イデアル格子で作る
効率の良い公開鍵暗号方式、他

草川 恵太 (東京工業大学)

結果は？

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,...,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

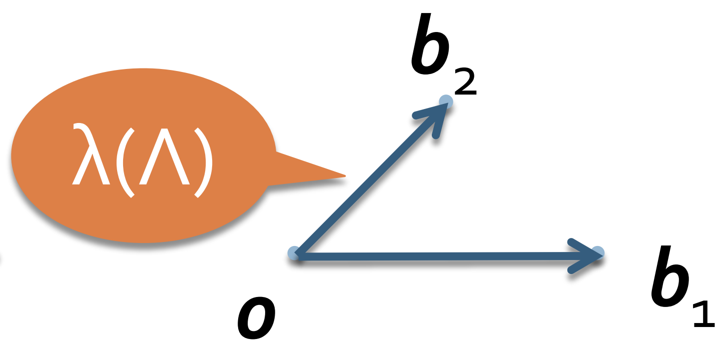
説明は？

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,…,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

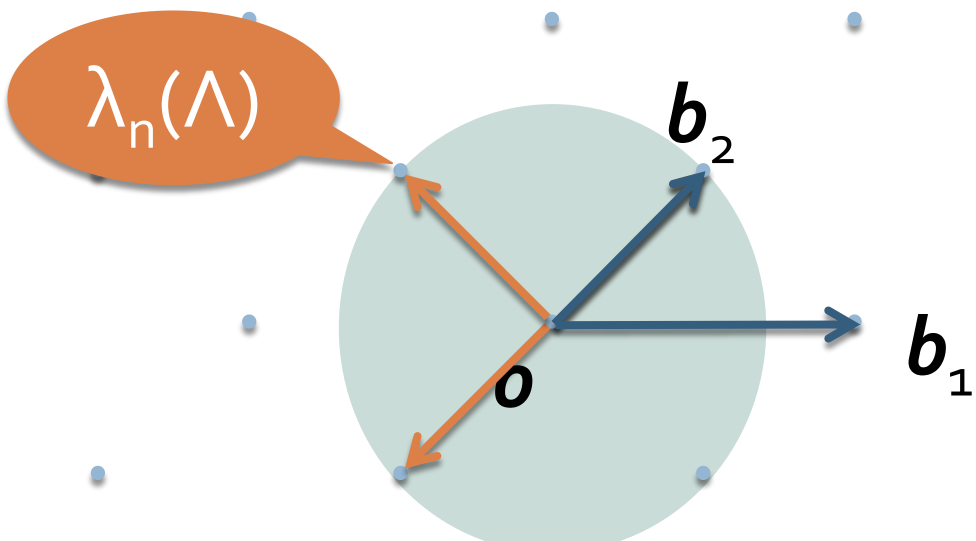
格子

- $\boldsymbol{B}=[\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n] \in \mathbb{Q}^{n\times n}$
- $L(\boldsymbol{B}) := \{\Sigma_i \alpha_i \boldsymbol{b}_i \mid \alpha_i \in \mathbb{Z} \text{ for all } i\} \subseteq \mathbb{Q}^n$
- $\lambda(\Lambda)$: Λ中の最短ベクトルの長さ



