Post-Quantum Cryptography
耐量子暗号

NTT セキュアプラットフォーム研究所
草川恵太

今日の予定

- 量子計算機と耐量子暗号と NIST の標準化 (30min–1h)
- Regev の LWE $\geq$ SIVP の解説 (1h–1.5h)
- (暗号を量子構成する話 30min)

!!! A Personal View !!!

量子計算機とアニーラ

アニーラー

- 物理計算機の一種
  e.g., スパゲティソート、膜による最短経路の解法、三体問題
- 2008 年頃から D-Wave 社が量子アニーラーを言い始める
- 問題を物理状態にマッピングして、ゆっくり冷やしてイジング問題を解く
- 進展
  - 2011 – 128 qubits
  - 2013 – 512 qubits
  - 2017 – 2000 qubits
- D-Wave machine vs CIM vs GPGPU
  - 2018/05 CIM vs D-Wave 2000Q [https://arxiv.org/abs/1805.05217]
  - 2018/06 Beating CIM by GPU [https://arxiv.org/abs/1806.08422]

量子計算機

- 色々な実装方法がある（らしい）
- 計算可能性: 古典 TM = 量子 TM
- 計算の効率: 多分 exp. なギャップがある
- Raz and Tal: BQP と PH のオラクル付き分離

量子計算機

- 色々な実装方法がある（らしい）
- 計算可能性: 古典 TM $=$ 量子 TM
- 計算の効率: 多分 exp. なギャップがある
- Raz and Tal: BQP と PH のオラクル付き分離
- 現状
  - SOTA is 72 qubits? 53 qubits?
  - ロードマップ: 次は $>$ 100 qubits な実機が出る（らしい）

アルゴリズム

Grover's Alg. (1996)

- Find $x \in [N]$ s.t. $F(x) = 1$
- 量子: $O(N^{1/2})$ 時間 (最悪時には $\Omega(N^{1/2})$)
- 古典: 最悪時には $\Omega(N)$ 時間

Shor's Alg. (1994)

- N を素因数分解せよ (または離散対数問題を解け)
- 量子: poly($logN$) 時間
- 古典: sub-exp. –exp. 時間

Quantum Random Walk

- 古典ランダムウォークと異なる挙動をする
  $\rightarrow$ グラフ状態を作って探索問題を解けることがある

暗号と量子計算機の関係

共通鍵暗号

Grover's Alg やその応用 (BHT Alg. 等) が怖い

- ブロック暗号: 鍵長を二倍する (AES128→AES256)
- ハッシュ関数: 出力を 3/2 倍する (e.g., SHA256→SHA384)

公開鍵暗号

Shor's Alg. が怖い

- RSA 暗号/署名: 素因数分解されるので、理論的には脆弱
- 離散対数ベースの暗号/署名: 離散対数問題が解かれるので、理論的には脆弱

耐量子暗号

Post-Quantum Cryptography

- 大規模量子計算機 $\rightarrow$ 素因数分解や離散対数問題が解ける
- 耐量子暗号が必要
  量子でも破れない、古典で計算可能な暗号
- 候補
  - ハッシュ・共通鍵ベース
  - 格子ベース
  - 符号ベース
  - 多変数多項式ベース
  - 同種写像ベース
  - 他

NIST PQC 標準化

NIST PQC 標準化スケジュール

- 2015/04: PQC Workshop
- 2016/02: 開始の告知 @ PQCrypto 2016
- 2016/12: Call for Submission
- 2017/11/30: 投稿〆切
- 2017/12/23: Round 1 開始
- 2018/04: 第一回標準化会議
- 2019/01: Round 2 開始
- 2019/08: 第二回標準化会議
- 2020/06 頃: Round 3 開始
- + 2 年?: Draft Standards Ready
- 2022–2024: 標準化文書完成

ただしハッシュベース署名は需要が多いとのことで、先だって SP になる予定

NIST PQC Round 1 Candidates

投稿数 82→ 書類チェックで 69 候補に

BIG QUAKE, BIKE, CFPKM, Classic McEliece, Compact LWE, CRYSTALS-Dilithium, CRYSTALS-Kyber, DAGS, Ding Key Exchange, DME, DRS, DualModeMS, Edon-K, EMBLEM and R.EMBLEM, Falcon, FrodoKEM, GeMSS, Giophantus, Gravity-SPHINCS, GuessAgain, Gui, Hila5, HiMQ-3, HK17, HQC, KCL, KINDI, LAC, LAKE, LEDAkem, LEDApkc, Lepton, Lima, Lizard, LOCKER, LOTUS, LUOV, McNie, Mersenne-756839, MQDSS, NewHope, NTRUEncrypt, pqNTRUsign, NTRU-HRSS-KEM, NTRU Prime, NTS-KEM, Odd Manhattan, Ouroboros-R, Picnic, Post-Quantum RSA-Encryption, Post-Quantum RSA-Signature, pqsigRM, QC-MDPC KEM, qTESLA, RaCoSS, Rainbow, Ramstake, RankSign, RLCE-KEM, Round2, RQC, RVB, SABER, SIKE, SPHINCS+, SRTPI, Three Bears, Titanium, WalnutDSA

NIST PQC Round 1: 暗号と署名

(DME と SRTPI は暗号と署名の両方を提案している)

暗号 49: BIG QUAKE, BIKE, CFPKM, Classic McEliece, Compact LWE, CRYSTALS-Kyber, DAGS, Ding Key Exchange, DME, Edon-K, EMBLEM and R.EMBLEM, FrodoKEM, Giophantus, GuessAgain, Hila5, HK17, HQC, KCL, KINDI, LAC, LAKE, LEDAkem, LEDApkc, Lepton, Lima, Lizard, LOCKER, LOTUS, McNie, Mersenne-756839, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, NTS-KEM, Odd Manhattan, Ouroboros-R, Post-Quantum RSA-Encryption, QC-MDPC KEM, Ramstake, RLCE-KEM, Round2, RQC, RVB, SABER, SIKE, SRTPI, Three Bears, Titanium

署名 22: CRYSTALS-Dilithium, DME, DRS, DualModeMS, Falcon, GeMSS, Gravity-SPHINCS, Gui, HiMQ-3, LUOV, MQDSS, pqNTRUsign, Picnic, Post-Quantum RSA-Signature, pqsigRM, qTESLA, RaCoSS, Rainbow, RankSign, SPHINCS+, SRTPI, WalnutDSA

NIST PQC Round 1: 暗号

暗号 49:

- 符号ベース 17: BIG QUAKE, BIKE, Classic McEliece, DAGS, ~~Edon-K~~, HQC, LAKE, LEDAkem, LEDApkc, Lepton, LOCKER, McNie, NTS-KEM, Ouroboros-R, QC-MDPC KEM, RLCE-KEM, RQC
- 格子ベース 22: Compact LWE, CRYSTALS-Kyber, Ding Key Exchange, EMBLEM and R.EMBLEM, FrodoKEM, Giophantus, Hila5, KCL, KINDI, LAC, Lima, Lizard, LOTUS, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan, Round2, SABER, Titanium, Three Bears
- 多変数多項式ベース 3: CFPKM, DME, ~~SRTPI~~
- 同種写像ベース 1: SIKE
- メルセンヌ素数ベース 2: Mersenne-756839, Ramstake,
- その他 4: Post-Quantum RSA-Encryption, ~~RVB~~, GuessAgain, ~~HK17~~

NIST PQC Round 1: 署名

署名 22:

- 符号ベース 3: pqsigRM, RaCoSS, ~~RankSign~~
- 格子ベース 5: CRYSTALS-Dilithium, DRS, Falcon, pqNTRUsign, qTESLA
- 多変数多項式ベース 8: DME, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow
- ハッシュベース 2: Gravity-SPHINCS, SPHINCS+
- 共通鍵ベース 2: Picnic,
- その他 2: Post-Quantum RSA-Signature, WalnutDSA

RSA ベース

Post-Quantum RSA-Enc/Sig

[BHLV17]

