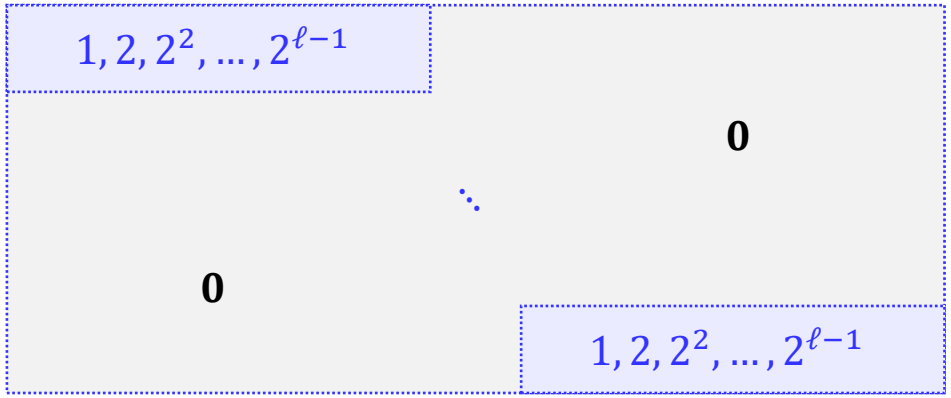
https://eatcs.org/index.php/component/content/article/1-news/2917-2022-05-21-20-13-45

[Vai] Vinod Vaikuntanathan. Homomorphic Encryption Reference. http://people.csail.mit.edu/vinodv/FHE/FHE-refs.html

Gadget行列

- ガジェット行列（$q = 2^{\ell}$）

$$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{g}^T & & \boldsymbol{0} \\ & \ddots & \\ \boldsymbol{0} & & \boldsymbol{g}^T \end{pmatrix} \text{ for } \boldsymbol{g}^T = (1, 2, \dots, 2^{\ell-1})$$



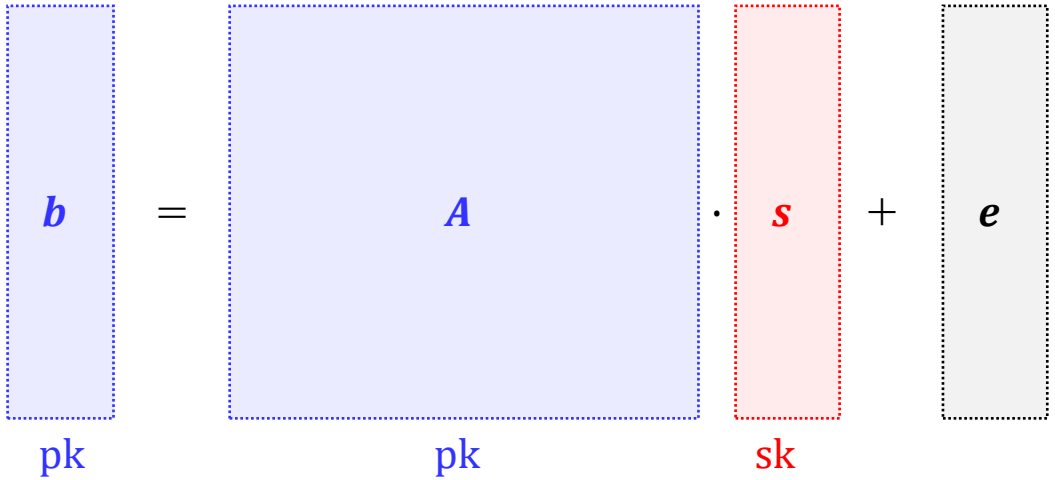
- 関数G^{-1}

$$\boldsymbol{G}^{-1}: \mathbb{Z}_q^n \to \{0,1\}^{n\lceil \log q \rceil} \text{ s.t. } \forall \boldsymbol{x} \in \mathbb{Z}_q^n, \boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{x}) = \boldsymbol{x} \in \mathbb{Z}_q^n$$