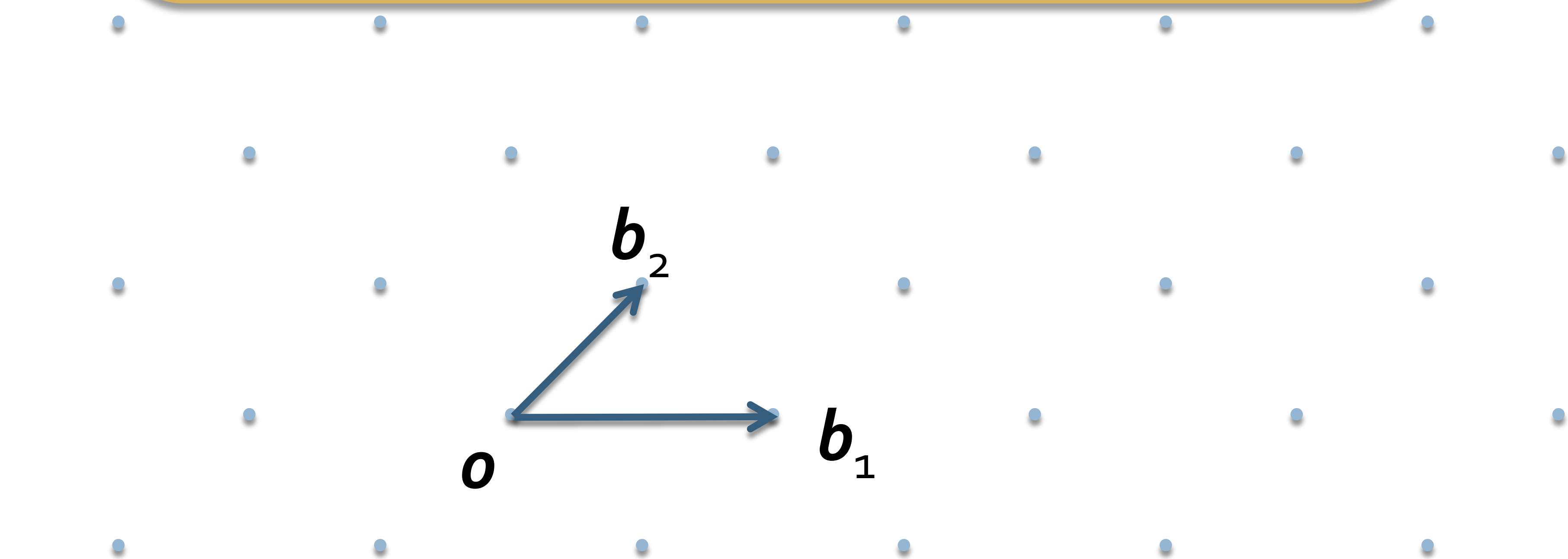
格子定数2

- $\lambda_n(\Lambda)$: Λ中の線形独立なベクトルの組の長さの最大値の最小値
- $\lambda_n(\Lambda) = \min_{\boldsymbol{s}:\text{lin. ind. set in } \Lambda} \max_i \|\boldsymbol{s}_i\|$
- $\lambda_n(\Lambda) = \min\{r: \dim(\mathrm{span}(B_n(r) \cap \Lambda))=n\}$



