

格子問題をベースとした 暗号について

東京工業大学 数理・計算科学専攻
田中研究室 草川恵太

流れ

- 導入
- 基礎
 - ▣ 格子の定義/格子定数
- 格子とハッシュ関数
 - ▣ average-case/worst-case connection
- おわりに
 - ▣ 歴史
 - ▣ 未解決問題

導入

格子問題と暗号

- 数論系以外の候補
- 量子計算機でも難しいとされている
 - 数論系は量子計算機を使うと解ける
- 安全性を最悪時から保証できる
 - average-case/worst-case connection
 - 以下a/wと略す
 - 数論系のa/w
 - cf: DLPのrandom self reducibility (RSR)
 - 群Gを固定するとRSRがある

歴史

- 1800-
 - ▣ Lagrange, Gauss, Hermite, Minkowski,...
- [Lenstra-Lenstra-Lovasz '82]
 - ▣ LLLアルゴリズム (近似度 2^n)
- [Ajtai '96]
 - ▣ a/w 付の一方向性関数族の構成
- [Ajtai-Dwork '97]
 - ▣ a/w 付の公開鍵暗号方式構成
- [Ajtai '98]
 - ▣ l_2 normでのSVPのNP困難性 (ただしランダム帰着)

ジャンル

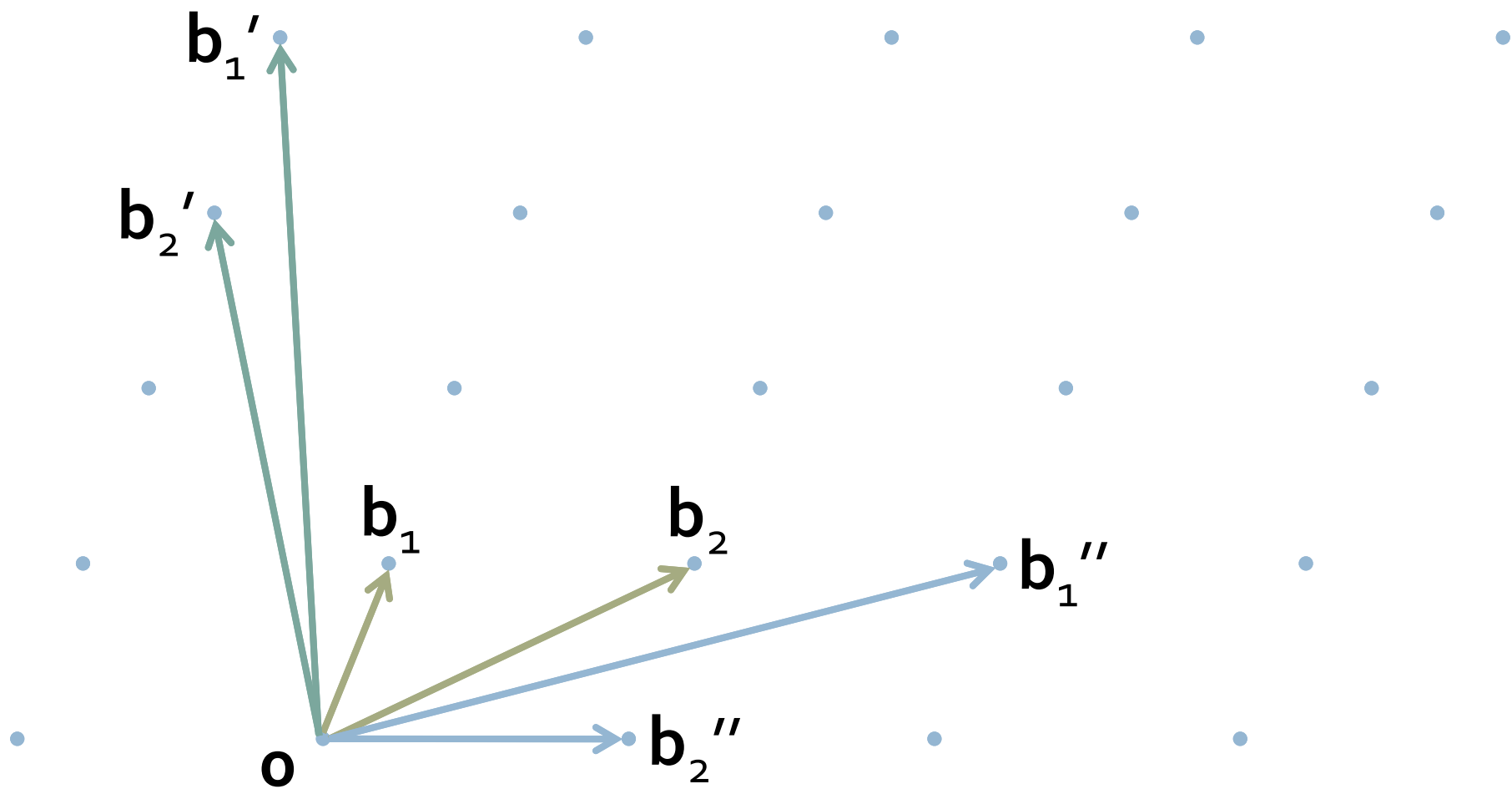
- 基底の縮小とその応用
 - 攻撃に使われることが多い
 - ナップサック暗号, RSA暗号, etc.
- 格子暗号 (a/w無)
 - 公開鍵暗号, 署名
 - GGH, NTRU, etc
- 格子暗号 (a/w付)
 - ハッシュ関数, 公開鍵暗号
 - AD暗号, Regev暗号, etc
- 格子問題の困難性

基礎

格子の定義

- 数学的な定義
 - 格子 $L := \mathbb{R}^m$ 中の離散加群
- 直観的な定義
 - 基底 $B = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ の整数係数線形結合の集合
 - 格子 $L(B) := \{\sum_i \alpha_i \mathbf{b}_i \mid \alpha_i \in \mathbb{Z}, \text{ for all } i\}$
 - 1つの格子に対して様々な基底がある
 - 行列の行の基本変形について不変
- 基本領域
 - $P(B) = \{\sum_i \alpha_i \mathbf{b}_i \mid 0 \leq \alpha_i < 1 \text{ for all } i\}$

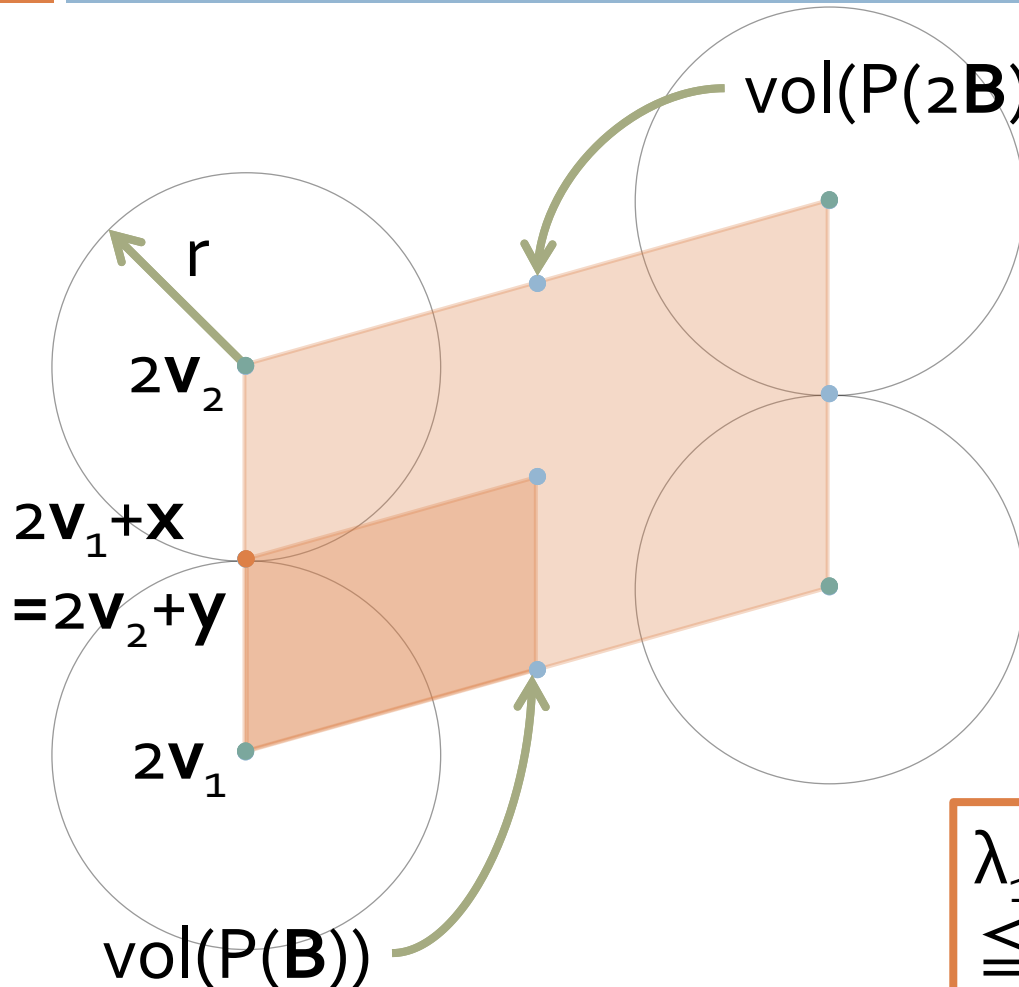
例：格子



格子定数

- $\det(L)$
 - 格子の基本領域の体積
 - \mathbf{B} が格子 L の基底であるとき
$$\det(L) = \text{abs}(\det(\mathbf{B})) = \text{vol}(P(\mathbf{B}))$$
- $\lambda_1(L)$
 - 最短ベクトルの長さ
 - $\lambda_1(L) \leq (n/\pi e)^{1/2} (\det(L))^{1/n}$ [Minkowski]
 - 証明は幾何学的に行う