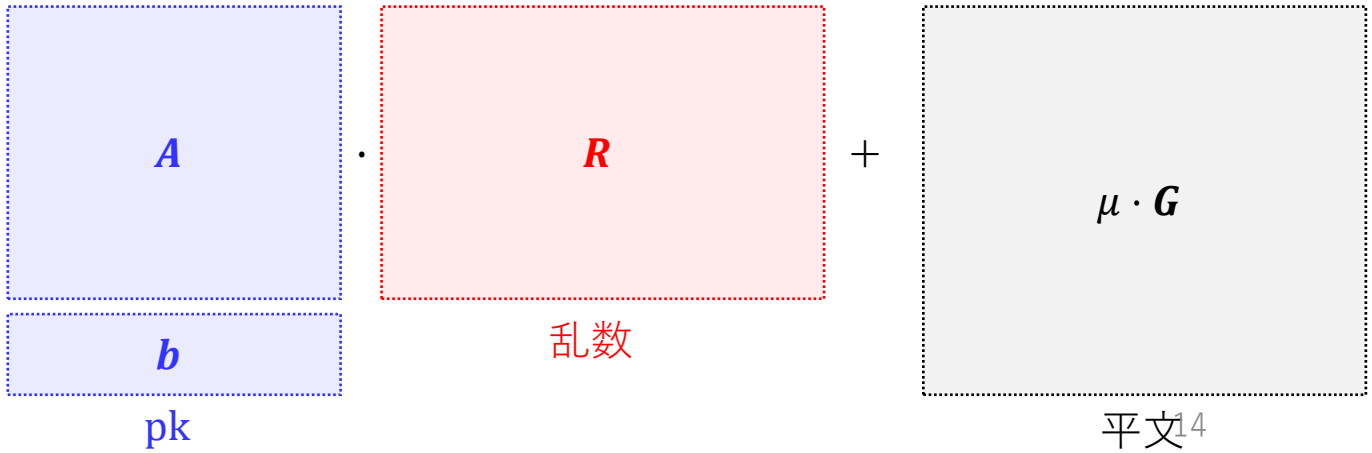
  - （一般的には）ベクトルの各要素のビット列分解
    $\boldsymbol{G}^{-1}\big((3,4,7)\big) = (1,1,0,0,0,1,1,1,1) = \boldsymbol{v}^T$
    $\boldsymbol{G}\boldsymbol{v} = (1\cdot 1 + 2\cdot 1 + 2^2\cdot 0, 1\cdot 0 + 2\cdot 0 + 2^2\cdot 1, 1\cdot 1 + 2\cdot 1 + 2^2\cdot 1) = (3,4,7)$
  - 行列に対しても拡張可能：行列$\boldsymbol{M} = (\boldsymbol{m_1}, \dots, \boldsymbol{m_n}) \in \mathbb{Z}^{n\times n}$に対して，
    $\boldsymbol{G}^{-1}(\boldsymbol{M}) = [\boldsymbol{G}^{-1}(\boldsymbol{m}_1) || \cdots || \boldsymbol{G}^{-1}(\boldsymbol{m}_n)] \in \{0,1\}^{n\ell\times n}$

GSW FHE：鍵生成，暗号化

- **KeyGen:** # Regev暗号と同じ
  - Sample $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$, $\boldsymbol{e} \leftarrow D_{\mathbb{Z}_q^m,s}$
  - Compute $\left(\boldsymbol{A}, \boldsymbol{b^T} = \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}\right) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$
  - Output $\mathrm{pk} = \boldsymbol{B} = \begin{bmatrix}\boldsymbol{A}\\ \boldsymbol{b}^{\mathrm{T}}\end{bmatrix}, \mathrm{sk} = \boldsymbol{t}^{\mathrm{T}} = \left(-\boldsymbol{s}^{\mathrm{T}}, 1\right)$

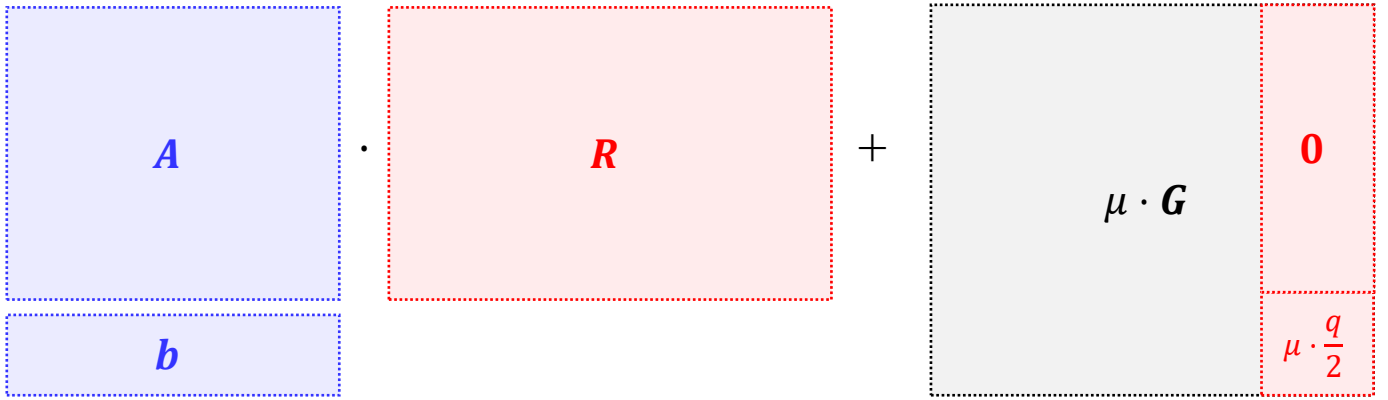


- $\mathrm{Enc}_{\mathrm{pk}}(\mu \in \{0,1\})$
  - Sample $\boldsymbol{R} \leftarrow \{0,1\}^{m\times n\lceil \log q\rceil}$
  - Compute $\boldsymbol{C} = \boldsymbol{BR} + \mu \cdot \boldsymbol{G} \in \mathbb{Z}_q^{(n+1)\times(n+1)\ell}$
  - Output $\mathrm{ct} = \boldsymbol{C}$