N のサイズが 2^{40} バイトなら、Shor's Alg. でも 2^{100} step 必要

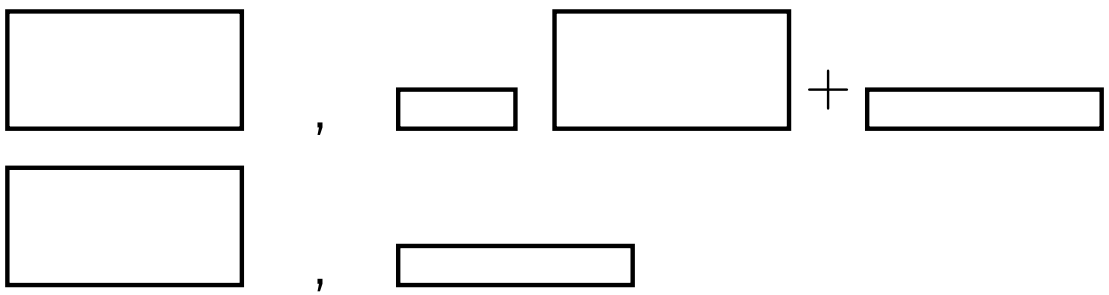
- パラメータ: $K = 2^k$ and B.
- 鍵生成: K 個の異なる B-bit 素数 $P_1, \ldots, P_K$ を生成
- $N = \prod_i P_i$, $e = 3$ とする

- pqrsa-n, N is 2^n-bytes
- pqrsa15, $K = 2^9$, $B = 2^9$
- pqrsa20, $K = 2^{14}$, $B = 2^9$
- pqrsa25, $K = 2^{18}$, $B = 2^{10}$
- pqrsa30, $K = 2^{23}$, $B = 2^{10} \approx$ hard as SHA256 (Category II)

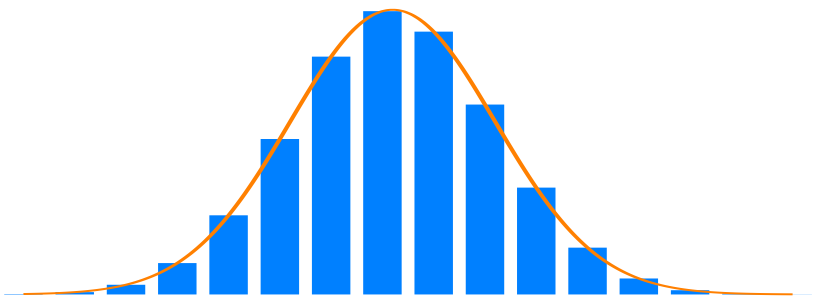
格子ベース

LWE

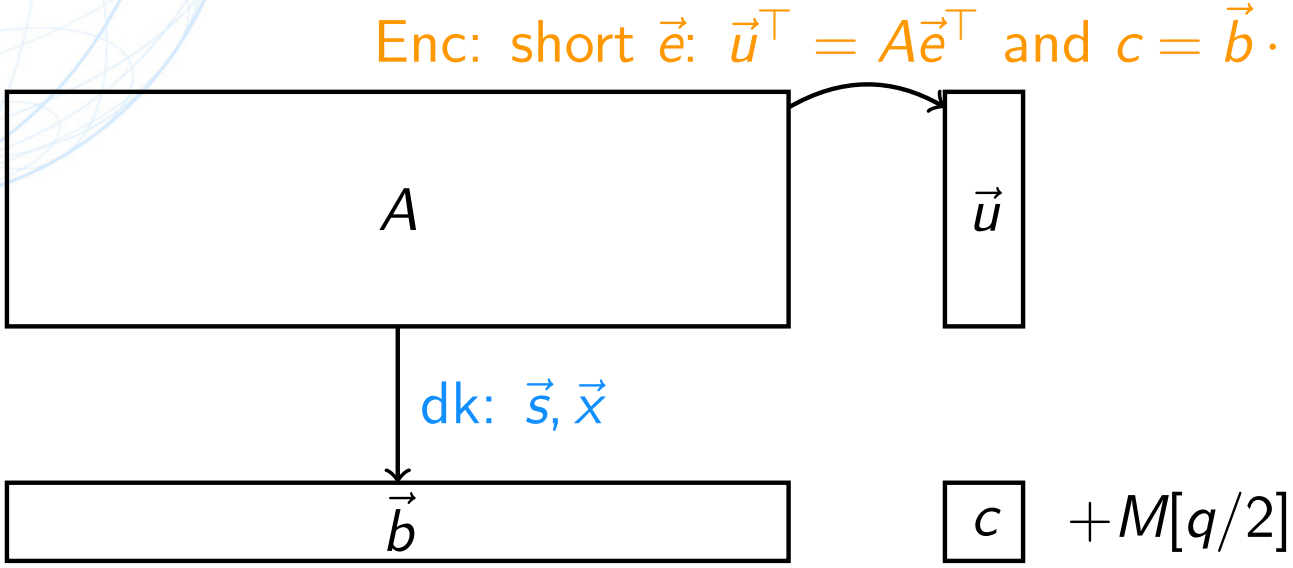
- Learning with Errors (LWE): 以下を識別するのは困難
  - $(A, \vec{s}A + \vec{x})$ $(A \leftarrow \mathbb{Z}_q^{n \times m}, \vec{s} \leftarrow \mathbb{Z}_q^n, \vec{x} \leftarrow \chi^m)$
  - $(A, \vec{b})$ $(A \leftarrow \mathbb{Z}_q^{n \times m}, \vec{b} \leftarrow \mathbb{Z}_q^m)$



χ の例: 離散ガウス分布



Regev PKE [Reg05,Reg09]



$$ek = (A, \vec{b}), dk = (\vec{s}, \vec{x}), ct = (\vec{u}, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - \vec{s} \cdot \vec{u}^\top &= M[q/2] + \vec{b} \cdot \vec{e}^\top - \vec{s} \cdot A\vec{e}^\top \\ &= M[q/2] + (\vec{s}A + \vec{x}) \cdot \vec{e}^\top - \vec{s} \cdot A\vec{e}^\top \\ &= M[q/2] + \vec{x} \cdot \vec{e}^\top \approx M[q/2]\end{aligned}$$

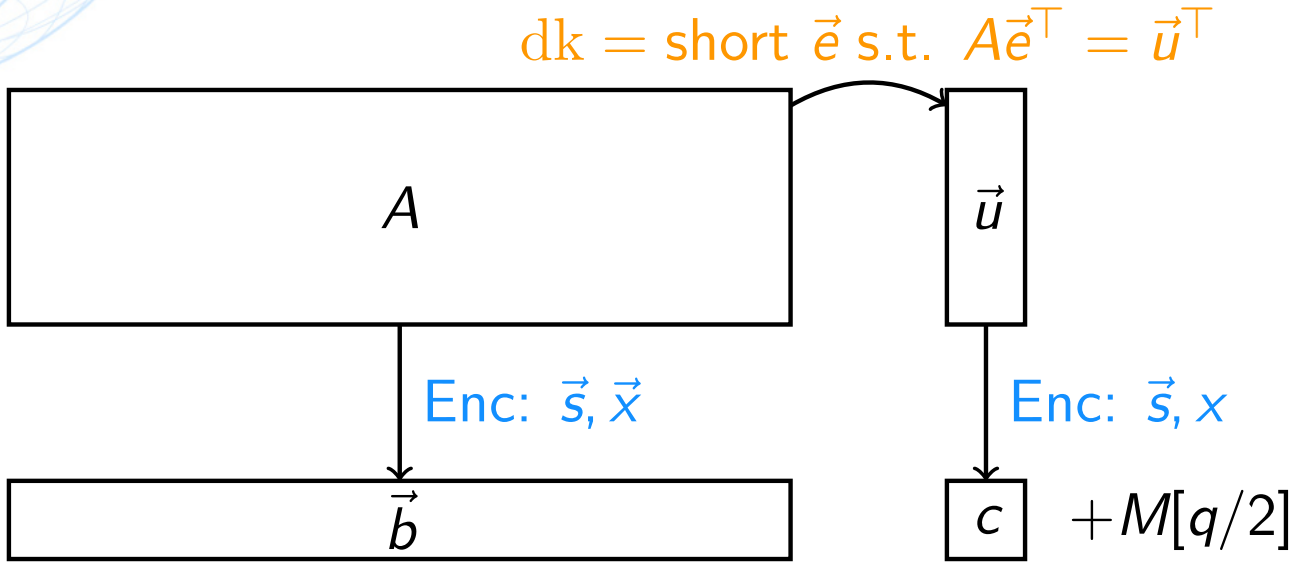
First Goal

Enc 22: Compact LWE, CRYSTALS-Kyber, Ding Key Exchange, EMBLEM and R.EMBLEM, FrodoKEM, Giophantus, Hila5, KCL, KINDI, LAC, Lima, Lizard, LOTUS, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan, Round2, SABER, Titanium, Three Bears