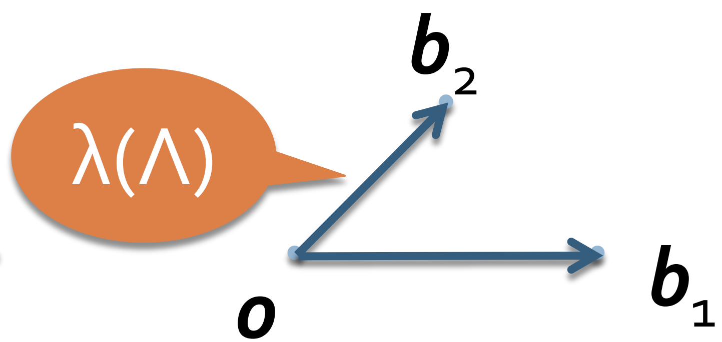
格子: 例

$$\boldsymbol{B} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$$



双对格子

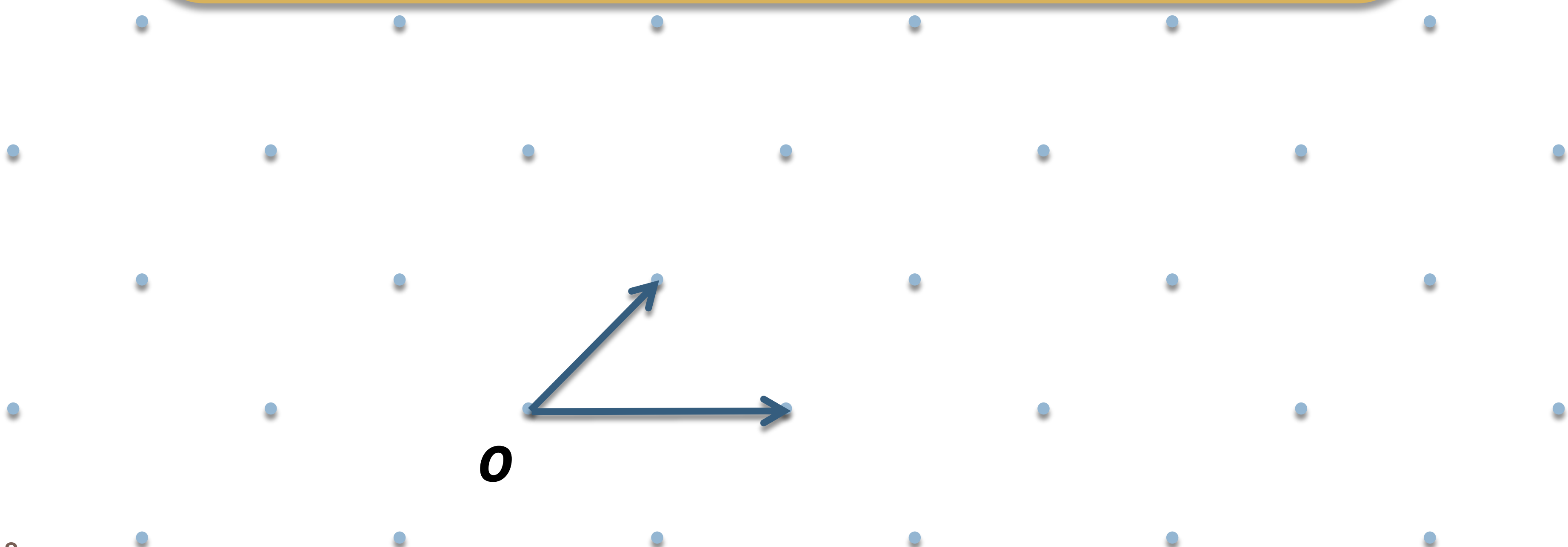
- $\boldsymbol{B}=[\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n] \in \mathbb{Q}^{n\times n}$
- $L(\boldsymbol{B}) := \{\sum_i \alpha_i \boldsymbol{b}_i \mid \alpha_i \in \mathbb{Z} \text{ for all } i\} \subseteq \mathbb{Q}^n$
- $\Lambda^* = \{\boldsymbol{x} \mid \langle \boldsymbol{x}, \boldsymbol{v}\rangle \in \mathbb{Z} \text{ for all } \boldsymbol{v} \text{ in } \Lambda\}$
- $\Lambda^* = L(\boldsymbol{B}^{-T})$



双对格子: 例

$$\boldsymbol{B} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \qquad \boldsymbol{B}^{-T} = \begin{pmatrix} -1/2 & 1 \\ 1/2 & 0 \end{pmatrix}$$