Minkowski's Lemma



$$\text{vol}(P(2\mathbf{B})) = 2^n \text{vol}(P(\mathbf{B}))$$

球が接したとき

$$\bigcup_{\mathbf{v} \in L(2\mathbf{B})} \mathbf{v} + B(r)$$

$$\subset \bigcup_{\mathbf{v} \in L(2\mathbf{B})} \mathbf{v} + P(2\mathbf{B}) = \mathbb{R}^n$$

$$\text{vol}(B(r)) = r^n \pi^{n/2} \Gamma(n/2 + 1)$$

$$< \text{vol}(P(2\mathbf{B})) = 2^n \det(L(\mathbf{B}))$$

$$(\mathbf{y}-\mathbf{x})/2 = \mathbf{v}_1 - \mathbf{v}_2 \in B(r) \cap L$$

$$\lambda_1(L) \leq \|\mathbf{v}_1 - \mathbf{v}_2\| \leq r$$

$$\leq (2/\sqrt{\pi}) \Gamma(n/2 + 1)^{1/n} \det(L)^{1/n}$$

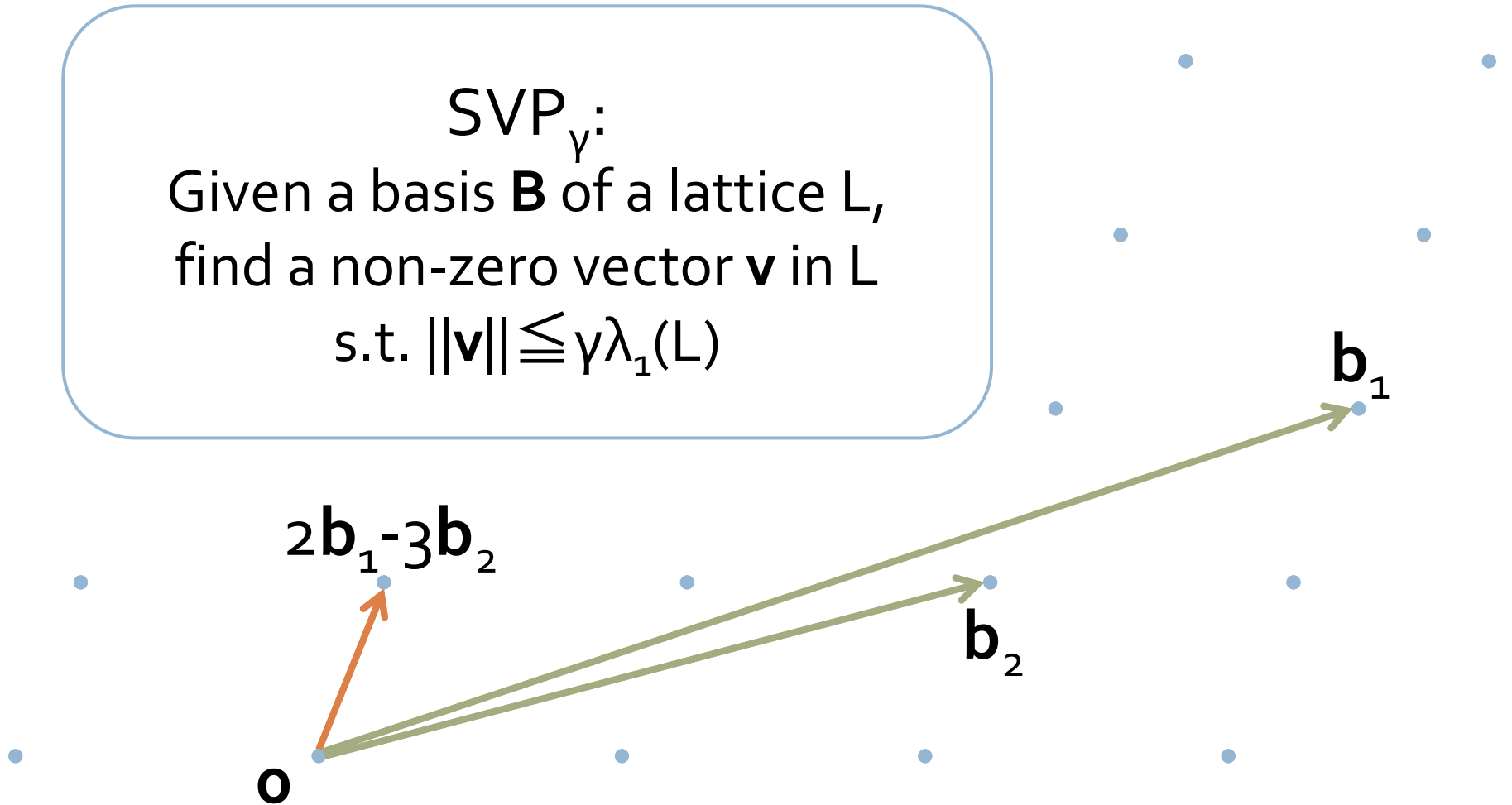
$$= \Theta(\sqrt{n}) (\det(L))^{1/n}$$

SVP (Shortest Vector Problem)

SVP_γ:

Given a basis \mathbf{B} of a lattice L ,
find a non-zero vector \mathbf{v} in L

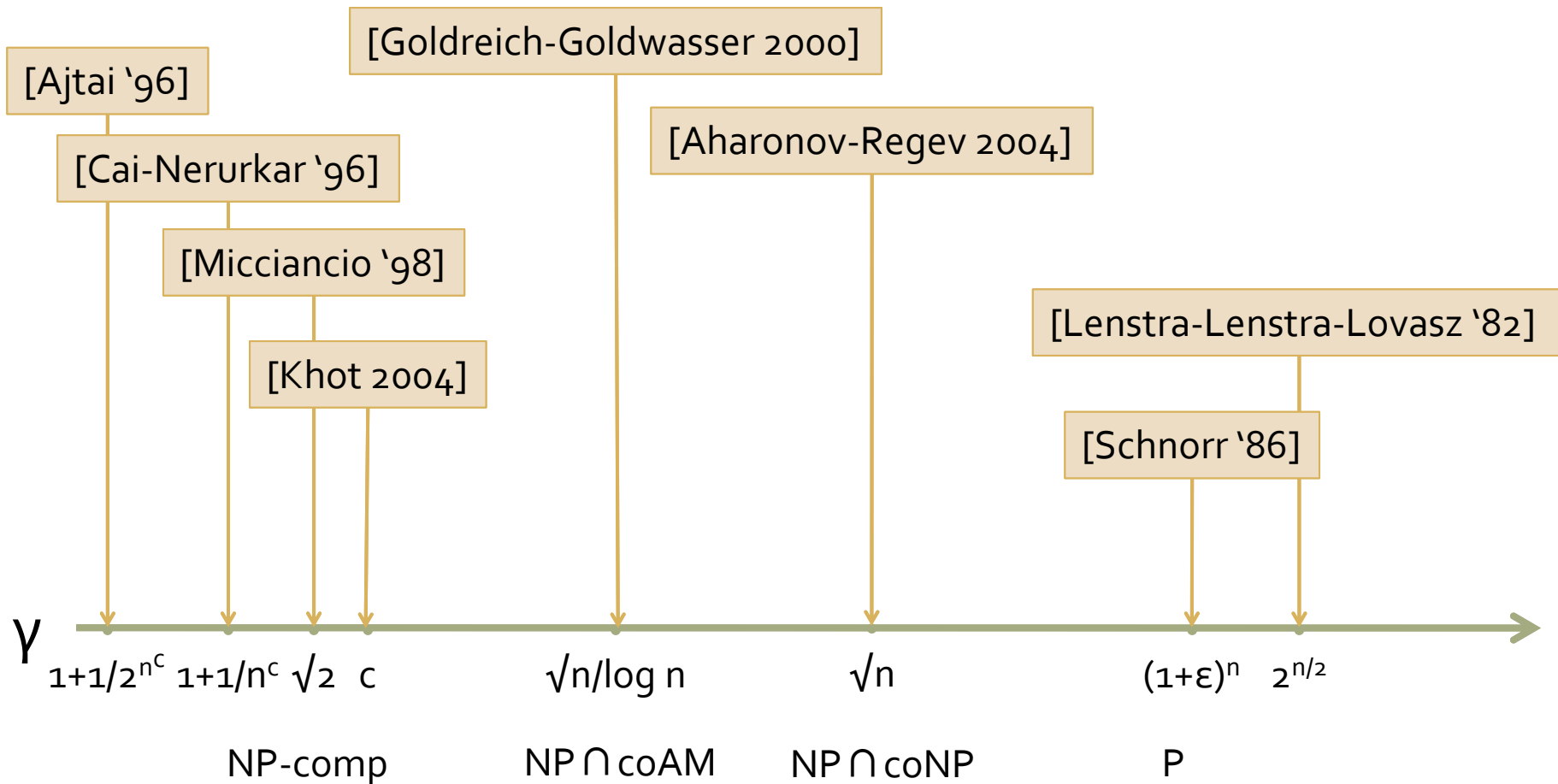
$$\text{s.t. } \|\mathbf{v}\| \leq \gamma \lambda_1(L)$$



GapSVP _{γ}

- SVP _{γ} の決定版
- Input: \mathbf{B} , d
- Output: YES or NO
 - YES: \exists non-zero vector $\mathbf{v} \in L(\mathbf{B})$ s.t. $\|\mathbf{v}\| \leq d$
 - NO: \forall non-zero vector $\mathbf{v} \in L(\mathbf{B})$, $\|\mathbf{v}\| > \gamma d$

GapSVP_γの困難性



その他

□ 双対格子

- $L^* = \{y \in \mathbb{R}^n \mid \text{for all } x \text{ in } L, \langle x, y \rangle \in \mathbb{Z}\}$

- L の基底が $B = [b_1, \dots, b_n]$ のとき L^* の基底は ${}^t(B^{-1})$

- $\text{del}(L^*) = 1/\text{det}(L)$

□ 線形空間

- $\text{lsp}(b_1, \dots, b_n) = \{\sum_i \alpha_i b_i \mid \alpha_i \in \mathbb{R} \text{ for all } i\}$

格子とハッシュ関数

格子とハッシュ関数

□ General

- [Ajtai '96] (OWFs)
- [GGH '96] (CRHFs)
- [Cai-Nerurker '97] (CRHFs)
- [Micciancio 2002] (CRHFs)
- [Micciancio-Regev 2004] (CRHFs)

□ Cyclic or Ideal Lattice

- [Micciancio 2002] (OWFs)
- [Lybashevsky-Micciancio 2006] (CRHFs)
- [Peikert-Rosen 2006] (CRHFs)

ハッシュ関数

- $H(q, m) = \{h_A: \{0, 1\}^m \rightarrow \mathbb{Z}_q^n \mid \mathbf{A} \in \mathbb{Z}_q^{n \times m}\}$
 - $h_A(\mathbf{x}) = \mathbf{Ax} \bmod q, m > n \log q$
 - $\mathbf{A} = [\mathbf{a}_1, \dots, \mathbf{a}_m]$ と書くと
 - $h_A(\mathbf{x}) = \sum x_i \mathbf{a}_i \bmod q$
 - 計算コスト: \mathbb{Z}_q 上での足し算を nm 回
- cf: $\Lambda(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{Ax} = \mathbf{0} \bmod q\}$
 - 離散かつ加群 $\rightarrow \Lambda(\mathbf{A})$ は格子

ハッシュ関数族と衝突

- 敵 \mathcal{F} は $H(q, m)$ の衝突耐性を破る
 - $\Pr[\mathbf{A} \leftarrow_{\mathbb{R}} \mathbb{Z}_q^{n \times m}; (\mathbf{x}, \mathbf{x}') \leftarrow \mathcal{F}(1^n, \mathbf{A}): \text{Col}(\mathbf{x}, \mathbf{x}') = \text{yes}] \geq n^{-c}$
- 敵 \mathcal{F} は $(\mathbf{x}, \mathbf{x}')$ を出力する ($\mathbf{Ax} = \mathbf{Ax}' \pmod{q}$)
 - $\mathbf{x} - \mathbf{x}' \in \{-1, 0, 1\}^m - \mathbf{0}$ の長さは \sqrt{m} 以下
 - $\Lambda(\mathbf{A})$ の長さ \sqrt{m} 以下のベクトルを出力できる
- 目標: 格子問題の最悪時を解く敵の構成
 - どんな格子問題?