Sig 5: CRYSTALS-Dilithium, DRS, Falcon, pqNTRUsign, qTESLA,

Gentry-Peiekrt-Vaikuntanathan (GPV) PKE

The Dual of Regev

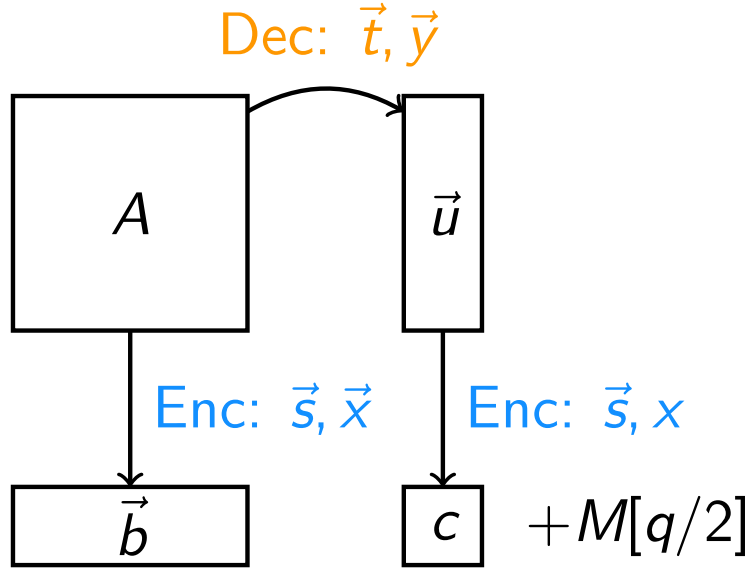


$$ek = (A, \vec{u}), dk = \vec{e}, ct = (\vec{b}, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - \vec{b} \cdot \vec{e}^\top &= M[q/2] + \vec{s} \cdot \vec{u}^\top + x - (\vec{s}A + \vec{x}) \cdot \vec{e}^\top \\ &= M[q/2] + \vec{s} \cdot A \cdot \vec{u}^\top + x - (\vec{s}A + \vec{x}) \cdot \vec{e}^\top \\ &= M[q/2] + x - \vec{x} \cdot \vec{e}^\top \approx M[q/2]\end{aligned}$$

Lindner-Peikert PKE

Let $\vec{s}, \vec{t} \leftarrow \chi^n$

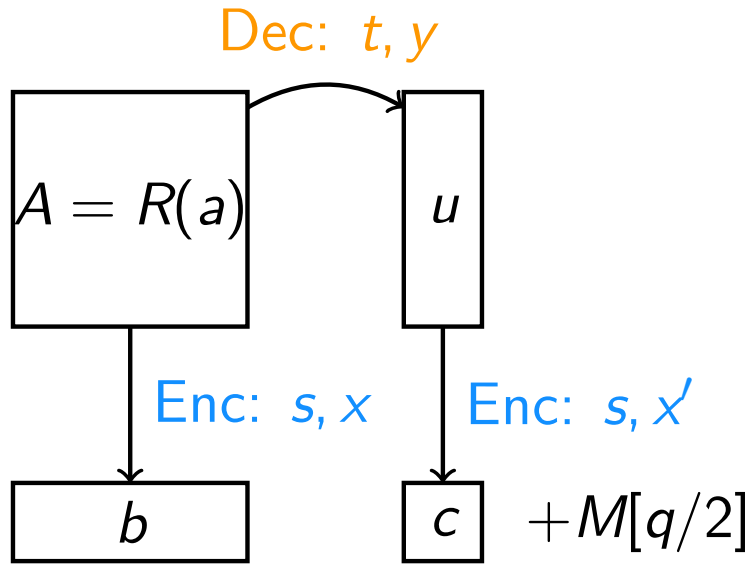


$$ek = (A, \vec{u}), dk = (\vec{t}, \vec{y}), ct = (\vec{b}, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - \vec{b} \cdot \vec{t}^\top &= M[q/2] + \vec{s} \cdot \vec{u}^\top + x - (\vec{s}A + \vec{x}) \cdot \vec{t}^\top \\ &= M[q/2] + \vec{s} \cdot (A \cdot \vec{t}^\top + \vec{y}^\top) + x - (\vec{s}A + \vec{x}) \cdot \vec{t}^\top \\ &= M[q/2] + \vec{s} \cdot \vec{y}^\top + x - \vec{x} \cdot \vec{t}^\top \approx M[q/2]\end{aligned}$$

Lyubashevsky-Peikert-Regev (LPR) PKE

Compress $A \in \mathbb{Z}_q^{n \times n}$ into $a \in \mathbb{Z}_q[X]/(X^n + 1)$ (Let $\vec{s}, \vec{t} \leftarrow \chi^n$)

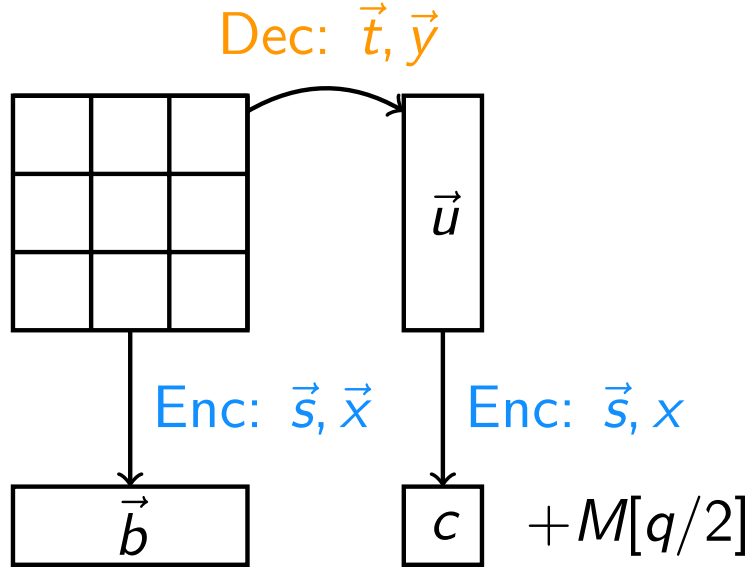


$$ek = (a, u), dk = (t, y), ct = (b, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - bt &= M[q/2] + su + x' - (sa + x)t \\ &= M[q/2] + s(at + y) + x' - (sa + x)t \\ &= M[q/2] + sy + x' - xt \approx M[q/2]\end{aligned}$$

Module-LWE PKE

Compress $A \in \mathbb{Z}_q^{n \times n}$ into $a_{11}, \ldots, a_{33} \in \mathbb{Z}_q[X]/(X^{n/3}+1)$ (Let $\vec{s}, \vec{t} \leftarrow \chi^n$)

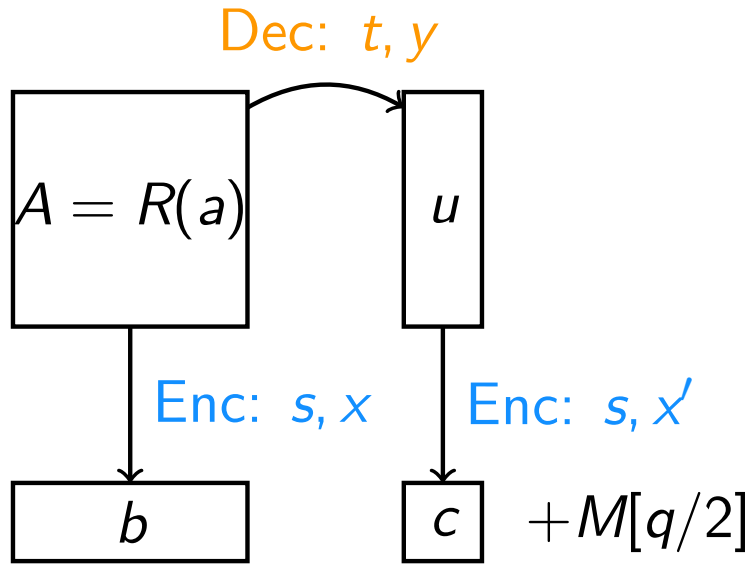


$$ek = (A, \vec{u}), dk = (\vec{t}, \vec{y}), ct = (\vec{b}, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - \vec{b} \cdot \vec{t}^{\top} &= M[q/2] + \vec{s} \cdot \vec{u}^{\top} + x - (\vec{s}A + \vec{x}) \cdot \vec{t}^{\top} \\ &= M[q/2] + \vec{s} \cdot (A \cdot \vec{t}^{\top} + \vec{y}^{\top}) + x - (\vec{s}A + \vec{x}) \cdot \vec{t}^{\top} \\ &= M[q/2] + \vec{s} \cdot \vec{y}^{\top} + x - \vec{x} \cdot \vec{t}^{\top} \approx M[q/2]\end{aligned}$$