GSW FHE：復号

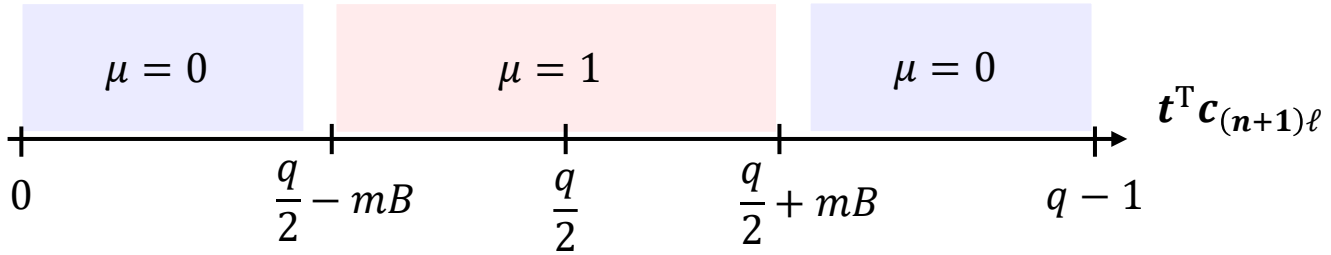
- $\mathrm{Dec}_{\mathrm{sk}}(\mathrm{ct})$
  - Output 1 if $\mathbf{t}^{\mathrm{T}}\boldsymbol{c}_{(n+1)\ell} \approx q/2$,
    and 0 otherwise.
    # $\boldsymbol{c}_{(n+1)\ell}$ は$\boldsymbol{C}$の$(n+1)\ell$列目のベクトル



- 秘密鍵ベクトル$\boldsymbol{t}$と暗号文行列$\boldsymbol{C}$の関係

  $\boldsymbol{t}^{\mathrm{T}}\boldsymbol{C} = \boldsymbol{t}^{T}(\boldsymbol{BR} + \mu \cdot \boldsymbol{G}) = \boldsymbol{e}^{\mathrm{T}}\boldsymbol{R} + \mu \cdot \boldsymbol{t}^{\mathrm{T}}\boldsymbol{G} = \boldsymbol{e'}^{\mathrm{T}} + \mu \cdot \boldsymbol{t}^{\mathrm{T}}\boldsymbol{G}$

  - $\boldsymbol{R} \in \{0,1\}^{m \times n\ell}, |\boldsymbol{e}| < B$なので，$\left|e'^{T}\right| < mB$
  - $\boldsymbol{t}$と$\boldsymbol{c}_{(n+1)\ell}$の掛け算：$\boldsymbol{t}^{\mathrm{T}}\boldsymbol{c}_{(n+1)\ell} = \boldsymbol{e}^{T}\boldsymbol{r}_{\ell} + \mu \cdot q/2$ （Regev暗号と同様に正しく復号できる）



GSW FHE：正当性、Eval

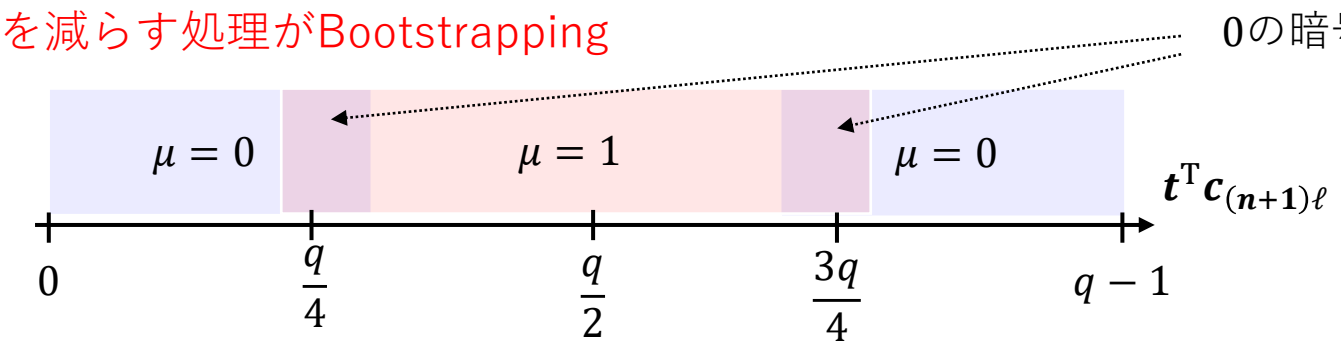
- 秘密鍵ベクトル$\boldsymbol{t}$と暗号文行列$\boldsymbol{C}$の関係

$$\boldsymbol{t}^{\mathrm{T}}\boldsymbol{C} = \boldsymbol{e'}^{\mathrm{T}} + \mu \cdot \boldsymbol{t}^{\mathrm{T}}\boldsymbol{G}$$