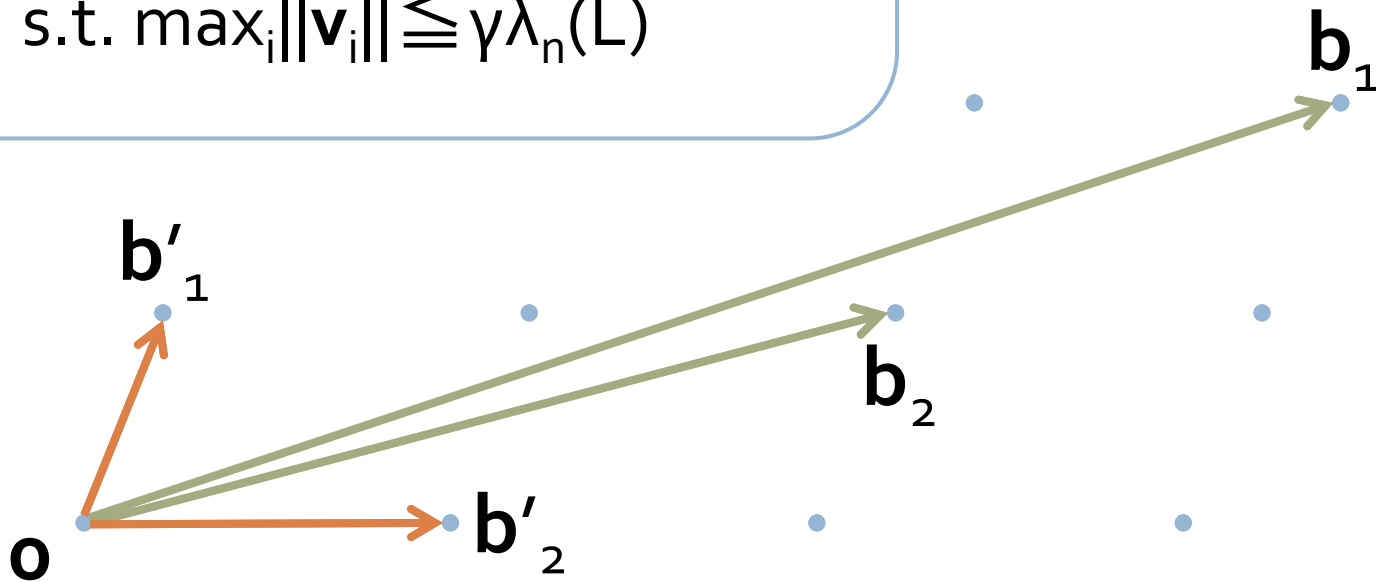
格子定数

- 格子定数: $\lambda_n(L)$
 - $\lambda_1(L)$ の拡張
 - $\lambda_n(L) = \min_{\{v_1, \dots, v_n \in L, \text{線形独立}\}} \max_i \|v_i\|$
- $\lambda_i(L)$: successive minima [Minkowski]
 - $\lambda_i(L) = \min\{r : \dim(\text{Lsp}(L \cap B(r))) \geq i\}$

SIVP (Shortest Independent Vectors Problem)

SIVP $_{\gamma}$:

Given a basis \mathbf{B} of a lattice L ,
find independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$
s.t. $\max_i \|\mathbf{v}_i\| \leq \gamma \lambda_n(L)$



Incremental SIVP (IncSIVP_γ)

- IncSIVP_γ
 - 入力: 基底 \mathbf{B} , 独立なベクトルの組 $\mathbf{S}=(s_1, \dots, s_n) \subset L(\mathbf{B})$
 - $\|\mathbf{S}\| > \gamma \lambda_n(L(\mathbf{B}))$
 - 出力: $\mathbf{S}' \subset L(\mathbf{B})$
 - $\|\mathbf{S}'\| \leq \|\mathbf{S}\|/2$
 - $\mathbf{S}'=(s'_1, \dots, s'_n)$ は独立

- IncSIVP_γ が解ける \rightarrow SIVP_γ が解ける
- 敵 \mathcal{F} を使って IncSIVP_γ を解く



[Ajtai '96]

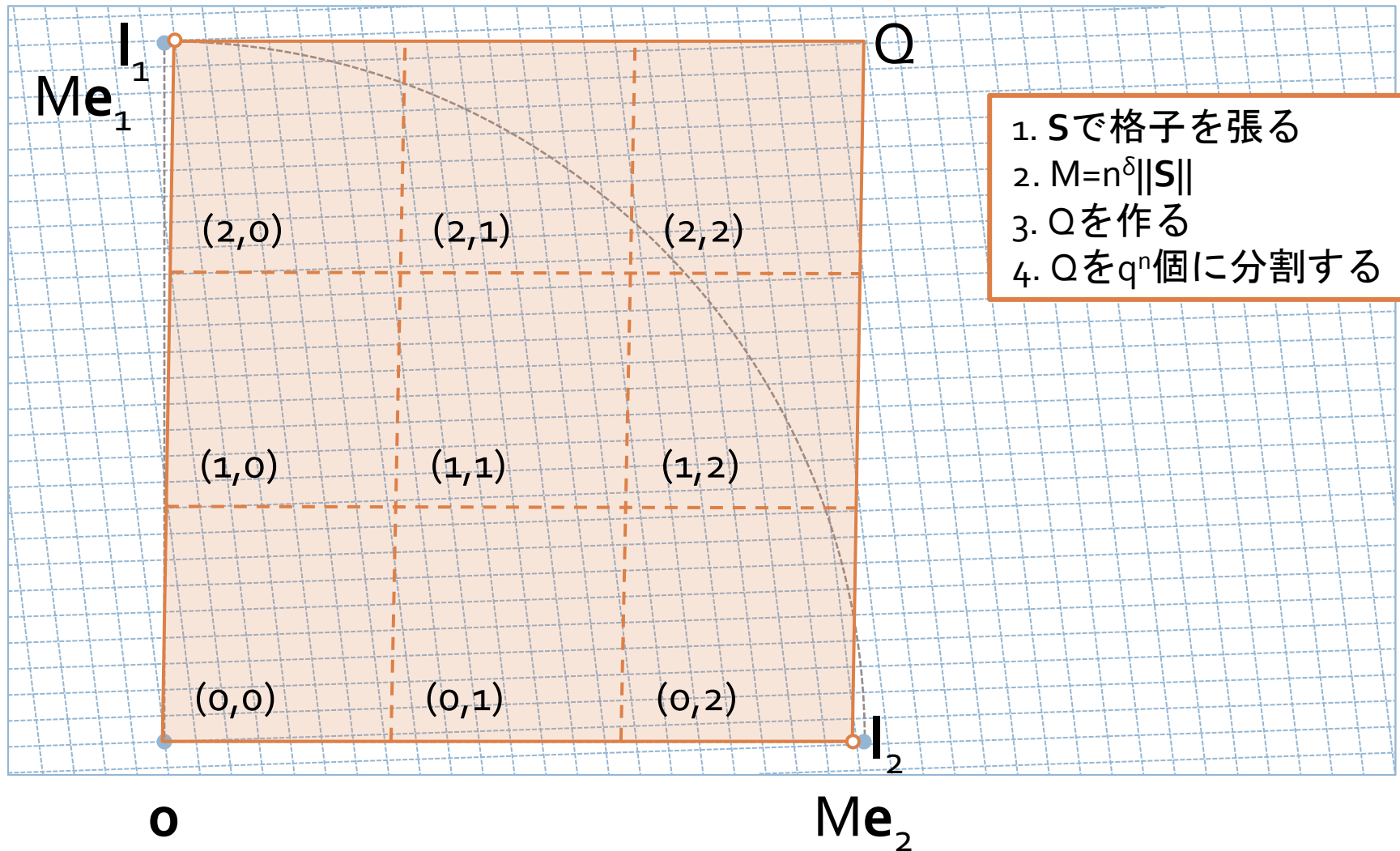
[Ajtai '96]の構成法

- 方針: 敵 \mathcal{F} を使って IncSIVP_γ を解く
- 敵 \mathcal{F} を使うには?
 - 基底 \mathbf{B} とベクトルの組 \mathbf{S} を使って,
 $\mathbf{A} = [\mathbf{a}_1, \dots, \mathbf{a}_m] \in \mathbb{Z}_q^{n \times m}$ を構成する
 - 敵 \mathcal{F} は $\mathbf{A}\mathbf{z} = \mathbf{0} \pmod{q}$ となる $\mathbf{z} \in \{-1, 0, 1\}^m - \{\mathbf{0}\}$ を出力
 - $\mathbf{B}, \mathbf{S}, \mathbf{A}, \mathbf{z}$ から $\|\mathbf{s}\| \leq \|\mathbf{S}\|/2$ となる $\mathbf{s} \in L(\mathbf{B})$ を計算する
 - n 回繰り返して $\mathbf{S}' = (\mathbf{s}'_1, \dots, \mathbf{s}'_n)$ を得る
 - 各 \mathbf{s}'_i はそれなりの確率で線形独立であることはテクニカルなので略