Lyubashevsky-Peikert-Regev (LPR) PKE

Compress $A \in \mathbb{Z}_q^{n \times n}$ into $a \in \mathbb{Z}_q[X]/(X^n + 1)$ (Let $\vec{s}, \vec{t} \leftarrow \chi^n$)

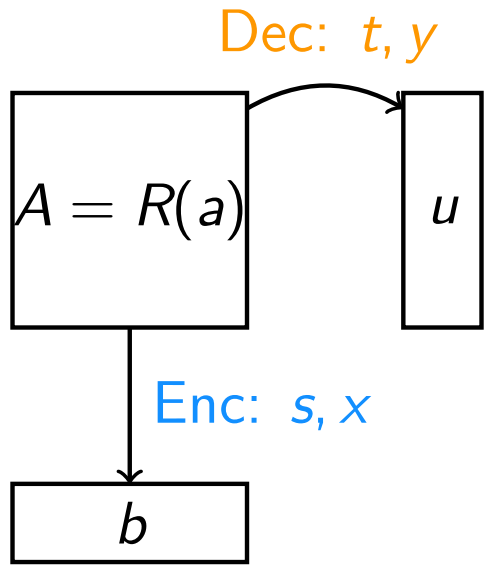


$$ek = (a, u), dk = (t, y), ct = (b, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - bt &= M[q/2] + su + x' - (sa + x)t \\ &= M[q/2] + s(at + y) + x' - (sa + x)t \\ &= M[q/2] + sy + x' - xt \approx M[q/2]\end{aligned}$$

NTRU PKE

Fix $u = 0 \rightarrow a \cdot t + y = 0$



$$ek = a, dk = (t, y), ct = b \text{ or } pb + M$$

$$b = sa + x \Longrightarrow b \cdot t = (sa + x)t = sat + xt = s(-y) + xt \approx 0$$

$$c = pb + M$$

$ct = p(sa + x)t + Mt$ over $\mathbb{Z}$.

NIST PQC Round 1: 格子ベース

暗号 22: Compact LWE, CRYSTALS-Kyber, Ding Key Exchange, EMBLEM and R.EMBLEM, FrodoKEM, Giophantus, Hila5, KCL, KINDI, LAC, Lima, Lizard, LOTUS, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan, Round2, SABER, Titanium

署名 5: CRYSTALS-Dilithium, DRS, Falcon, pqNTRUsign, qTESLA,

現場限り - 1

現場限り - 2

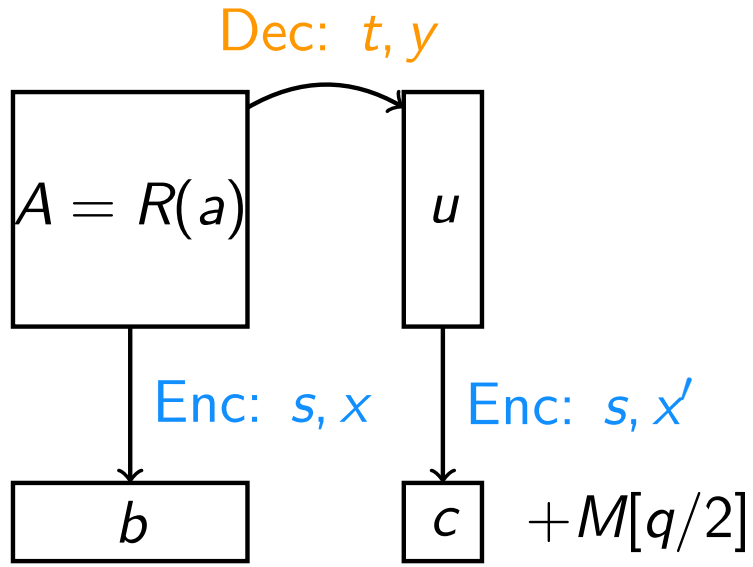
メルセンヌ素数ベース

NIST PQC Round 1: メルセンヌ素数ベース

- Mersenne 2: Mersenne-756839, Ramstake,

Lyubashevsky-Peikert-Regev (LPR) PKE

Compress $A \in \mathbb{Z}_q^{n \times n}$ into $a \in \mathbb{Z}_q[X]/(X^n + 1)$ (Let $\vec{s}, \vec{t} \leftarrow \chi^n$)



$$ek = (a, u), dk = (t, y), ct = (b, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - bt &= M[q/2] + su + x' - (sa + x)t \\ &= M[q/2] + s(at + y) + x' - (sa + x)t \\ &= M[q/2] + sy + x' - xt \approx M[q/2]\end{aligned}$$

アイデア

$x = 2$ を代入:

$$x^n - 1 \to P = 2^n - 1$$

$$a = a_{n-1}x^{n-1} + \cdots + a_0 \to a \in [0, P] \sim \{0,1\}^n$$

$\mathbb{Z}[x]/(x^n - 1)$ の代わりに $\mathbb{Z}/P\mathbb{Z}$ を考える

Theorem

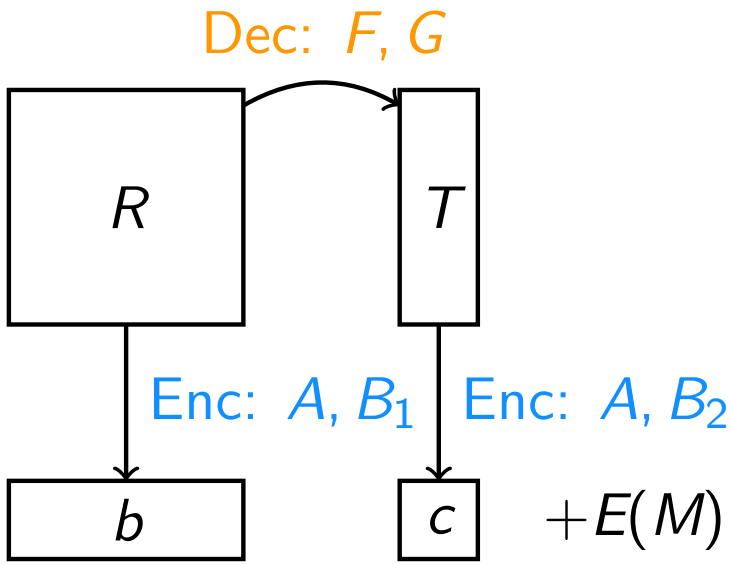
$P = 2^n - 1$ とする. H: ハミング重み

For all $A, B \in \{0,1\}^n$:

- $H(A + B \bmod P) \leq H(A) + H(B)$
- $H(A \cdot B \bmod P) \leq H(A) \cdot H(B)$
- $H(-A \bmod P) = n - H(A)$ *if* $A \neq 0$

Mersenne-based PKE a la LPR

$F, G, A, B_1, B_2 \leftarrow B_{n,h}$.