- 暗号文行列$\boldsymbol{C_1}, \boldsymbol{C_2}$の準同型演算（暗号化したままの演算）
  - 加算（XOR）：
    - $\boldsymbol{C}_{\mathrm{add}} = \boldsymbol{C}_1 + \boldsymbol{C}_2$,
    - $\boldsymbol{t}^{\mathrm{T}}\boldsymbol{C}_{\mathrm{add}} = \boldsymbol{t}^{\mathrm{T}}\boldsymbol{C}_1 + \boldsymbol{t}^{\mathrm{T}}\boldsymbol{C}_2 = (\boldsymbol{e}_1'^{T} + \boldsymbol{e}_2'^{T}) + (\mu_1 + \mu_2) \cdot \boldsymbol{t}^{\mathrm{T}}G$
  - 乗算（AND）：
    - $\boldsymbol{C}_{\mathrm{mult}} = \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$
    - $\boldsymbol{t}^{\mathrm{T}}\boldsymbol{C}_{\mathrm{mult}} = \boldsymbol{t}^{T}\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = \boldsymbol{e}_1'^{T}\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + \mu_1\boldsymbol{t}^{T}\boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = (\boldsymbol{e}_1'^{T}\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + \mu_1 \cdot \boldsymbol{e}_2'^{T}) + \mu_1\mu_2 \cdot \boldsymbol{t}^{T}\boldsymbol{G}$
  - NAND：
    - $\boldsymbol{C}_{\mathrm{NAND}} = \boldsymbol{G} - \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$
    - $\boldsymbol{t}^{T}\boldsymbol{C}_{NAND} = \boldsymbol{t}^{T}\boldsymbol{G} - \left(\boldsymbol{e}_1'^{T}\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + \mu_1 \cdot \boldsymbol{e}_2'^{T}\right) - \mu_1\mu_2 \cdot \boldsymbol{t}^{T}\boldsymbol{G} = -\left(\boldsymbol{e}_1'^{T}\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + \mu_1 \cdot \boldsymbol{e}_2'^{T}\right) + (1 - \mu_1\mu_2) \cdot \boldsymbol{t}^{T}\boldsymbol{G}$

GSW FHE：Bootstrapping

- 準同型演算すると暗号文に含まれるノイズが増加
  - ノイズが一定値（例えば$\mathrm{q}/4$）より大きくなると，暗号文を正しく復号できない
  - 暗号文内のノイズを減らす処理がBootstrapping



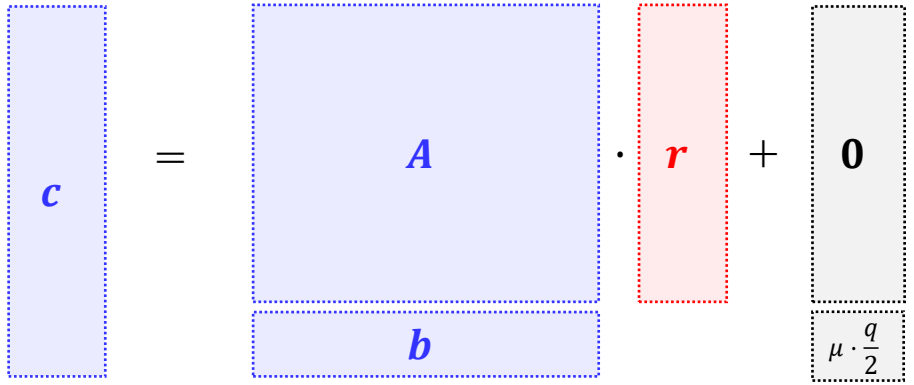
- Bootstrapping
  - 暗号化したまま復号回路Decを計算
  - 暗号文C, 秘密鍵の暗号文$C_{\mathrm{sk}} = \mathrm{Enc}_{\mathrm{pk}}(\mathrm{sk})$から$\mathrm{Eval}(\mathrm{Dec}'_c, C_{\mathrm{sk}})$を計算（$\mathrm{Dec}'_c\ (\mathrm{sk}) \coloneqq \mathrm{Dec}_{\mathrm{sk}}(c)$）
  - NANDの準同型演算毎にbootstrappingすることで無制限に準同型暗号できる
    → 暗号パラメータが演算する回路に依存しない

Decは$\mathbb{Z}_q^n$のベクトルの内積
→$O(\log n)$程度の深さの回路で表される

Regev暗号 & GSW FHE

Regev暗号

- 暗号文はベクトル$\boldsymbol{c} \in \mathbb{Z}_q^{(n+1)}$ s.t. $\boldsymbol{t}^T\boldsymbol{c} = \text{noise} + \mu \cdot q/2$ for $\boldsymbol{t} \in \mathbb{Z}_q^{n+1}$.
- 暗号文サイズ ≈2KB



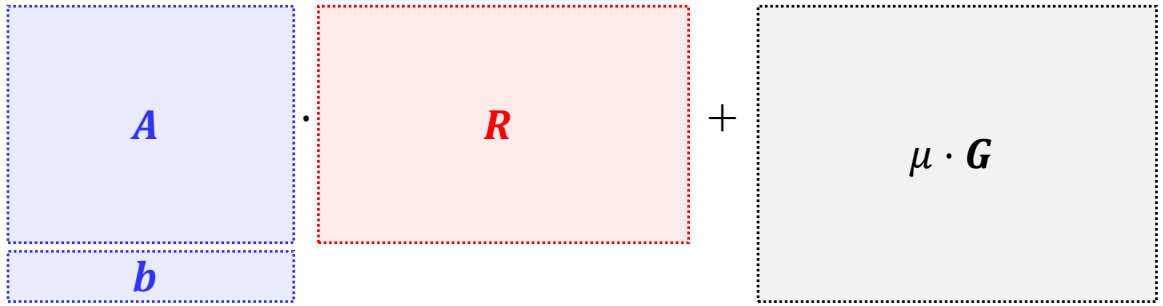
GSW FHE

- 暗号文は行列$\boldsymbol{C} \in \mathbb{Z}_q^{(n+1)\times(n+1)\ell}$ s.t. $\boldsymbol{t}^T\boldsymbol{C} = \text{noise} + \mu \cdot \boldsymbol{t}^T G$ for $\boldsymbol{t} \in \mathbb{Z}_q^{n+1}$
- XOR, AND, NANDの準同型演算