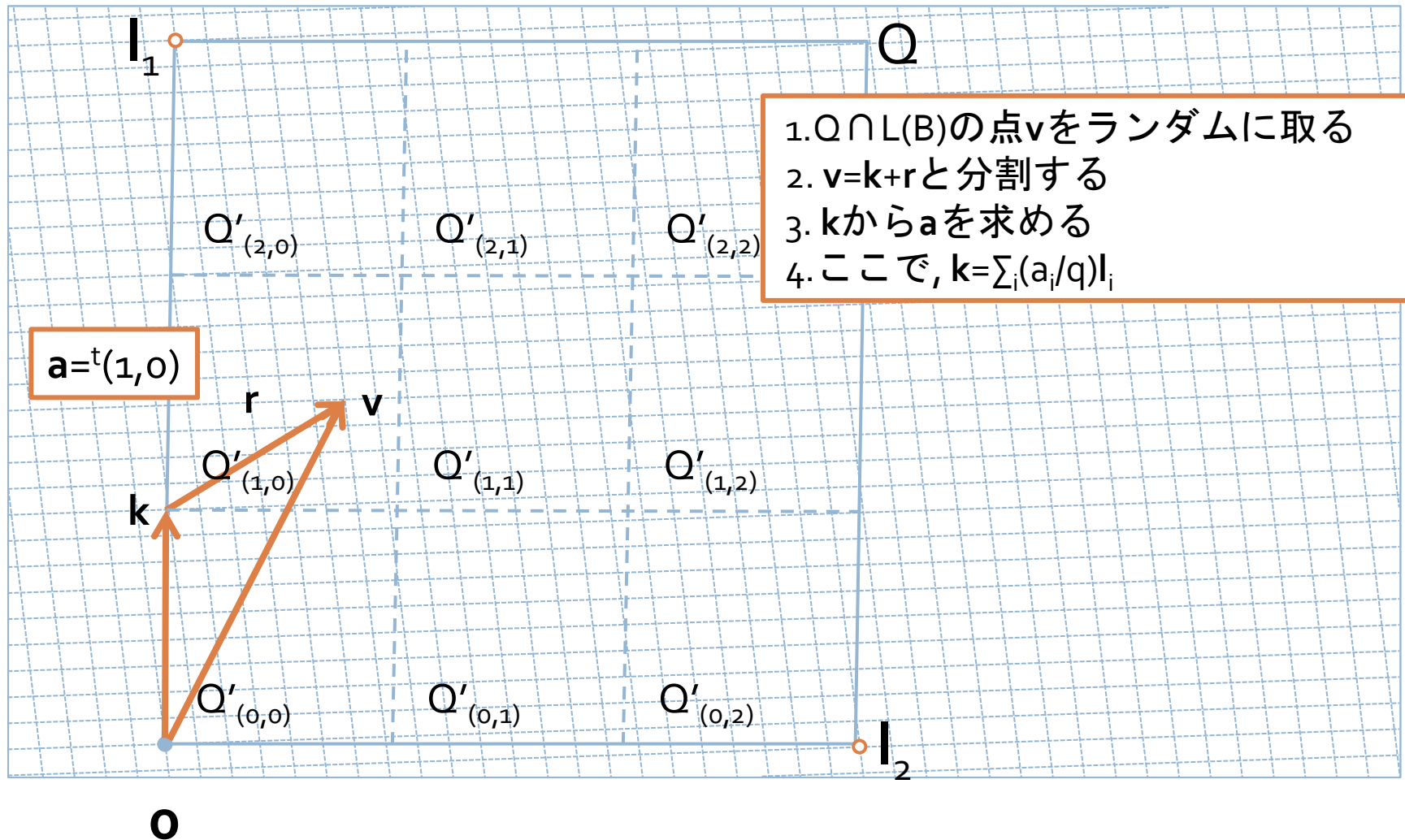
Sampling Algorithm S

- Pseudo-Cube Q の構成
- Pseudo-Cube Q の分割
- サンプリング
 - Q 中の格子の点 v_i をサンプリング
 - 分割に基づいて a_i を出力

Sampling Algorithm S



Sampling Algorithm S



Sampling Algorithm S

- Pseudo-Cube Q の構成
 - $Q = \{\sum_i x_i l_i \mid 0 \leq x_i < 1\}$ (l_i は $M e_i$ に近い)
- Pseudo-Cubeの分割
 - Q を q^n 個の Q' に分割
- サンプリング
 - $Q \cap L(B)$ の点 v をサンプリング
 - $v = k + r$ とする (k は Q'_a の開始点, $r \in Q'_a$)
 - a を出力
- ポイント
 - 各 Q' に入っている格子点の数は大体同じ
 - $k = \sum_i (a_i/q) l_i$
 - r は短い $\|r\| = (1/q) \max_i \|l_i\| = O((1/q) M \sqrt{n})$

IncSIVP $_{\gamma}$ を解く

- S を m 回使って, $\mathbf{A}=[\mathbf{a}_1, \dots, \mathbf{a}_m]$ を得る
 - $\mathbf{v}_i = \mathbf{k}_i + \mathbf{r}_i$, $\mathbf{k}_i = \sum_j (a_{(i,j)}/q) \mathbf{l}_j$
- $(\mathbf{x}, \mathbf{x}') = \mathcal{F}(\mathbf{1}^n, \mathbf{A})$ とし, $\mathbf{z} = \mathbf{x} - \mathbf{x}'$ とする
 - $\mathbf{A}\mathbf{z} = \mathbf{0} \pmod{q}$
- $\mathbf{s} = \sum_i z_i \mathbf{r}_i$

IncSIVP $_{\gamma}$

Input: \mathbf{B}, \mathbf{S} (s.t. $\|\mathbf{S}\| \geq \gamma \lambda_n(L(\mathbf{B}))$)

Output: $\mathbf{s} \in L(\mathbf{B})$ s.t. $\|\mathbf{s}\| \leq \|\mathbf{S}\|/2$

IncSIVP_γ を解く ($s \in L(\mathbf{B})$)

□ $s \in L(\mathbf{B})$?

□ $s = \sum_i z_i \mathbf{r}_i = \sum_i z_i \mathbf{v}_i - \sum_i z_i \mathbf{k}_i$
□ cf: $\mathbf{v}_i = \mathbf{k}_i + \mathbf{r}_i$, $\mathbf{k}_i = \sum_j (a_{(i,j)}/q) \mathbf{l}_j$

□ $\sum_i z_i \mathbf{v}_i, \sum_i z_i \mathbf{k}_i \in L(\mathbf{B})$

□ $\mathbf{v}_i \in L(\mathbf{B})$

□ $\mathbf{A}z = \mathbf{0} \pmod{q}$ より $\sum_i z_i \mathbf{a}_i = \mathbf{0} \pmod{q}$

□ よって $\sum_i z_i \mathbf{k}_i \in L(\mathbf{B})$

補足: $\sum_i z_i \mathbf{k}_i \in L(\mathbf{B})$ について

■ $\mathbf{l}_i \in L(\mathbf{S}) \subseteq L(\mathbf{B})$

■ for all j , $\sum_i z_i a_{(i,j)} = 0 \pmod{q}$
→ for all j , $\sum_i z_i a_{(i,j)}/q \in \mathbb{Z}$

■ $\sum_i z_i \mathbf{k}_i = \sum_i z_i (\sum_j (a_{(i,j)}/q) \mathbf{l}_j)$
→ $= \sum_j (\sum_i z_i a_{(i,j)}/q) \mathbf{l}_j \in L(\mathbf{B})$

IncSIVP_γ

Input: \mathbf{B}, \mathbf{S} (s.t. $\|\mathbf{S}\| \geq \gamma \lambda_n(L(\mathbf{B}))$)

Output: $s \in L(\mathbf{B})$ s.t. $\|s\| \leq \|\mathbf{S}\|/2$

IncSIVP $_{\gamma}$ を解く ($\|s\|$ の不等式)

□ $\|s\| \leq \|S\|/2?$

補足:

■ $M = n^{\delta} \|S\|$

■ $r_i \in Q'$ で Q' の一辺は $O(M/q)$

□ $s = \sum_i z_i r_i = \sum_i z_i v_i - \sum_i z_i k_i$

■ cf: $v_i = k_i + r_i$, $k_i = \sum_j (a_{(i,j)}/q) l_j$

□ $z_i \in \{-1, 0, 1\}$ と $\|r_i\| = O((1/q)M\sqrt{n})$ より

$\|s\| \leq m O((1/q) n^{\delta+0.5} \|S\|)$

□ よって, $mn^{\delta+0.5}/q = 1/2$ と調整すれば解ける

IncSIVP $_{\gamma}$

Input: B, S (s.t. $\|S\| \geq \gamma \lambda_n(L(B))$)

Output: $s \in L(B)$ s.t. $\|s\| \leq \|S\|/2$

近似度/問題点

- 近似度をよくしたい
 - δ が近似度に効いてくる
 - M を小さくする必要がある ($M=n^\delta \|S\|$)
- r_i を短くしたい
 - Q' を小さくしたい
 - M を小さくする必要がある
- a_i が(ほぼ)一様分布であるためには
 - 各 Q' に含まれる格子点の数が同じ
 - M を大きくする必要がある