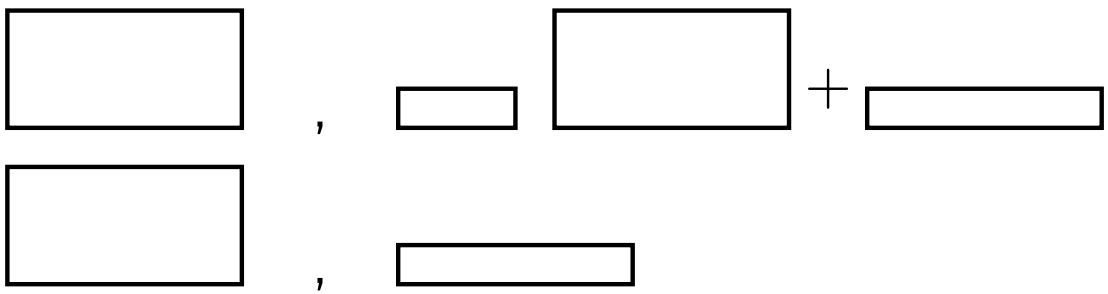
$$ek = (R, T), dk = (F, G), ct = (C_1, C_2 + E(M))$$

$$\begin{aligned}(C_2 + E(M)) - C_1F &= E(M) + (AT + B_2) - (AR + B_1)F \\ &= E(M) + A(RF + G) + B_2 - ARF + B_1F \\ &= E(M) + AG + B_2 - B_1F \approx E(M)\end{aligned}$$

符号ベース

LPN 問題/仮定

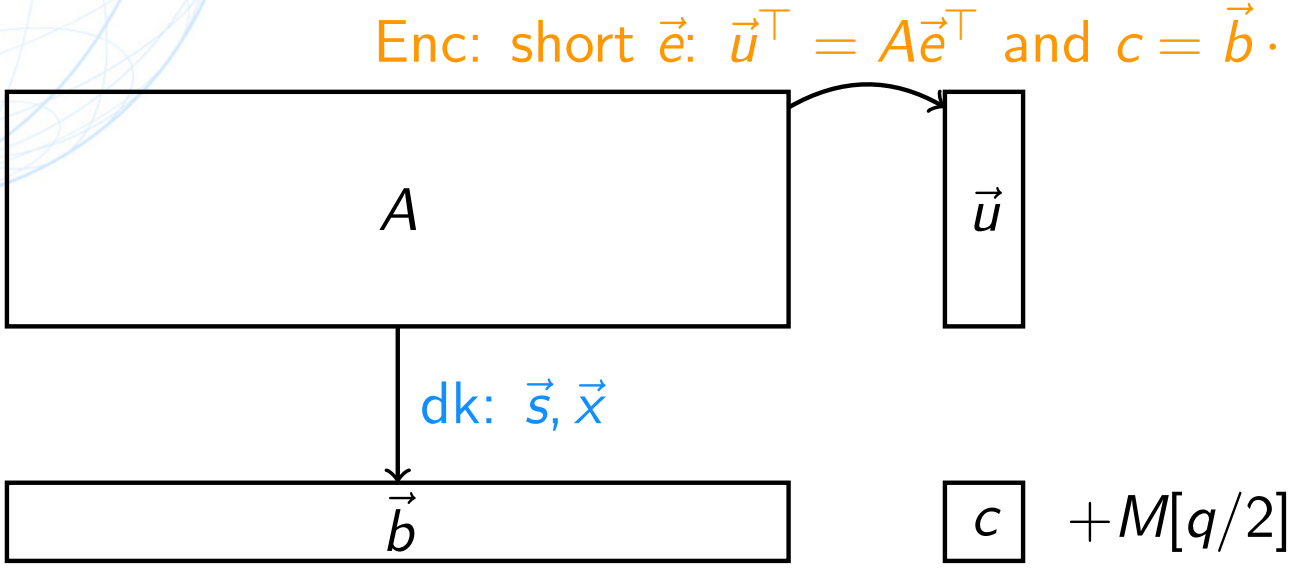
- Learning with Parity Noises (LPN): 以下を識別するのは困難
  - $(A, sA + x)$ $(A \leftarrow F^{n \times m},\ s \leftarrow F^{n},\ x \leftarrow \chi^{m})$
  - (A, b) $(A \leftarrow F^{n \times m},\ b \leftarrow F^{m})$



χ の例: ベルヌーイ分布

$$\Pr[x = 1] = 1/4 \text{ and } \Pr[x = 0] = 3/4$$

Regev PKE

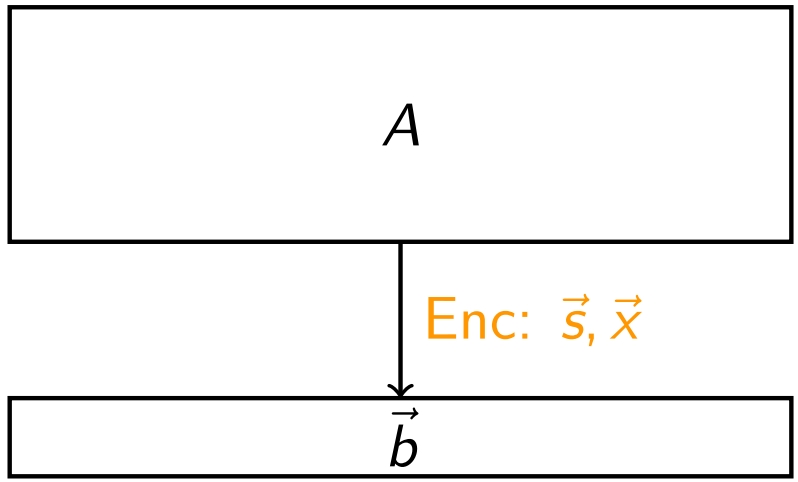


$$ek = (A, \vec{b}), dk = (\vec{s}, \vec{x}), ct = (\vec{u}, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - \vec{s} \cdot \vec{u}^\top &= M[q/2] + \vec{b} \cdot \vec{e}^\top - \vec{s} \cdot A\vec{e}^\top \\ &= M[q/2] + (\vec{s}A + \vec{x}) \cdot \vec{e}^\top - \vec{s} \cdot A\vec{e}^\top \\ &= M[q/2] + \vec{x} \cdot \vec{e}^\top \approx M[q/2]\end{aligned}$$

McEliece PKE [McE78]

$A = SGP$: $S \leftarrow GL_k(F)$, G は $[n, k]$-線型符号の生成行列, $P \leftarrow S_n$.



$$ek = A, dk = (S, G, P), ct = b = sA + x$$

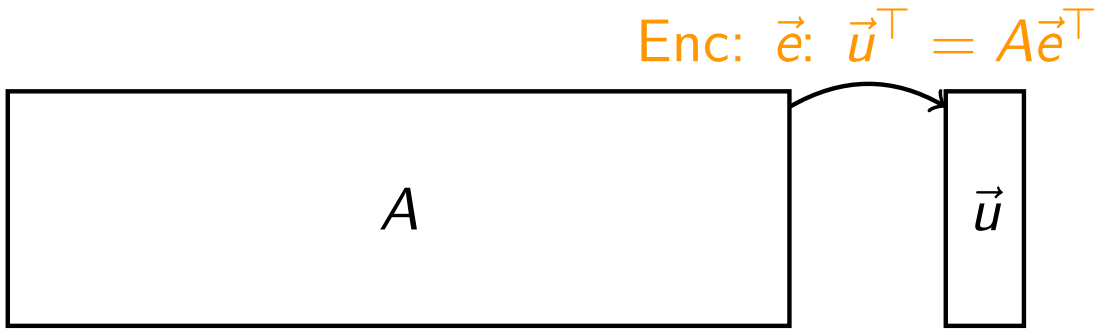
$$\vec{b}P^{-1} = (sA + x)P^{-1} = sSG + xP^{-1}$$

$$\rightarrow sS \text{ because } H(xP^{-1}) = H(x) \leq t$$

$$\rightarrow s$$

Niederreiter 暗号 [Nie86]

$A = SHP$: $S \leftarrow GL_{n-k}(F)$, H は $[n, k]$-線型符号のパリティ検査行列, $P \leftarrow S_n$.



$$ek = A, dk = (S, H, P), ct = u$$

$$S^{-1}u = H \cdot Pe$$

$$\rightarrow Pe \text{ because } H(Pe) = H(e) \leq t$$

$$\rightarrow e$$

NIST PQC Round 1: 符号ベース暗号

暗号 17: BIG QUAKE, BIKE, Classic McEliece, DAGS, Edon-K, HQC, LAKE, LEDAkem, LEDApkc, Lepton, LOCKER, McNie, NTS-KEM, Ouroboros-R, QC-MDPC KEM, RLCE-KEM, RQC,

署名 3: pqsigRM, RaCoSS, RankSign

Round 2

NIST PQC Round 1: 暗号

暗号 49:

- Code 17: BIG QUAKE, BIKE, Classic McEliece, DAGS, ~~Edon-K~~, HQC, LAKE, LEDAkem, LEDApkc, Lepton, LOCKER, McNie, NTS-KEM, Ouroboros-R, QC-MDPC KEM, RLCE-KEM, RQC
- Lattice 22: Compact LWE, CRYSTALS-Kyber, Ding Key Exchange, EMBLEM and R.EMBLEM, FrodoKEM, Giophantus, Hila5, KCL, KINDI, LAC, Lima, Lizard, LOTUS, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan, Round2, SABER, Titanium Three Bears
- MQ 3: CFPKM, DME, ~~SRTPI~~
- Isogeny 1: SIKE
- Mersenne 2: Mersenne-756839, Ramstake,
- Others 4: Post-Quantum RSA-Encryption, ~~RVB~~, GuessAgain, ~~HK17~~