$$\boldsymbol{t}^T(\boldsymbol{C}_1 + \boldsymbol{C}_2) = (\text{noise}_1 + \text{noise}_2) + (\mu_1 + \mu_2) \cdot \boldsymbol{t}^T G$$

$$\boldsymbol{t}^T\left(\boldsymbol{C}_1 \boldsymbol{G}^{-1}(\boldsymbol{C}_2)\right) = (\text{noise}_1 \boldsymbol{G}^{-1}(\boldsymbol{C}_2) + \mu_1 \cdot \text{noise}_2) + \mu_1\mu_2 \cdot \boldsymbol{t}^T \boldsymbol{G}$$

$$\boldsymbol{t}^{\mathrm{T}}\left(\boldsymbol{G} - \boldsymbol{C}_1 \boldsymbol{G}^{-1}(\boldsymbol{C}_2)\right) = -(\text{noise}_1 \boldsymbol{G}^{-1}(\boldsymbol{C}_2) + \mu_1 \cdot \text{noise}_2) + (1 - \mu_1\mu_2) \cdot \boldsymbol{t}^T \boldsymbol{G}$$



- 暗号文行列$\boldsymbol{C}$の$(n+1)\ell$番目の列ベクトル$c_{(n+1)\ell}$はRegev暗号文：$\boldsymbol{t}^T\boldsymbol{c}_{(n+1)\ell} = \text{noise} + \mu \cdot (q/2)$
- 暗号文サイズ ≈32KB、NAND（+bootstrapping）≈10ms

Gadget行列の性質: $\boldsymbol{G}$ –Trapdoor[MP12]

- Gadget行列$\boldsymbol{G}$についてのLWE問題は簡単に解ける （$\boldsymbol{b} = \boldsymbol{s}^T\boldsymbol{G} + \boldsymbol{e}$から$\boldsymbol{s}$を計算できる）
  - $q = 2^\ell$のとき（qが素数のときも処理自体は異なるが$\boldsymbol{s}$を計算できる）：

$$(b_1, b_2, \dots, b_\ell, \dots) = (s_1 + e_1, 2s_1 + e_2, \dots, 2^{\ell-2}s_1 + e_{\ell-1}, 2^{\ell-1}s_1 + e_\ell, \dots)$$

$$s_{1,0} = \begin{cases} 1 & \text{if } b_\ell \geq \frac{q}{2}, \\ 0 & \text{otherwise} \end{cases}$$

$$s_{1,1} = \begin{cases} 1 & \text{if } b_{\ell-1} - 2^{\ell-2} \cdot s_{1,0} \geq \frac{q}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

$$\vdots$$

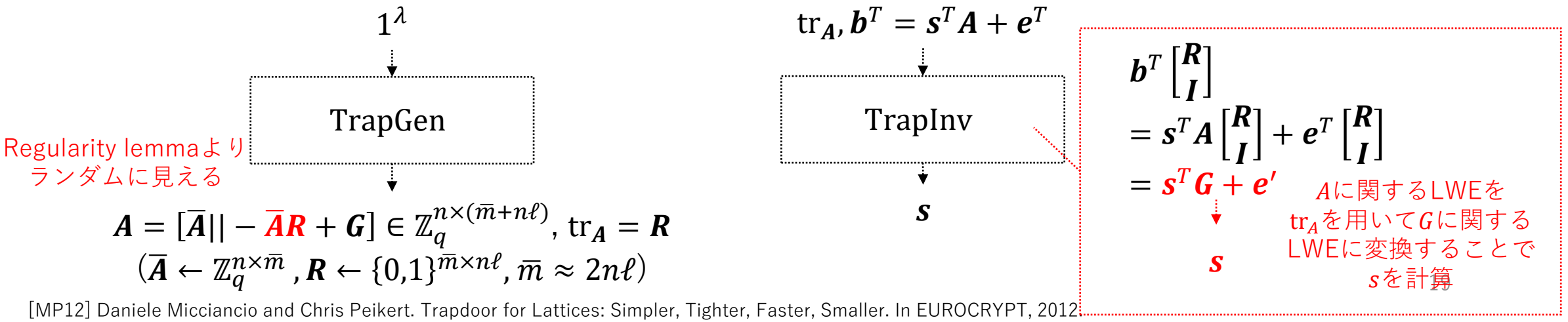
s_1のビット分解: $s_1 = \sum_{i\in[0,\ell-1]} s_{1,i} \cdot 2^i$

$b_\ell =$ | $s_{1,0}$ | e_ℓ |

msb

$b_{\ell-1} =$ | $s_{1,1}$ | $s_{1,0}$ | $e_{\ell-1}$ |

msb



[MP12] Daniele Micciancio and Chris Peikert. Trapdoor for Lattices: Simpler, Tighter, Faster, Smaller. In EUROCRYPT, 2012

量子性検証プロトコル

- （量子）証明者と古典検証者の間のプロトコル
  - 古典検証者は量子的な計算をせずとも，証明者が量子アルゴリズムであることを検証

- 典型的には，LWE問題の困難性の下で構成されるclaw-free functionを用いて構成される[BCM+18]
  - このclaw-free function自体は量子計算の古典検証プロトコル[Mah18]などで利用される

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device. In FOCS, 2018
[Mah18] Urmila Mahadev. Classical Verification of Quantum Computation. In FOCS, 2018.