休

醜



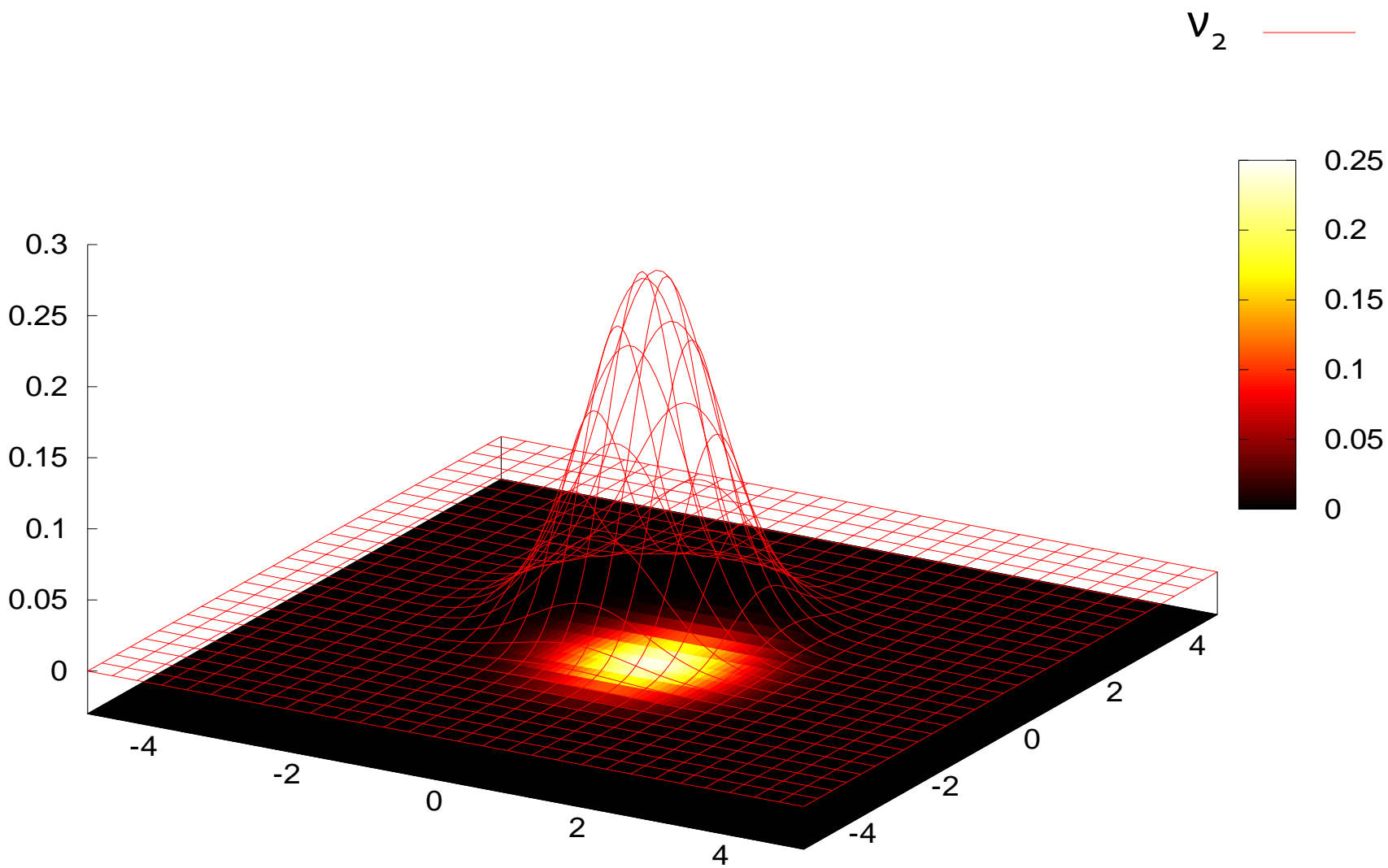
[Micciancio-Regev 2004]

格子とハッシュ関数 - MR04

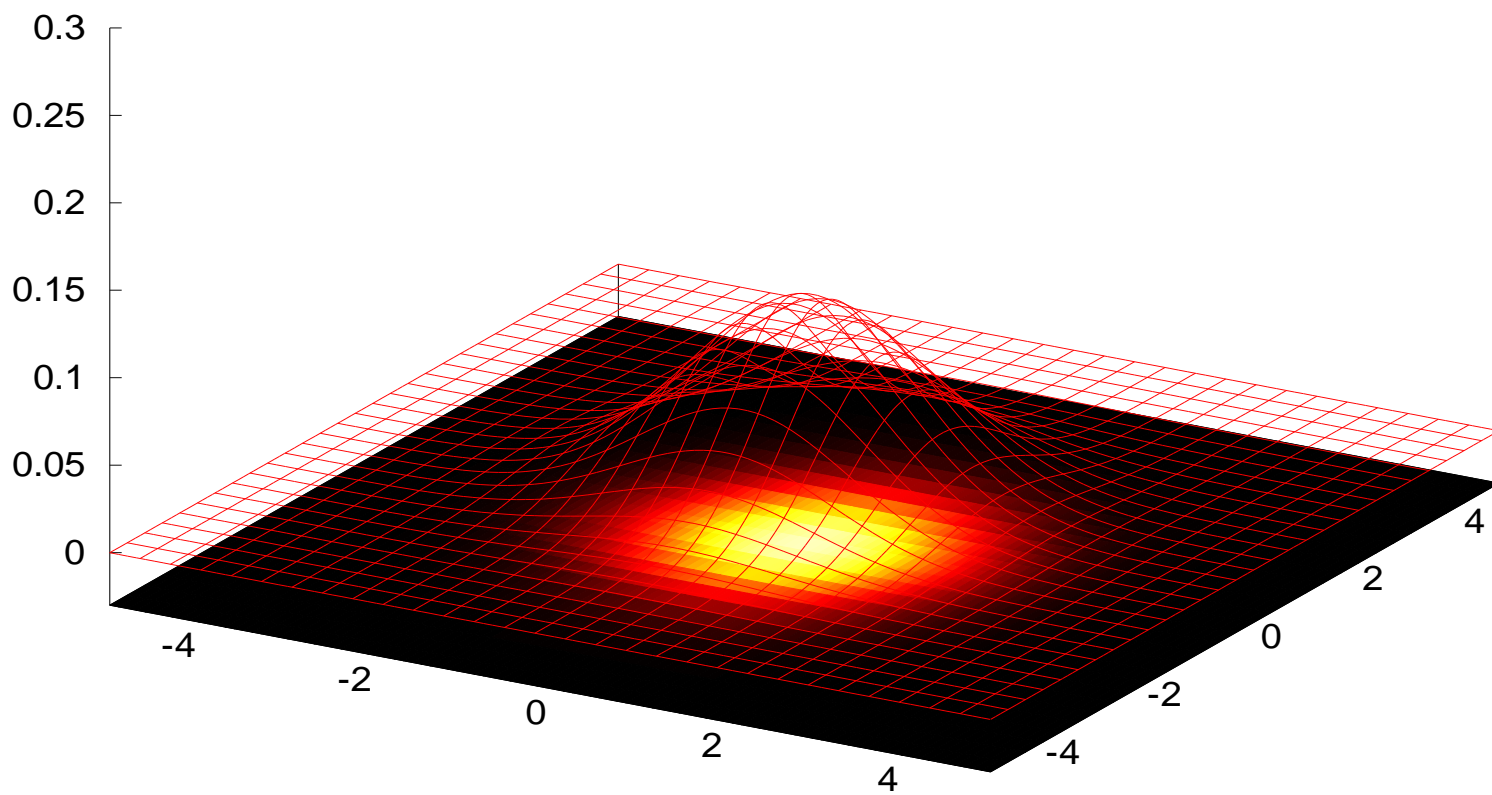
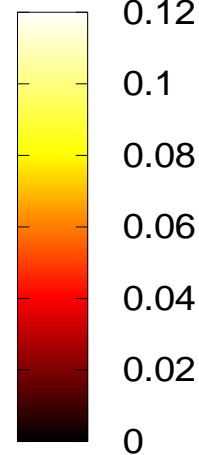
- [Micciancio-Regev 2004]
 - [Ajtai '96, GGH '96, Cai-Nerurkar '97, Micciancio 2002]と構成は似ている
 - 今までの問題点
 - v を Q 上一様分布にするためには, M を大きく
 - Q の一辺のサイズ M が近似度に影響
 - 改良
 - IncSIVPではなくIncGDDに
 - Q の作り方とSampling Algorithm S の構造を変更
 - n 次元ガウス分布とフーリエ解析を使って証明
 - 近似度が $O^{-(n)}$ のSIVPベース

ガウス分布

- $\rho_{s,c}(\mathbf{x}) = \exp(-\pi \|(\mathbf{x}-\mathbf{c})/s\|^2)$
 - $\int_{\mathbf{x} \in \mathbb{R}^n} \rho_{s,c}(\mathbf{x}) d\mathbf{x} = s^n$
- $v_{s,c}(\mathbf{x}) = \rho_{s,c}(\mathbf{x})/s^n$
 - $\int_{\mathbf{x} \in \mathbb{R}^n} v_{s,c}(\mathbf{x}) d\mathbf{x} = 1$
- $\forall \mathbf{x} \in L, D_{L,s,c}(\mathbf{x}) = v_{s,c}(\mathbf{x})/v_{s,c}(L) = \rho_{s,c}(\mathbf{x})/\rho_{s,c}(L)$
 - 格子上に離散化したn次元ガウス分布
- 性質
 - $\rho_s \xrightarrow{FT} s^n \rho_{1/s}$
 - $\rho_{s,c}(L) \leq \rho_s(L)$
 - $\rho(L-B(c\sqrt{n})) < 2^{-n} \rho(L)$
- もともと[Banaszyck '93]で使われていた