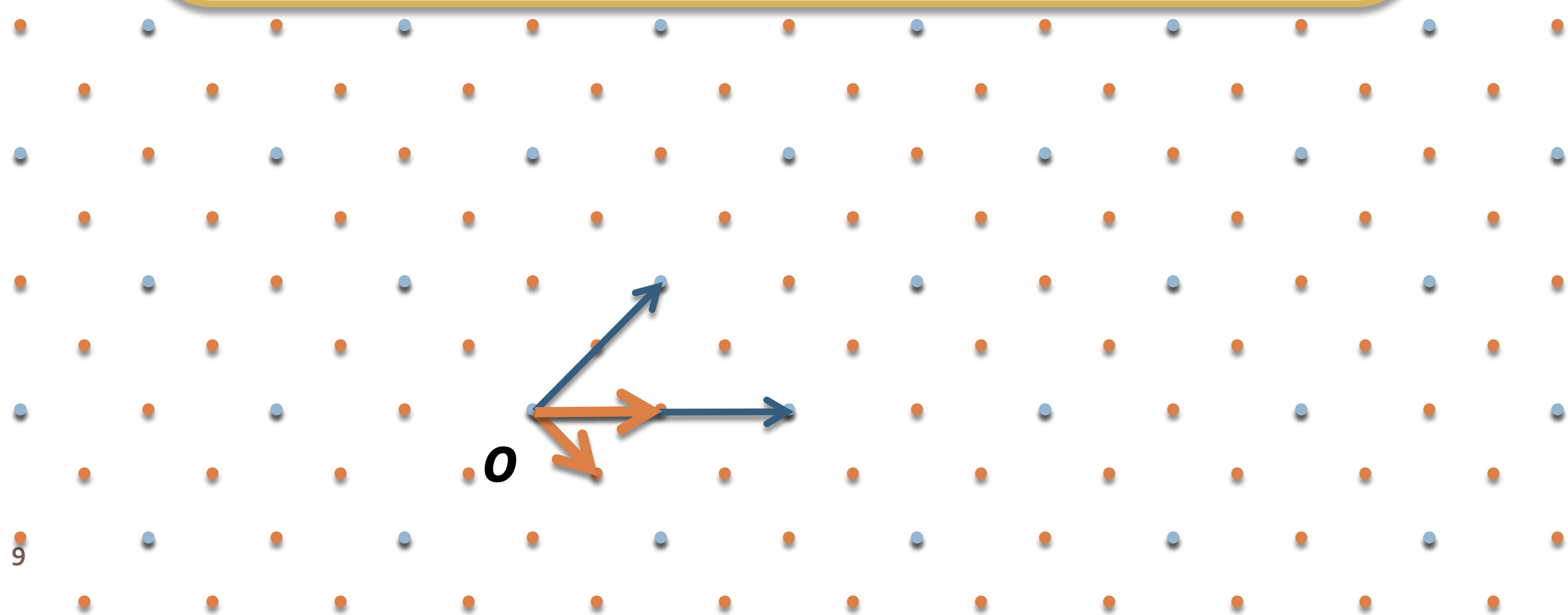
$$\boldsymbol{B}^{-1} = \begin{pmatrix} -1/2 & 1/2 \\ 1 & 0 \end{pmatrix}$$



双対格子: 例

$$\boldsymbol{B} = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \qquad \boldsymbol{B}^{-T} = \begin{pmatrix} -1/2 & 1 \\ 1/2 & 0 \end{pmatrix}$$

$$\boldsymbol{B}^{-1} = \begin{pmatrix} -1/2 & 1/2 \\ 1 & 0 \end{pmatrix}$$



特殊な格子

For $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$

- $\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \boldsymbol{Ae} = \boldsymbol{0} \bmod q\}$
- $\Lambda_q(\boldsymbol{A}) = \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{y} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} \bmod q\}$

$\Lambda_q^{\perp}(\boldsymbol{A})$

$\Lambda_q(\boldsymbol{A})$

特殊な格子

For $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$

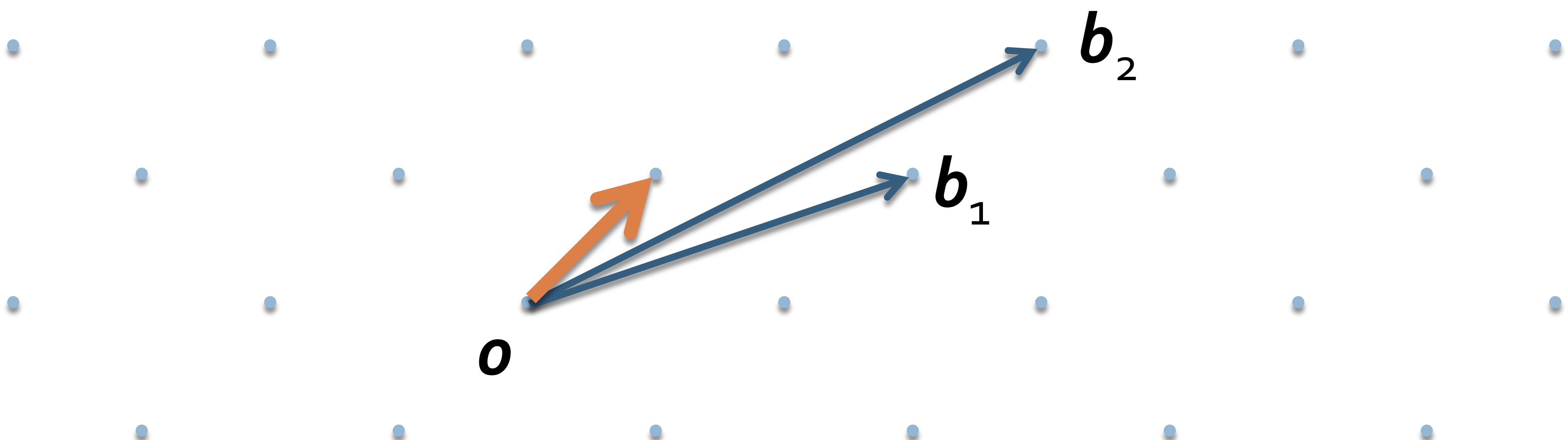
- $\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \boldsymbol{Ae} = \boldsymbol{0} \bmod q\}$
- $\Lambda_q(\boldsymbol{A}) = \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{y} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} \bmod q\}$