NIST PQC Round 2: 暗号

暗号 49→17:

- Code 17→7: BIKE, Classic McEliece, HQC, LEDAcrypt(=LEDAkem+LEDApkc), NTS-KEM, ROLLO(=LAKE+LOCKER+Ouroboros-R), RQC
- Lattice 22→9: CRYSTALS-Kyber, FrodoKEM, LAC, NewHope, NTRU(=NTRUEncrypt+NTRU-HRSS-KEM), NTRU Prime, Round5(=HILA5+Round2), SABER, Three Bears
- MQ 3→0:
- Isogeny 1→1: SIKE
- Mersenne 2→0:
- Others 4→0:

NIST PQC Round 1: 署名

署名 22:

- Code 3: pqsigRM, RaCoSS, ~~RankSign~~
- Lattice 5: CRYSTALS-Dilithium, DRS, Falcon, pqNTRUsign, qTESLA
- MQ 8: DME, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow
- Hash 2: Gravity-SPHINCS, SPHINCS+
- 共通鍵 1: Picnic,
- その他 2: Post-Quantum RSA-Signature, WalnutDSA

NIST PQC Round 2: 署名

署名 22→9:

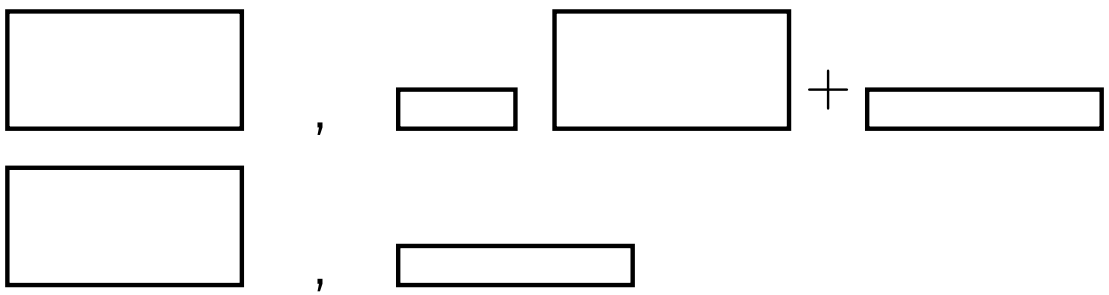
- Code 3→0:
- Lattice 5→3: CRYSTALS-Dilithium, Falcon, qTESLA
- MQ 8→4: GeMSS, LUOV, MQDSS, Rainbow
- Hash 2→1: SPHINCS+
- 共通鍵 1→1: Picnic
- Others 2→0:

休憩

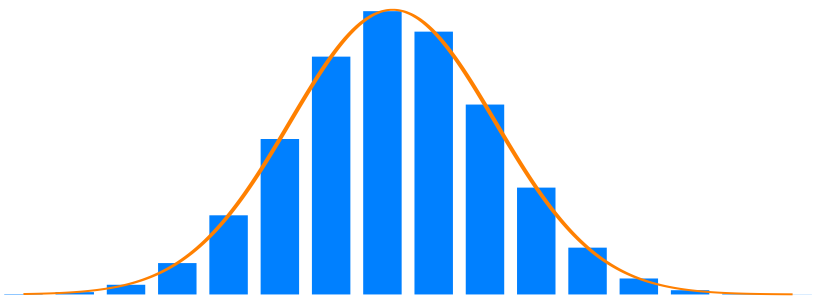
格子ベース

LWE

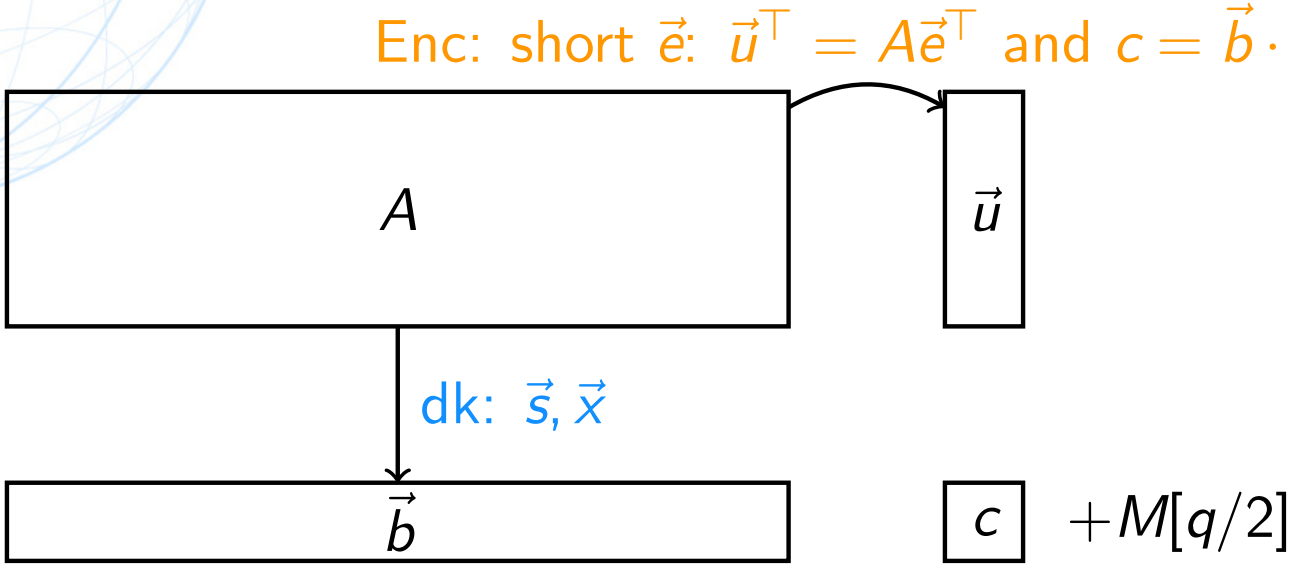
- Learning with Errors (LWE): 以下を識別するのは困難
  - $(A, \vec{s}A + \vec{x})$ $(A \leftarrow \mathbb{Z}_q^{n \times m},\ \vec{s} \leftarrow \mathbb{Z}_q^n,\ \vec{x} \leftarrow \chi^m)$
  - $(A, \vec{b})$ $(A \leftarrow \mathbb{Z}_q^{n \times m},\ \vec{b} \leftarrow \mathbb{Z}_q^m)$



χ の例: 離散ガウス分布



Regev 暗号 [Reg05,Reg09]

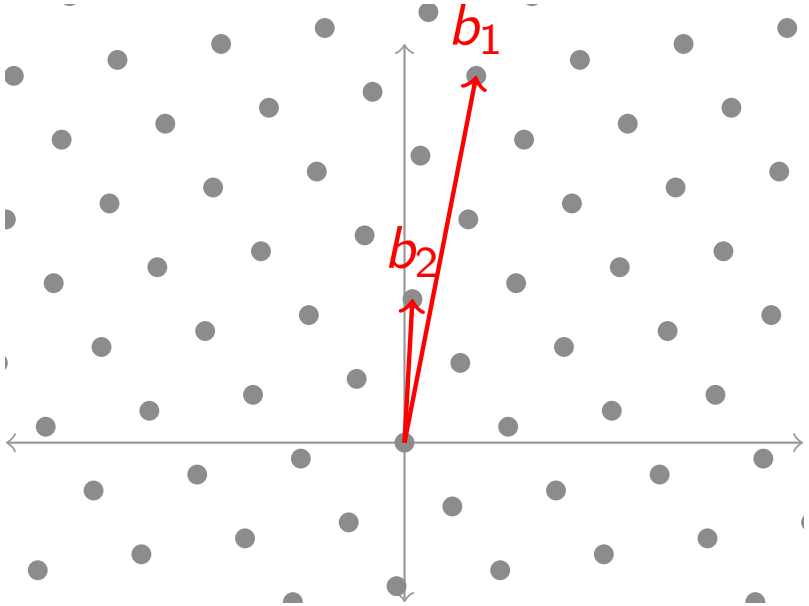


$$ek = (A, \vec{b}), dk = (\vec{s}, \vec{x}), ct = (\vec{u}, c + M[q/2])$$

$$\begin{aligned}(c + M[q/2]) - \vec{s} \cdot \vec{u}^\top &= M[q/2] + \vec{b} \cdot \vec{e}^\top - \vec{s} \cdot A\vec{e}^\top \\ &= M[q/2] + (\vec{s}A + \vec{x}) \cdot \vec{e}^\top - \vec{s} \cdot A\vec{e}^\top \\ &= M[q/2] + \vec{x} \cdot \vec{e}^\top \approx M[q/2]\end{aligned}$$