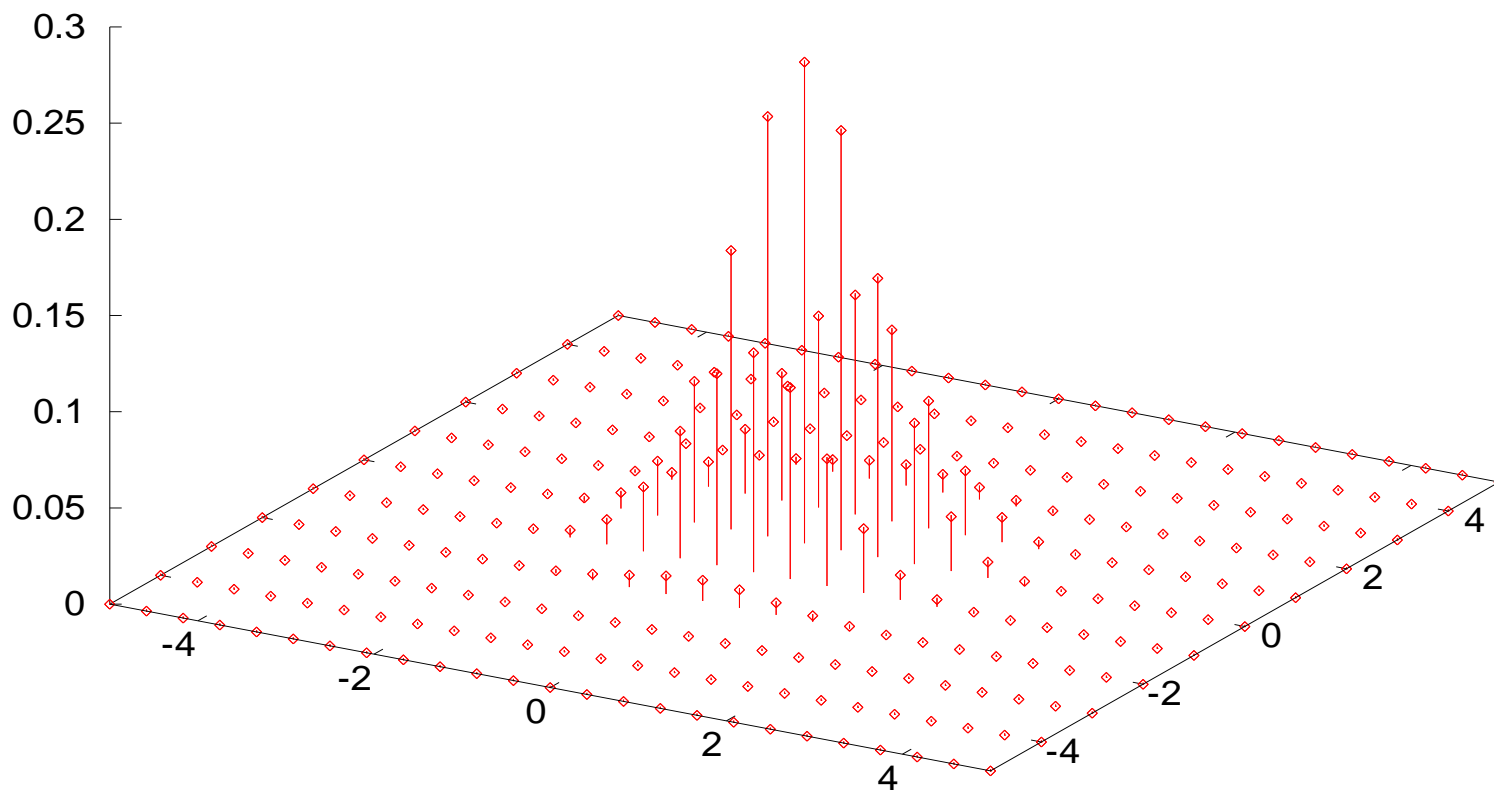
v_3 ———




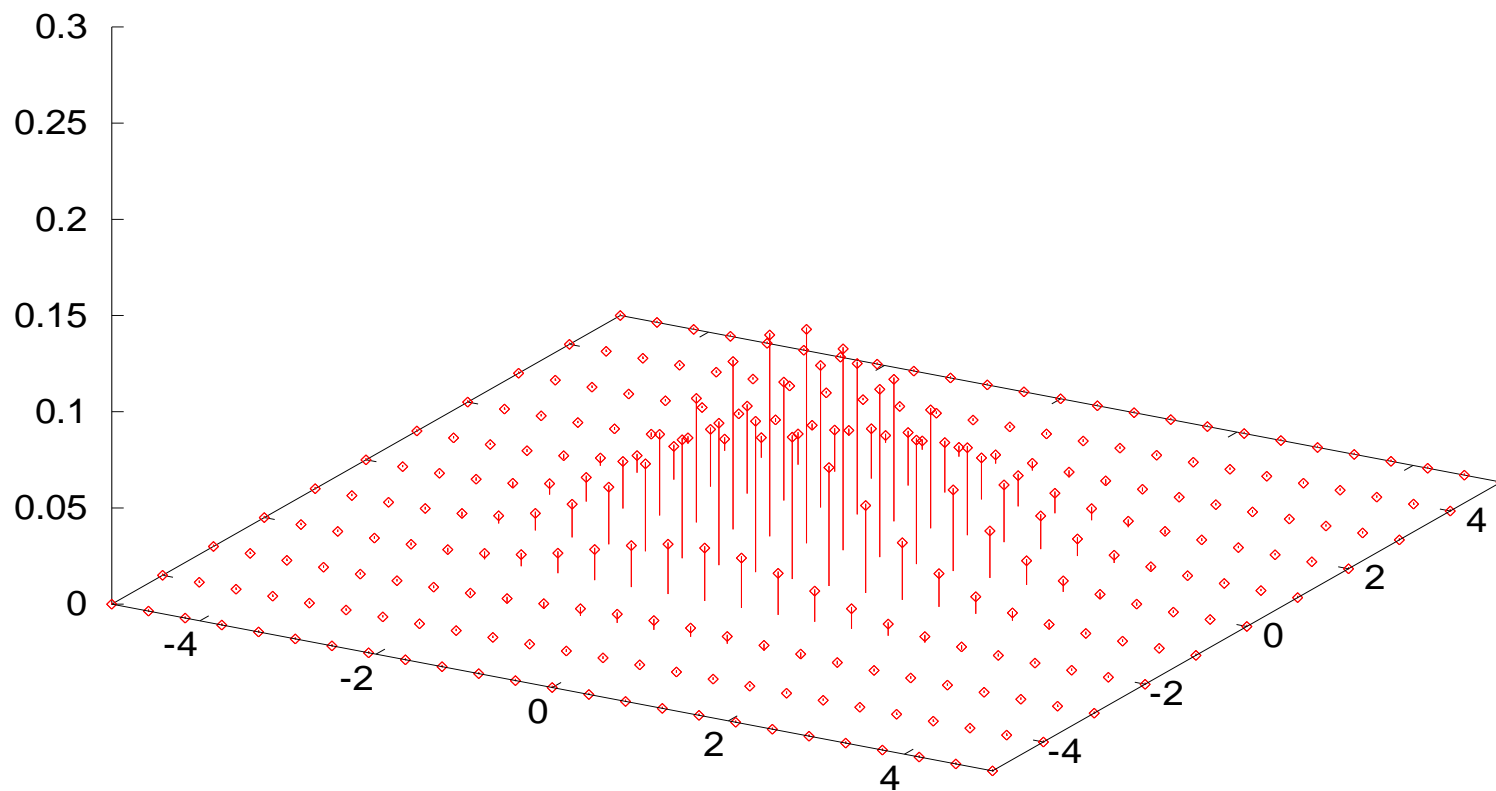
補足: 図の気持ち

- ガウス分布の性質を保って
いそう
- s のサイズが小さいとガウス
分布の性質を保たなさそう

$$D_{L,2}$$



$D_{L,3}$ 



Smoothing Parameter

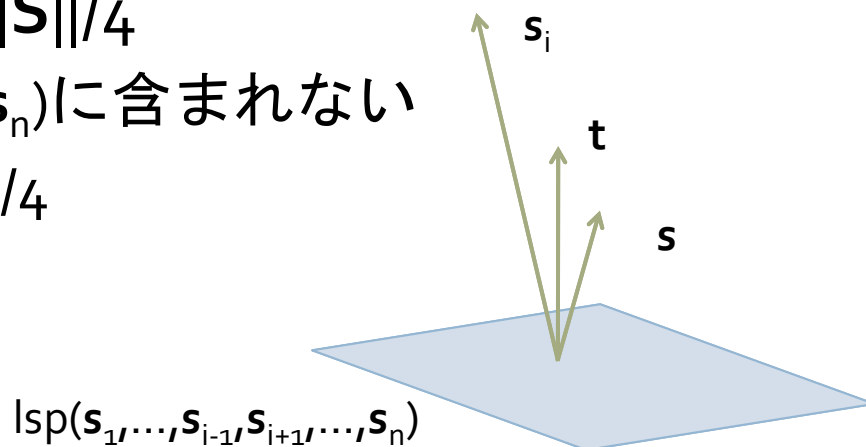
- $\eta_\varepsilon(L) := \min\{s: \rho_{1/s}(L^* - \{\mathbf{0}\}) \leq \varepsilon\}$
- $s \geq \eta_\varepsilon(L(\mathbf{B}))$ ならば
 $\Delta(v_{s,c} \bmod P(\mathbf{B}), U(P(\mathbf{B}))) \leq \varepsilon/2$
- 性質
 - $\varepsilon = 2^{-n}$ ならば, $\eta_\varepsilon(L) \leq (1/\lambda_1(L^*)) \sqrt{n}$
 - $\eta_\varepsilon(L) \leq \lambda_n(L) O(\log(n(1+1/\varepsilon)))$

IncGDD $_{\gamma, g}^{\phi}$

- Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, r > \gamma(n)\phi(L(\mathbf{B}))$
- Output: $s \in L(\mathbf{B})$ s.t. $\|s - \mathbf{t}\| \leq (\|\mathbf{S}\|/g) + r$
- η_{ϵ} は λ_n と関係があるので IncGDD $_{\gamma, g}^{\eta_{\epsilon}}$ でも OK
 - 再掲: $\eta_{\epsilon}(L) \leq \lambda_n(L)O(\log(n(1+1/\epsilon)))$

SIVPが解けるか?

- $\text{IncGDD}_{\gamma,8}^{\lambda n}$ が解けると $\text{SIVP}_{8\gamma}$ が解ける
 - $s_i = \|S\|$ となる i を探す
 - t を $\text{lsp}(s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n)$ と垂直な長さ $\|S\|/2$ のベクトルとする
 - IncGDD で $(B, S, t, \|S\|/8)$ を解く \rightarrow 解 s を得る
 - $\|s-t\| \leq \|S\|/8 + \|S\|/8 = \|S\|/4$
 - s は $\text{lsp}(s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n)$ に含まれない
 - $\|s\| \leq \|s-t\| + \|t\| \leq 3\|S\|/4$
 - 解 s を s_i と置き換える



Sampling Algorithm S

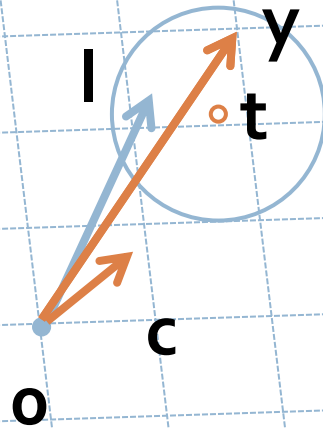
- Pseudo-Cubeの構成
 - ▣ $Q=P(S)$ になる点がポイント
- Pseudo-Cubeの分割
- サンプリング
 - ▣ Q 中の点 v_i をサンプリング
 - v_i は Q 中の格子点ではない
 - ▣ 分割に基づいて a_i を出力

Sampling Algorithm S

- Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, s > \eta_\epsilon(\mathbf{B})$
- Output: $\mathbf{a} \in \mathbb{Z}_q^n$ (一様分布に従う)
- 中間目標: $\mathbf{c} \in P(\mathbf{B})$ (一様分布に従う) と $\mathbf{y} \in L(\mathbf{B})$
- Algorithm - 1:
 - $\mathbf{l} \leftarrow v_{s, \mathbf{t}}$
 - $\mathbf{c} = -\mathbf{l} \bmod P(\mathbf{B})$
 - $\Delta(\mathbf{c}, U(P(\mathbf{B}))) \leq \epsilon/2$
 - $\mathbf{y} = \mathbf{c} + \mathbf{l}$
 - $\mathbf{y} \in L(\mathbf{B})$ かつ \mathbf{y} は $\mathbf{c} + \mathbf{t}$ に近い
 - $\mathbf{y} \sim D_{L(\mathbf{B}), s, \mathbf{c} + \mathbf{t}}$