Noisy Trapdoor Claw-free function（NTCF）

- 関数族

ある有限集合　鍵空間

$$F := \{f_{k,b} : X \to D_Y\}_{k \in K, b \in \{0,1\}}$$

ある有限集合Y上の確率分布の集合

- ４つのアルゴリズム
  - 鍵生成：$(k, t_k) \leftarrow \mathrm{Gen}(1^\lambda)$
  - 逆元計算：$x \leftarrow \mathrm{Inv}(t_k, b \in \{0,1\}, y \in Y)$
  - 値域の要素確認：
    $1 \text{ or } 0 \leftarrow \mathrm{Chk}(k \in K, b, x \in X, y)$
    output 1 if $y \in \mathrm{Supp}(f_{k,b}(x))$; 0 otherwise.

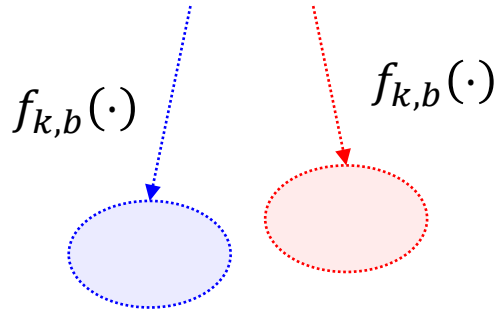
- サンプリング：$|\psi\rangle = \mathrm{Samp}(k, b)$

$$|\psi\rangle \approx \sum_{x \in X, y \in Y} \sqrt{(f_{k,b}(x)(y)}|x\rangle|y\rangle$$

Noisy Trapdoor Claw-free Function (NTCF)

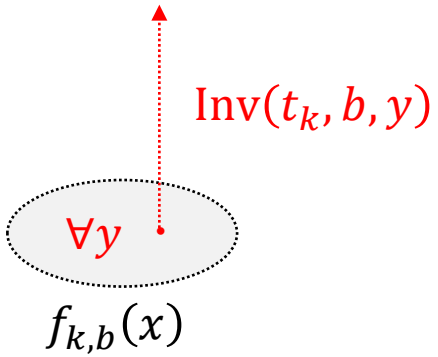
Trapdoor injectivity

$\forall b \in \{0,1\}, x \neq x' \in X$



$\mathrm{Supp}\left(f_{k,b}(x)\right) \cap \mathrm{Supp}\left(f_{k,b}(x')\right) = \phi$

$\forall b \in \{0,1\}, x \in X$



Clawの集合

$R_k \coloneqq \{(x_0, x_1) : f_{k,0}(x_0) = f_{k,1}(x_1)\}$

Efficient Range Superposition

$\exists f'_{k,b},$

$\mathrm{Samp}(k,b)$

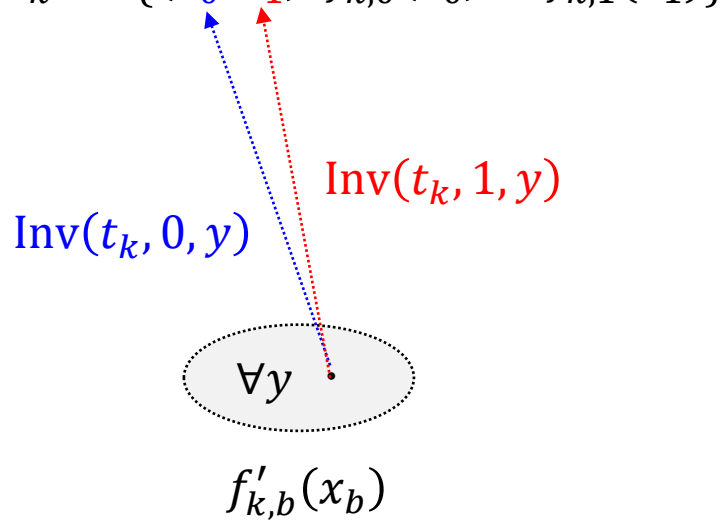
$= |\psi\rangle$

$= \sum_{x \in X, y \in Y} \sqrt{\left(f'_{k,b}(x)\right)(y)}\,|x\rangle|y\rangle$

$\approx$

$\sum_{x \in X, y \in Y} \sqrt{\left(f_{k,b}(x)\right)(y)}\,|x\rangle|y\rangle$

$R_k \coloneqq \{(x_0, x_1) : f_{k,0}(x_0) = f_{k,1}(x_1)\}$



Noisy Trapdoor Claw-free function（NTCF）

- （Adaptive hardcore bit性）：
  - 以下の集合を考える：

$\mathrm{d} \in G_{k,b,x}$かどうかはk, t_k, b, xから効率的にチェックできる

$$G_{k,b,x} \text{ s.t. } \Pr\left[d \in G_{k,b,x} : d \leftarrow \{0,1\}^w\right] = \mathrm{negl}(\lambda)$$