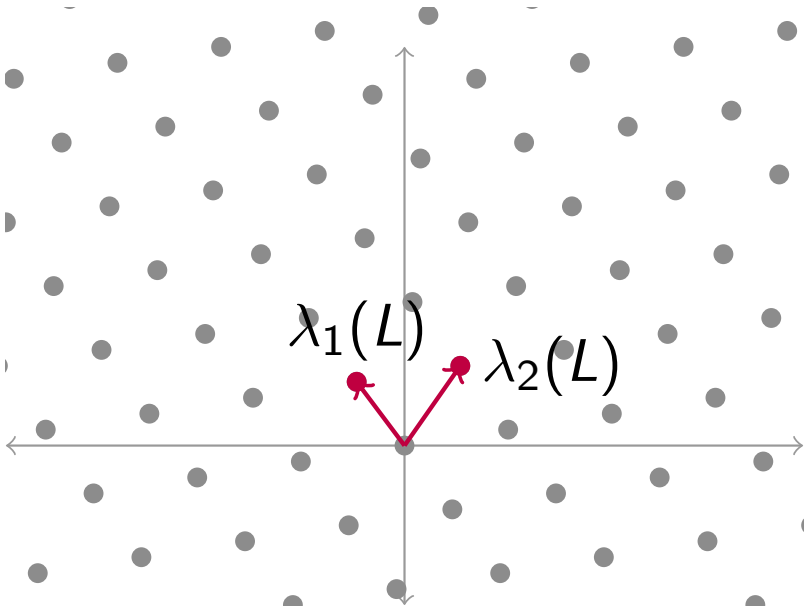
格子

- $B = [b_1, \ldots, b_n] \in \mathbb{Z}^{n \times n}$
- B が張る格子: $L(B) := \{\sum_i \alpha_i b_i \mid \alpha_i \in \mathbb{Z}\}$



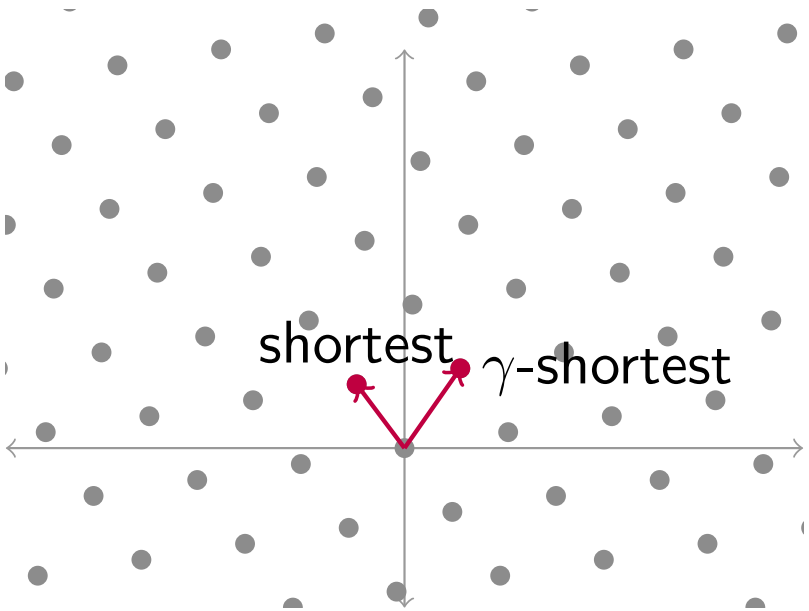
格子定数

- Succive minimum:
  $\lambda_i(L) := \inf\{r : L \cap B(r)$ が i 個の線型独立ベクトルを含む$\}$
- $\lambda_1(L)$: 最短ベクトルの長さ
- $\lambda_n(L)$: 最短独立ベクトル集合中の最長ベクトルの長さ



最短ベクトル問題他

- SVP: 入力 B: 出力非零 $v \in L(B)$ with $\|v\| = \lambda_1(L(B))$
- SVP_γ: 入力 B: 出力非零 $v \in L(B)$ with $\|v\| \leq \gamma\lambda_1(L(B))$
- GapSVP_γ: 入力 B と $d > 0$: 出力 YES if $\|v\| \leq d$, NO if $\|v\| > \gamma d$
- SIVP_γ: 入力 B: 出力独立なベクトル集合 V with $\|V\| \leq \gamma\lambda_n(L(B))$



格子問題と LWE

- (Regev 2005) If n-dim. LWE is quantumly solved, then n-dim GapSVP$_\gamma$ is quantumly solved.

格子問題と LWE

- (Regev 2005) If n-dim. LWE is quantumly solved, then n-dim GapSVP$_\gamma$ is quantumly solved.
- (Peikert 2009) If n-dim. LWE is classically solved, then n-dim GapSVP$_\gamma$ is classically solved (with $q = 2^n$).

格子問題と LWE

- (Regev 2005) If n-dim. LWE is quantumly solved, then n-dim GapSVP$_\gamma$ is quantumly solved.
- (Peikert 2009) If n-dim. LWE is classically solved, then n-dim GapSVP$_\gamma$ is classically solved (with $q = 2^n$).
- (Brakeski et al. 2013) If n-dim. LWE is classically solved, then $\sqrt{n}$-dim GapSVP$_\gamma$ is classically solved.

格子問題と LWE

- (Regev 2005) If n-dim. LWE is quantumly solved, then n-dim GapSVP$_\gamma$ is quantumly solved.
- (Peikert 2009) If n-dim. LWE is classically solved, then n-dim GapSVP$_\gamma$ is classically solved (with $q = 2^n$).
- (Brakeski et al. 2013) If n-dim. LWE is classically solved, then $\sqrt{n}$-dim GapSVP$_\gamma$ is classically solved.
- Eldar and Shor (2016/11/21): The proposal of quantum PT alg. for LWE with thin χ
  arXiv:1611.06999 [quant-ph]

格子問題と LWE

- (Regev 2005) If n-dim. LWE is quantumly solved, then n-dim GapSVP$_\gamma$ is quantumly solved.
- (Peikert 2009) If n-dim. LWE is classically solved, then n-dim GapSVP$_\gamma$ is classically solved (with $q = 2^n$).
- (Brakeski et al. 2013) If n-dim. LWE is classically solved, then $\sqrt{n}$-dim GapSVP$_\gamma$ is classically solved.
- Eldar and Shor (2016/11/21): The proposal of quantum PT alg. for LWE with thin χ
  arXiv:1611.06999 [quant-ph]

$\rightarrow$ (2016/11/24) Withdrawn

LWE の応用

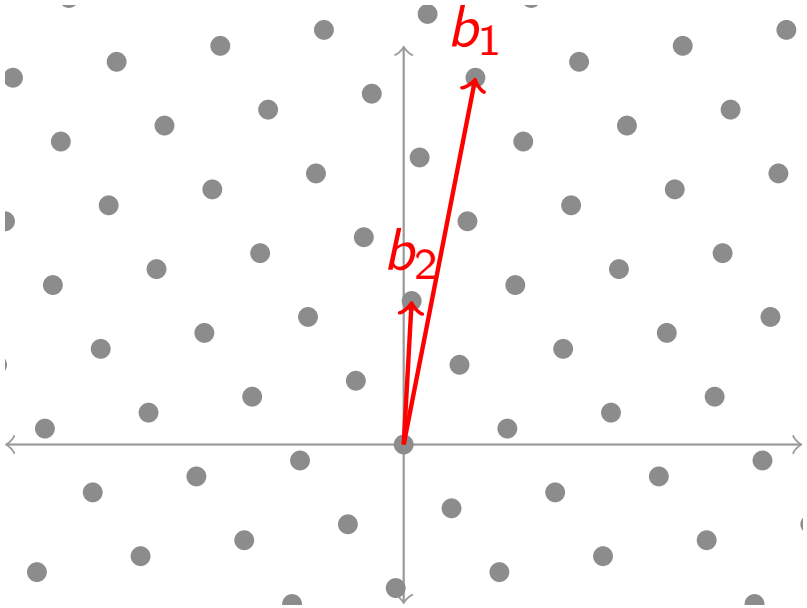
- 公開鍵暗号
- 署名
- 紛失転送
- ID ベース暗号
- 属性ベース暗号
- 一部の難読化 (Lockable Obf. など)
- 不正者追跡 [GoyKopWat18 など]
- 暗号方式の実現可能性の分離 [GoyKopWat17 など]
- 学習の不可能性の証明
- NIZK for NP [PeiShi19]
- 量子計算の古典検証 [Mah18]
- etc...