Sampling Algorithm S

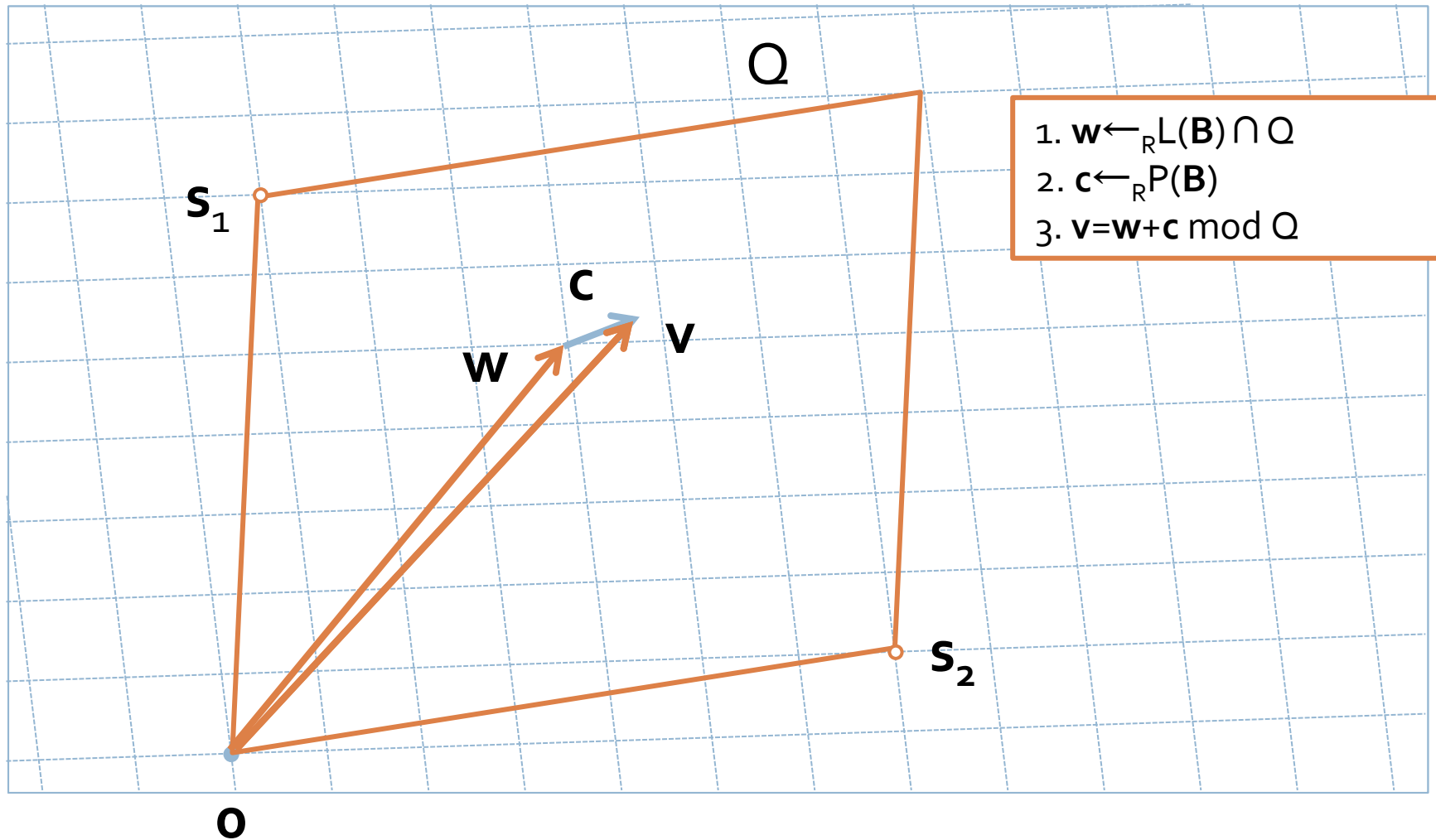
1. t を中心にガウス分布
2. l を選ぶ
3. $c = -l \pmod{P(B)}$
4. $y = c + l$



Sampling Algorithm S

- Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, s > \eta_\epsilon(\mathbf{B})$
- Output: $\mathbf{a} \in \mathbb{Z}_q^n$ (一様分布に従う)
- 中間目標: $\mathbf{v} \in \mathbb{Q}$ (一様分布に従う)
- Algorithm - 2:
 - ▣ $\mathbf{w} \in L(\mathbf{B}) \cap \mathbb{Q}$ をランダムに選ぶ
 - ▣ $\mathbf{v} = \mathbf{c} + \mathbf{w} \bmod \mathbb{Q}$
 - ▣ ポイント: \mathbf{v} は \mathbb{Q} 上ほぼ一様分布

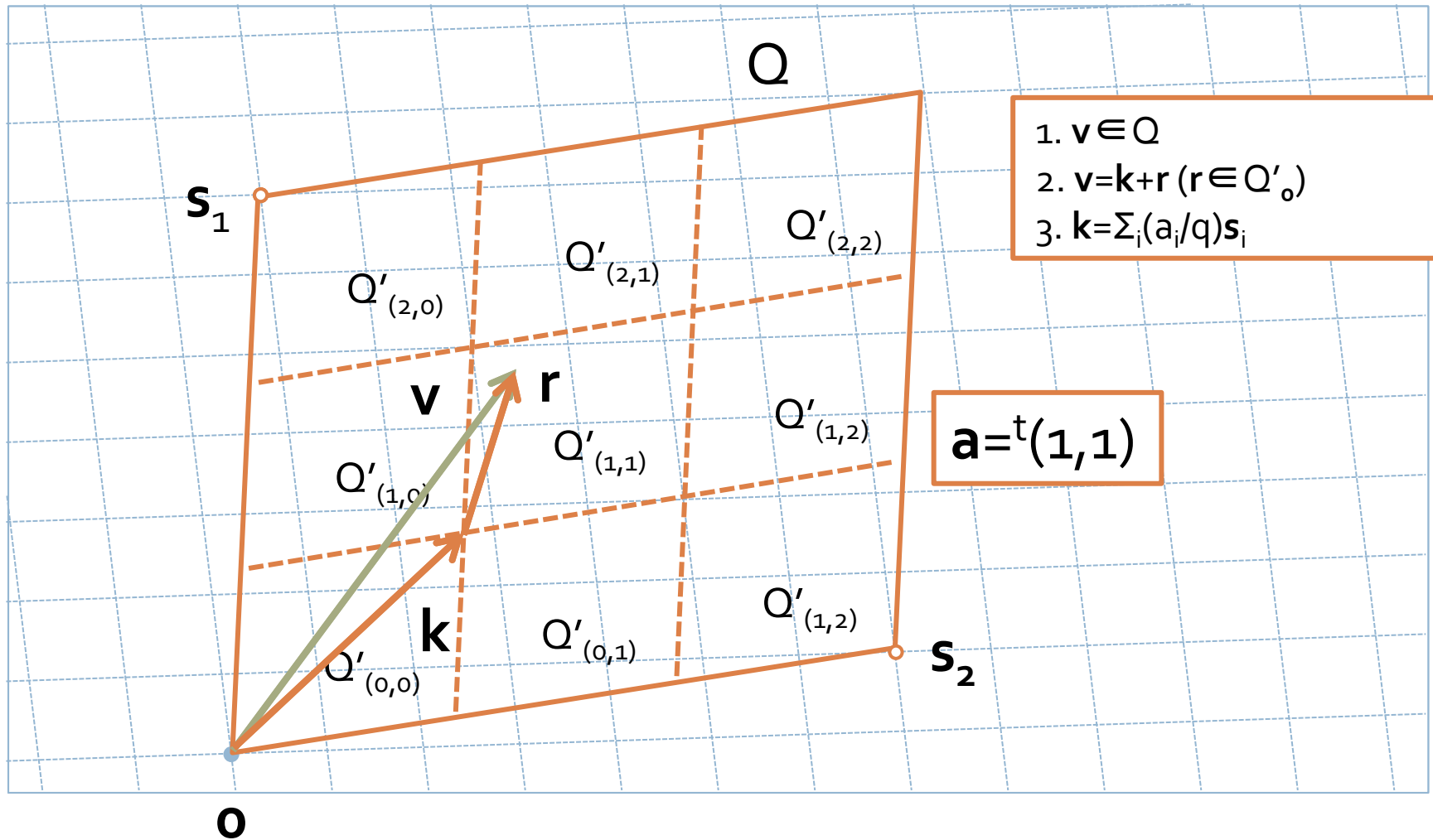
Sampling Algorithm S



Sampling Algorithm S

- Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, s > \eta_\varepsilon(\mathbf{B})$
- Output: $\mathbf{a} \in \mathbb{Z}_q^n$ (一様分布に従う)
- Algorithm - 3: \mathbf{v} を使って, \mathbf{a} を作る
 - \mathbf{a} を \mathbf{v} が入っている Q'_a のインデックスとする
 - $\mathbf{v} = \mathbf{r} + \sum_i (a_i/q) \mathbf{s}_i$
 - $\mathbf{r} \in Q'_0$ かつ $\|\mathbf{r}\| \leq (1/q) \|\mathbf{S}\| \sqrt{n}$

Sampling Algorithm S



IncGDD を解く

- S を m 回使って, $A=[\mathbf{a}_1, \dots, \mathbf{a}_m]$ を得る
- $\mathbf{z} = \mathcal{F}(1^n, A)$ とする ($A\mathbf{z} = \mathbf{0} \pmod{q}$, $\mathbf{z} \in \{-1, 0, 1\}^m - \{\mathbf{0}\}$)
- $\mathbf{x} := \sum_i z_i (\mathbf{c}_i - \mathbf{v}_i) + \sum_i z_i (\sum_j (a_{(i,j)}/q) \mathbf{s}_j)$
- $\mathbf{s} := \mathbf{x} - \sum_i z_i \mathbf{y}_i$

- 示すべきこと
 - $\mathbf{s} \in L(\mathbf{B})$
 - $\|\mathbf{s} - \mathbf{t}\| \leq (\|\mathbf{S}\|/g) + r$

IncGDD

Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, r > \gamma(n)\phi(L(\mathbf{B}))$

Output: $\mathbf{s} \in L(\mathbf{B})$ s.t. $\|\mathbf{s} - \mathbf{t}\| \leq (\|\mathbf{S}\|/g) + r$

IncGDD を解く ($s \in L(\mathbf{B})$)