x_bのビット列表現

$$H_k := \left\{ \begin{array}{c} \left(b, x_b, d, d \cdot \left(J(x_0) \oplus J(x_1)\right)\right) : \\ b \in \{0,1\}, (x_0, x_1) \in R_k, d \in G_{k,0,x_0} \cap G_{k,1,x_1} \end{array} \right\}$$

$$H'_k := \{(b, x_b, d, c) : (b, x_b, d, c \oplus 1) \in H_k\}$$

  - 任意の多項式時間量子攻撃者Aに対して，

$$\left|\Pr\left[A(k) \in H_k : (k, t_k) \leftarrow \mathrm{Gen}(1^\lambda)\right] - \Pr\left[A(k) \in H'_k : (k, t_k) \leftarrow \mathrm{Gen}(1^\lambda)\right]\right| = \mathrm{negl}(\lambda)$$

量子性検証プロトコル

検証者　　証明者

$(k, t_k) \leftarrow \mathrm{Gen}$

k →

← $y \in Y$

$c \in \{0,1\}$ →

Accept if $\mathrm{Chk}(k, b, x_b, y) = 1$

← (b, x_b) if $c = 0$　Preimage test

$x_0 \leftarrow \mathrm{Inv}(k, t_k, 0, y)$
$x_1 \leftarrow \mathrm{Inv}(k, t_k, 1, y)$
Accept if $d \cdot (x_0 \oplus x_1) = 0$

← d if $c = 1$　Equation test

高い確率で両方のテストにacceptされる（古典）証明者が存在すれば、
その証明者（アルゴリズム）を用いてadaptive hardcore bit性を破れる

↓

Adaptive hardcore bit性から、少なくともこのプロトコルに高い確率で
acceptされる証明者は古典アルゴリズムではない

NTCFの構成

（公開情報だけから計算できない）NTCF

$$\left(f_{k,b}(x)\right)(y) = D_{B_0}(y - \boldsymbol{A}x - b \cdot \boldsymbol{As})$$

$f_{k,b}$のsupport

- $\mathrm{Supp}\left(f_{k,0}(x)\right) = \{\boldsymbol{A}x + \boldsymbol{e}_0 : \boldsymbol{e}_0 \in \mathrm{Supp}(D_{B_0})\}$
- $\mathrm{Supp}\left(f_{k,1}(x)\right) = \{\boldsymbol{A}(x + \boldsymbol{s}) + \boldsymbol{e}_0 : \boldsymbol{e}_0 \in \mathrm{Supp}(D_{B_0})\}$

つまり，xと$x - \boldsymbol{s}$に対して同じsupportを持つ

$\mathrm{Inv}(t_k, b \in \{0,1\}, y \in Y)$:

- $\boldsymbol{s}_0 \leftarrow \mathrm{TrapInv}(\mathrm{tr}_{\boldsymbol{A}}, y)$
- Output $\boldsymbol{s}_0 - b \cdot \boldsymbol{s}$

（公開情報だけから計算できる）NTCF

$$\left(f'_{k,b}(x)\right)(y) = D_{B_0}(y - \boldsymbol{A}x - b \cdot (\boldsymbol{As} + \boldsymbol{e}))$$

$\mathrm{Gen}(1^\lambda)$:

- $(\boldsymbol{A}, \mathrm{tr}_{\boldsymbol{A}}) \leftarrow \mathrm{TrapGen}(1^\lambda)$
- Sample $\boldsymbol{s} \leftarrow \{0,1\}^n$ and $\boldsymbol{e} \leftarrow D_B$
- $k = (\boldsymbol{A}, \boldsymbol{t} = \boldsymbol{As} + \boldsymbol{e})$ and $t_k = (\mathrm{tr}_A, \boldsymbol{s})$

$f'_{k,b}$のsupport

- $\mathrm{Supp}\left(f'_{k,0}(x)\right) = \mathrm{Supp}\left(f_{k,0}(x)\right)$
- $\mathrm{Supp}\left(f'_{k,1}(x)\right) = \{\boldsymbol{A}(x + \boldsymbol{s}) + \boldsymbol{e}_0 + \boldsymbol{e} : \boldsymbol{e}_0 \in \mathrm{Supp}(D_{B_0})\}$

B_0をBより十分大きくとると
$e_0 + e$とe_0の分布が識別できない

$\mathrm{Chk}(k, b, x, y)$

- $e' = y - \boldsymbol{A}x - b \cdot (\boldsymbol{As} + \boldsymbol{e})$
- Output 1 if $\left|\left|e'\right|\right|_2 \leq B_0\sqrt{m}$, and 0 otherwise.