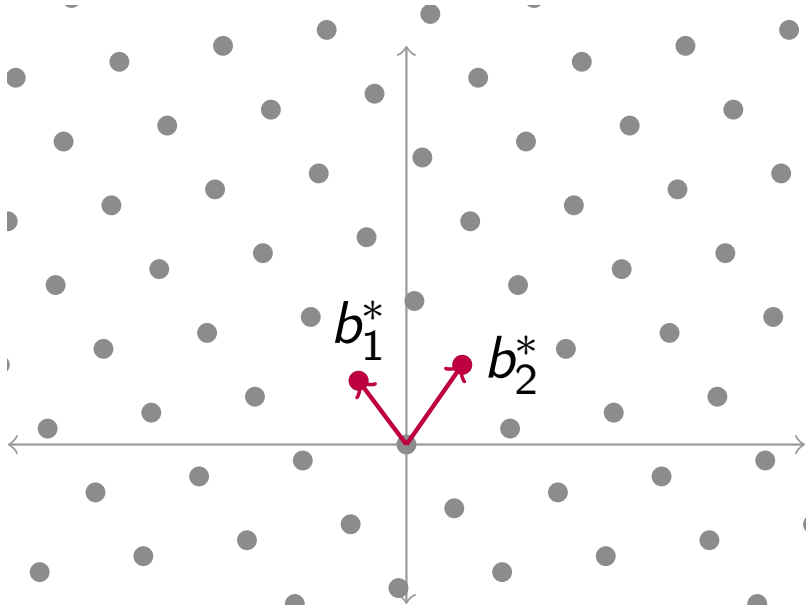
Reg05+PRS17 の解説

準備

格子と双対格子

- $B = [b_1, \ldots, b_n] \in \mathbb{Z}^{n \times n}$
- B が張る格子 $L(B) := \{\sum_i \alpha_i b_i \mid \alpha_i \in \mathbb{Z}\}$
- 双対格子: $L^* := \{y \in \mathbb{Z}^n \mid \forall x \in L, y \cdot x^\top \in \mathbb{Z}\}$
- L^* の基底: $B^* = B^{-\top}$

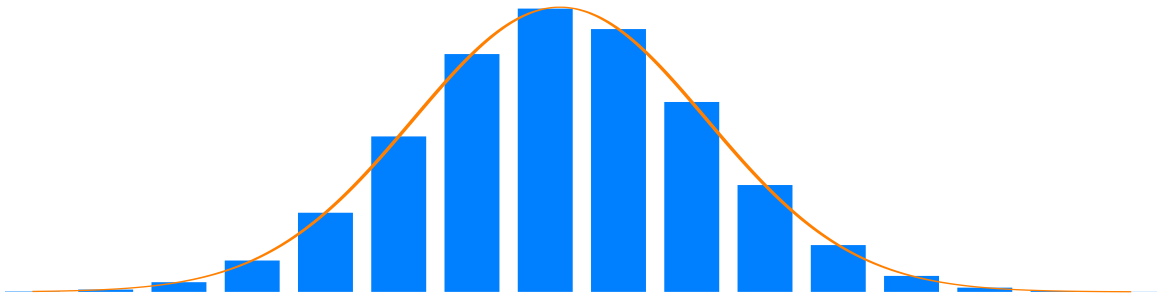




ガウス分布と格子

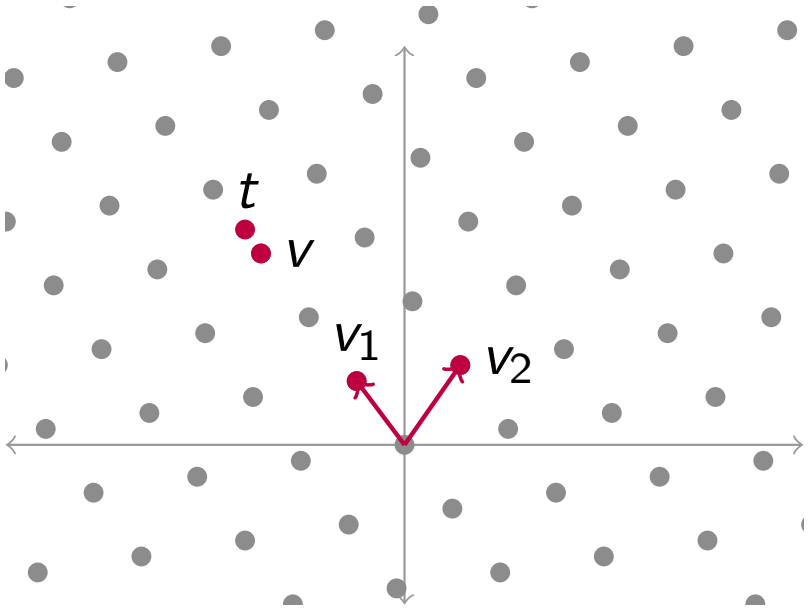
- $\rho_s(x) = \exp(-\pi \|x/s\|^2)$
- $D_{L,s}(x) := \frac{\rho_s(x)}{\sum_{y \in L} \rho_s(y)}$

1 次元格子上のガウス分布



最短ベクトル問題他

- SIVP_γ: 入力 B: 出力独立なベクトル集合 V with $\|V\| \leq \gamma\lambda_n(L(B))$
- DGS_ϕ: 入力 B: 出力 $D_{L(B),\phi}$ からのサンプル
- BDD_δ: 入力 B, t with $d(t, L(B)) \leq \delta$: 出力 $v \in L(B)$ s.t. $\|v - t\| < \delta$



Regev の定理

- $\mathrm{LWE}_{q,\alpha}$: サンプルが

$$(a, \langle a, s \rangle / q + e \bmod 1)$$

で、 $a \leftarrow \mathbb{Z}_q^n$, $e \leftarrow D_\alpha$

Theorem

$\alpha q > 2\sqrt{n}$, $\gamma \geq \sqrt{2n}\lambda_n(L)/\alpha$ とする.
DGS_γ から $LWE_{q,\alpha}$ (の平均時) への多項式時間量子帰着が存在する

- O. Regev (STOC 2005, J. ACM 2009)
- C. Peikert, O. Regev, N. Stephens-Davidowitz (STOC 2017)

以下、黒板

メモ

- Part 1: $D_{L,r}$ サンプラ $+\mathrm{LWE}_{q,\alpha}$ ソルバ $\to \mathrm{BDD}_{L^*,\alpha q/(\sqrt{2}r)}$ ソルバ
  - $(1/\kappa, \kappa)$-OCP (Oracle Comparison Problem) は $\mathrm{poly}(\kappa)$ 時間で解ける
  - $(\exp(-\kappa), \exp(-\kappa))$-OHCP (Oracle Hidden Centre Problem) も $\mathrm{poly}(\kappa, k)$ 時間で解ける
  - オラクル $\mathcal{O}(z, t)$ の構成 (x が hidden center になるように作る)
    1. BDD の問題は $x + v$ と L^*.
    2. $D_{L,\exp(t)r}$ のサンプルと $x - z + v$ を使って LWE 問題を作る
    3. LWE ソルバが YES$\to$1 を出力, NO$\to$0 を出力
- Part 2: $\mathrm{BDD}_{L^*,\alpha q/(\sqrt{2}r)}$ ソルバ $\to D_{L,r\cdot\sqrt{n}/\alpha q}$ サンプラ
  - 最終目標: $\sum_{x\in L} \rho(x) |x\rangle$ を作って測定
  - 出来たこと: R 大で, $\sum_{x\in L, \|x\|\le\sqrt{n}} \rho(x) |x \mod P(RL)\rangle$