- $s \in L(\mathbf{B})$?
 - $s = x - \sum_i z_i y_i$
- $x = \sum_i z_i (c_i - v_i) + \sum_i z_i (\sum_j (a_{(i,j)}/q) s_j) \in L(\mathbf{B})$
 - 前半:
 - $c_i - v_i = ((c_i + w_i) - v_i) - w_i \in L(\mathbf{B})$
 - $v = c + w \pmod Q, w \in L(\mathbf{B})$
 - 後半:
 - $s_i \in L(\mathbf{S}) \subseteq L(\mathbf{B})$
 - for any $j, \sum_i z_i a_{(i,j)}/q \in \mathbb{Z}$ ([Ajtai '96] と同じ)
 - よって $\sum_i z_i (\sum_j (a_{(i,j)}/q) s_j) \in L(\mathbf{B})$
- $y_i \in L(\mathbf{B})$

IncGDD

Input: $\mathbf{B}, \mathbf{S}, t, r > \gamma(n)\phi(L(\mathbf{B}))$

Output: $s \in L(\mathbf{B})$ s.t. $\|s - t\| \leq (\|\mathbf{S}\|/g) + r$

IncGDD を解く ($\|\mathbf{s}-\mathbf{t}\|$ の不等式)

- $\mathbf{s}=\mathbf{x}-\sum_i z_i \mathbf{y}_i$
- $\mathbf{x}=\sum_i z_i (\mathbf{c}_i-\mathbf{v}_i)+\sum_i z_i (\sum_j (a_{(i,j)}/q) \mathbf{s}_j)$
- $\|\mathbf{x}-\sum_i z_i \mathbf{c}_i\|$ は小さい
- $\|(\mathbf{c}_i+\mathbf{t}_i)-\mathbf{y}_i\|$ も小さい
 - $\mathbf{y}_i \sim D_{L,S,\mathbf{c}_i+\mathbf{t}_i}$
- $\|\mathbf{s}+\sum_i z_i \mathbf{t}_i\| \leq \|\mathbf{x}-\sum_i z_i \mathbf{c}_i\| + \|\sum_i z_i ((\mathbf{c}_i+\mathbf{t}_i)-\mathbf{y}_i)\|$

- どこかの $\mathbf{t}_i=-\mathbf{t}$ としておく

IncGDD

Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, r > \gamma(n)\phi(L(\mathbf{B}))$

Output: $\mathbf{s} \in L(\mathbf{B})$ s.t. $\|\mathbf{s}-\mathbf{t}\| \leq (\|\mathbf{S}\|/g)+r$

IncGDD を解く ($\|s-t\|$ の不等式)

- $\|x - \sum_i z_i c_i\| \leq \|S\|/g$?
- $\|x - \sum_i z_i c_i\| \leq (1/q)m\|S\|\sqrt{n}$
 - 左辺 = $\|\sum_i z_i (-v_i + \sum_j (a_{(i,j)}/q)s_j)\| = \|\sum_i z_i (-r_i)\|$
 - $r_i \in Q'$ より $\|r_i\| \leq (1/q)\|S\|\sqrt{n}$
- $(m/q)\sqrt{n} \leq 1/g$ と調整する

IncGDD

Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, r > \gamma(n)\phi(L(\mathbf{B}))$

Output: $s \in L(\mathbf{B})$ s.t. $\|s - \mathbf{t}\| \leq (\|S\|/g) + r$

IncGDD を解く ($\|\mathbf{s}-\mathbf{t}\|$ の不等式)

- $\|\sum_i z_i((\mathbf{c}_i+\mathbf{t}_i)-\mathbf{y}_i)\| \leq r$?
- $\mathbf{y}_i \sim D_{L(\mathbf{B}),s,\mathbf{c}_i+\mathbf{t}_i}$
- $\text{Exp}[\|(\mathbf{c}_i+\mathbf{t}_i)-\mathbf{y}_i\|^2] \leq O(s^2n)$
- $\text{Exp}[\|\sum_i z_i((\mathbf{c}_i+\mathbf{t}_i)-\mathbf{y}_i)\|^2] \leq \|\mathbf{z}\|^2 s^2 n / 6$
 - $s=2r/\gamma > \eta \epsilon(L(\mathbf{B})), \|\mathbf{z}\| \leq \sqrt{m}, \gamma=\sqrt{mn}$ とすれば
 - $\|\mathbf{z}\|^2 s^2 n / 6 \leq 2r^2 / 3$
 - Markovの不等式

IncGDD

Input: $\mathbf{B}, \mathbf{S}, \mathbf{t}, r > \gamma(n)\phi(L(\mathbf{B}))$

Output: $\mathbf{s} \in L(\mathbf{B})$ s.t. $\|\mathbf{s}-\mathbf{t}\| \leq (\|\mathbf{S}\|/g)+r$

MRO₄ まとめ

- QをP(S)にした
- n次元ガウス分布を使った
- 問題を変えた
 - IncGDD
 - cf: IncSIVP
- 近似度が小さくなった

未解決問題

未解決問題 – 計算量

- GapSVP_γ
- $\gamma=c$ で NP-hard
 - [Khot 2004]
- $\gamma=O(\sqrt{n}/\log n)$ で $\text{NP} \cap \text{coAM}$
 - [Goldreich-Goldwasser 2000]
- $\gamma=O(\sqrt{n})$ で $\text{NP} \cap \text{coNP}$
 - [Aharonov-Regev 2004]
- 量子だとどうなるのか?
- ノルムを変えるとどうなるのか?
 - Norm-Embedding [Regev-Rosen 2005]
 - [Peikert 2006]

未解決問題 – a/w

□ 一般の格子

- [Ajtai '96] (OWFs?, $O(n^8)$, SIVP)
- [GGH '96] (CRHFs, $O(n^8)$, SIVP)
- [Cai-Nerurker '97] (CRHFs, $O(n^{3+\epsilon})$, SIVP)
- [Micciancio 2002] (CRHFs, $O_{\sim}(n^3)$, SIVP)
- [Micciancio-Regev 2004] (CRHFs, $O_{\sim}(n)$, SIVP)

□ 特殊な格子

- [Micciancio 2002] (OWFs, $O_{\sim}(n)$, Cyclic-SVP)
- [Lybashevsky-Micciancio 2006] (CRHFs, $O_{\sim}(n)$, Ideal-)
- [Peikert-Rosen 2006] (CRHFs, $O_{\sim}(n)$, Cyclic-)

未解決問題 – a/w

- 近似度 $O(\sqrt{n})$ の a/w-connection
 - 近似度 $O(n)$ が最良 [Micciancio-Regev 2004]
 - 特殊な格子: $O(\sqrt{n})$? [Peikert-Rosen 2007]
 - Ideal Lattice より良い代数的な構造を持つ
 - 整数環上のイデアルと同型な格子
 - 決定版 (GapSVP_γ) は多項式時間で解ける
 - 誰か探索版 (SVP_γ) を解いてみませんか?

未解決問題 – 格子暗号

□ 1-bit Type

- [Ajtai-Dwork '97] ($O(n^8)$ -uSVP, a/wあり)
- [Regev 2004] ($O\sim(n^{1.5})$ -uSVP, a/wあり)
- [Regev 2005] (近似度 $O\sim(n^{1.5})$ のSVP, a/wあり)
- [Ajtai 2005] (特殊な $O(n^{1.5})$ -uSVP, a/wなし)

□ Multi-bit Type

- [GGH '97] (CVPベース)
- [NTRU '97] (多項式環, NTRU-CVPベース)
- [Cai-Cusick '98] (AD暗号+ナップサック)
- etc

未解決問題 – 格子暗号

- 効率のよい格子暗号
 - [Ajtai 2005]
 - 😊 鍵 $O(n^2)$ / 平文:暗号文=1: $O(n \log n)$
 - 😞 特殊な格子の平均時の困難性
 - [Regev 2005]
 - 😊 鍵 $O(n^2)$ / 平文:暗号文=1: $O(n \log n)$
 - 😊 近似度 $O(n^{1.5})$ の SVP, SIVP の最悪時の困難性
 - 😞 帰着が量子帰着
 - [Kawachi-Tanaka-Xagawa 2007]
 - 😊 平文:暗号文= $O(\log n)$: $O(n \log n)$
 - 😞 近似度が悪くなる
- 特殊な格子 (e.g., cyclic-, ideal-) を用いた暗号

未解決問題 – 格子暗号

- 数論系との比較
 - SVPからRSA問題への帰着はあるか?
 - (n, p, q, e, d) の d が小さいとLLLで解ける
 - d が小さくなくてもSVPが解ければ解けるか?
 - 一般に, 格子問題から数論系の問題への帰着は?
- CCA-secureな暗号
 - 1-bit暗号だと辛い?

未解決問題 – 署名

- SVPの困難性に基づく署名方式の構成
 - GGH, NSS, NTRUSign
 - ☹️ 特殊なCVPベース
 - ☹️ 攻撃されたのもうダメ
 - 一般的な構成法
 - ハッシュ関数+[Rompel 90, Naor-Yung 89]
 - ☹️ 効率が悪い, 面白くない
- (実は)できます
 - 公開鍵: $O\sim(n^2)$ / 秘密鍵: $O\sim(n)$ / 署名長: $O\sim(n^2)$
 - $SVP_{O\sim(n)}$ の最悪時から署名のROMでの安全性を保証
 - 次の機会に

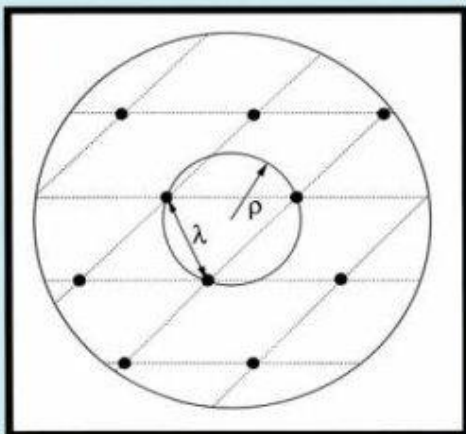
参考文献

- [Ajtai '96]
 - ▣ “Generating hard instances of lattice problems” (STOC 1996)
- [Cai '99]
 - ▣ “Some recent progress on the complexity of lattice problems” (ECCC 1999)
- [Micciancio-Regev 2004]
 - ▣ “Worst-case to average-case reductions based on Gaussian measures” (FOCS 2004)
- 他

参考文献

**COMPLEXITY OF
LATTICE PROBLEMS**
A Cryptographic
Perspective

Daniele Micciancio
Shafi Goldwasser



Complexity of Lattice Problems: A Cryptographic Perspective

暗号理論のための 格子の数学

D. ミッチアンチオ
S. ゴールドヴァッサー 著
林 彬 訳

Springer
シュプリンガー・ジャパン

御清聴

ありがとう

ございました