NTCFの構成

- $\mathrm{Samp}(k, b)$
  - Sample $\sum_{\boldsymbol{e}_0} \sqrt{D_{B_0}(\boldsymbol{e}_0)}\,|\boldsymbol{e}_0\rangle$ (by [Lem3.12, Reg05])
  - Compute $\sum_{x\in X,\boldsymbol{e}_0} \sqrt{D_{B_0}(\boldsymbol{e}_0)}\,|x\rangle|\boldsymbol{e}_0\rangle$
  - Using k and b, compute

    $\sum_{x\in X,e_0} \sqrt{D_{B_0}(\boldsymbol{e}_0)}\,|x\rangle|\boldsymbol{e}_0\rangle_e|\boldsymbol{A}x+\boldsymbol{e}_0+b\cdot\boldsymbol{t}\rangle$
  - Uncompute e register to obtain

    $\sum_{x\in X,e_0} \sqrt{D_{B_0}(\boldsymbol{e}_0)}\,|x\rangle|\boldsymbol{A}x+\boldsymbol{e}_0+b\cdot\boldsymbol{t}\rangle$

    $=\sum_{x,y} \sqrt{D(y-\boldsymbol{A}x-b\cdot\boldsymbol{t})}\,|x\rangle|y\rangle$

    $=\sum_{x,y} \sqrt{(f'_{k,b}(x))(y)}\,|x\rangle|y\rangle$

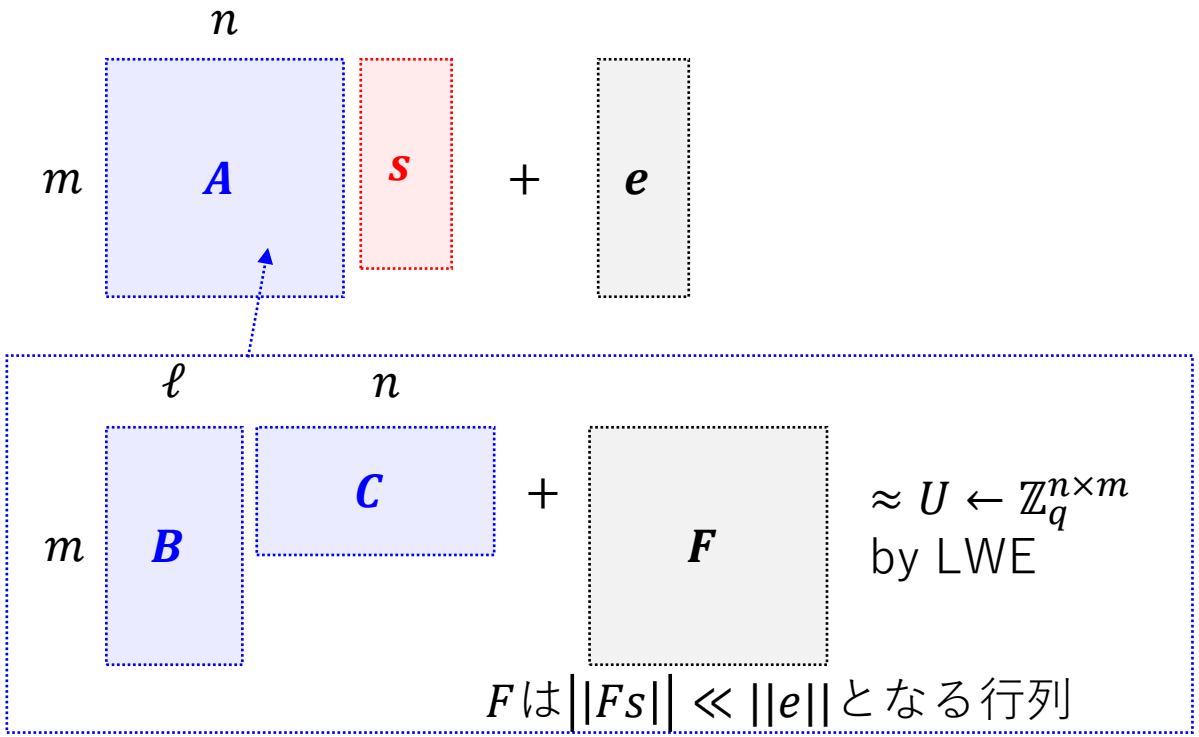
[Reg05] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In STOC, 2005.

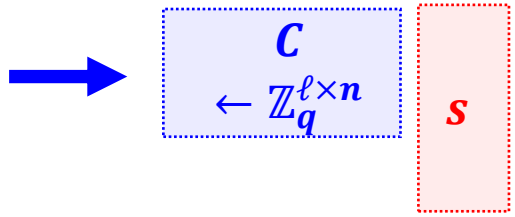
Adaptive hardcore bit性

Hardcore predicateに相当するdをうまく選べたとしてもhardcore bitを推測することは難しい

$s \in \{0,1\}^n, x_1 = x_0 - \boldsymbol{s}$より,
$d \cdot \left(J(x_0) \oplus J(x_1)\right) = \hat{d} \cdot \boldsymbol{s}$ for some $\hat{d}$ ($\hat{d}$はdに依存)

Hardcore bit以外に$\boldsymbol{s}$が依存している情報は…





頑張って計算すると…

$, \hat{d} \cdot \boldsymbol{s} \approx b \leftarrow \{0,1\}$

$\boldsymbol{s}$の情報が圧縮されている

まとめ

- 格子ベースの暗号技術について紹介
  - 公開鍵暗号：Regev暗号
  - 完全準同型暗号：Gentry-Sahai-Waters FHE (GSW FHE)
  - Noisy trapdoor claw-free function (NTCF)

- 展望
  - 格子は多彩な暗号技術を実現できる数理的な基盤
  - 完全準同型暗号（理論的な構成というよりかは実用化へ向けた研究フェーズ）
    - より効率的な方式の設計？
    - 具体的なパラメータ選定？
  - NTCF
    - 格子以外の（耐量子）仮定からの構成？