$$(\Lambda_q(\boldsymbol{A}))^* = (1/q)\,\Lambda_q^{\perp}(\boldsymbol{A})$$

最短ベクトル問題 (SVP)

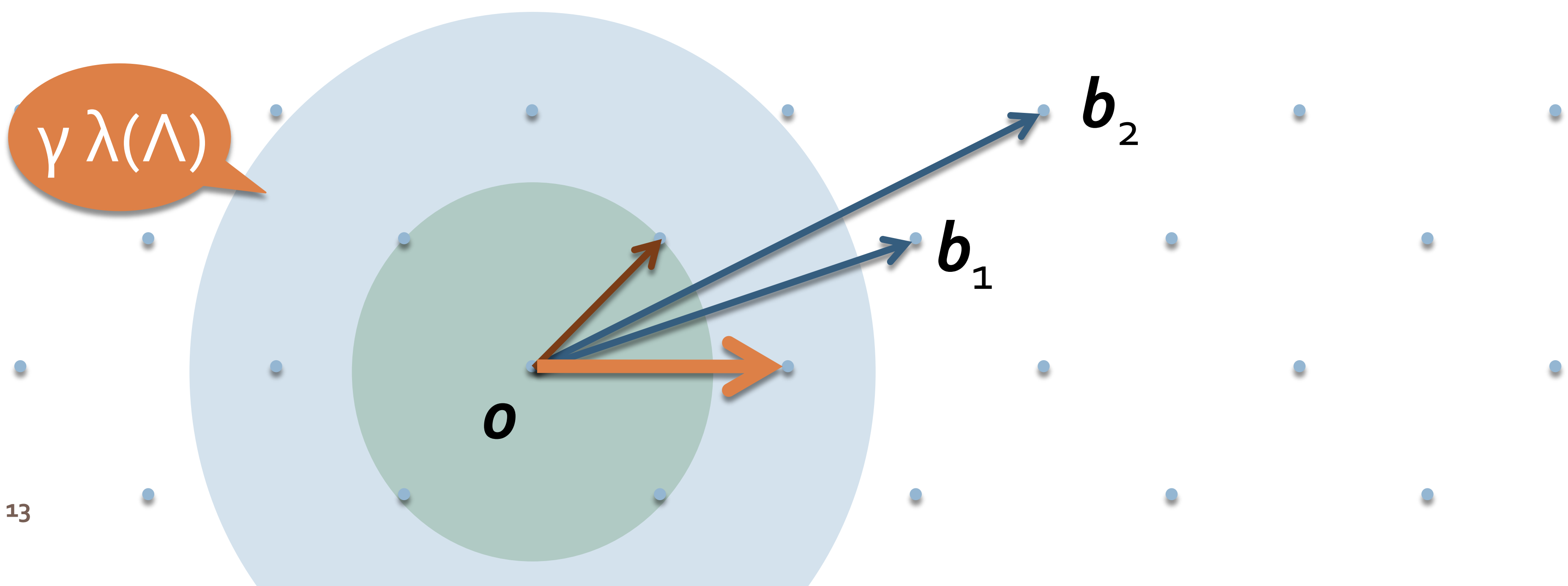
Given $\boldsymbol{B}$ of Λ

find $\boldsymbol{v} \in \Lambda - \{\boldsymbol{o}\}$ s.t. $\|\boldsymbol{v}\| = \lambda(\Lambda)$



近似版最短ベクトル問題 (SVP$_\gamma$)

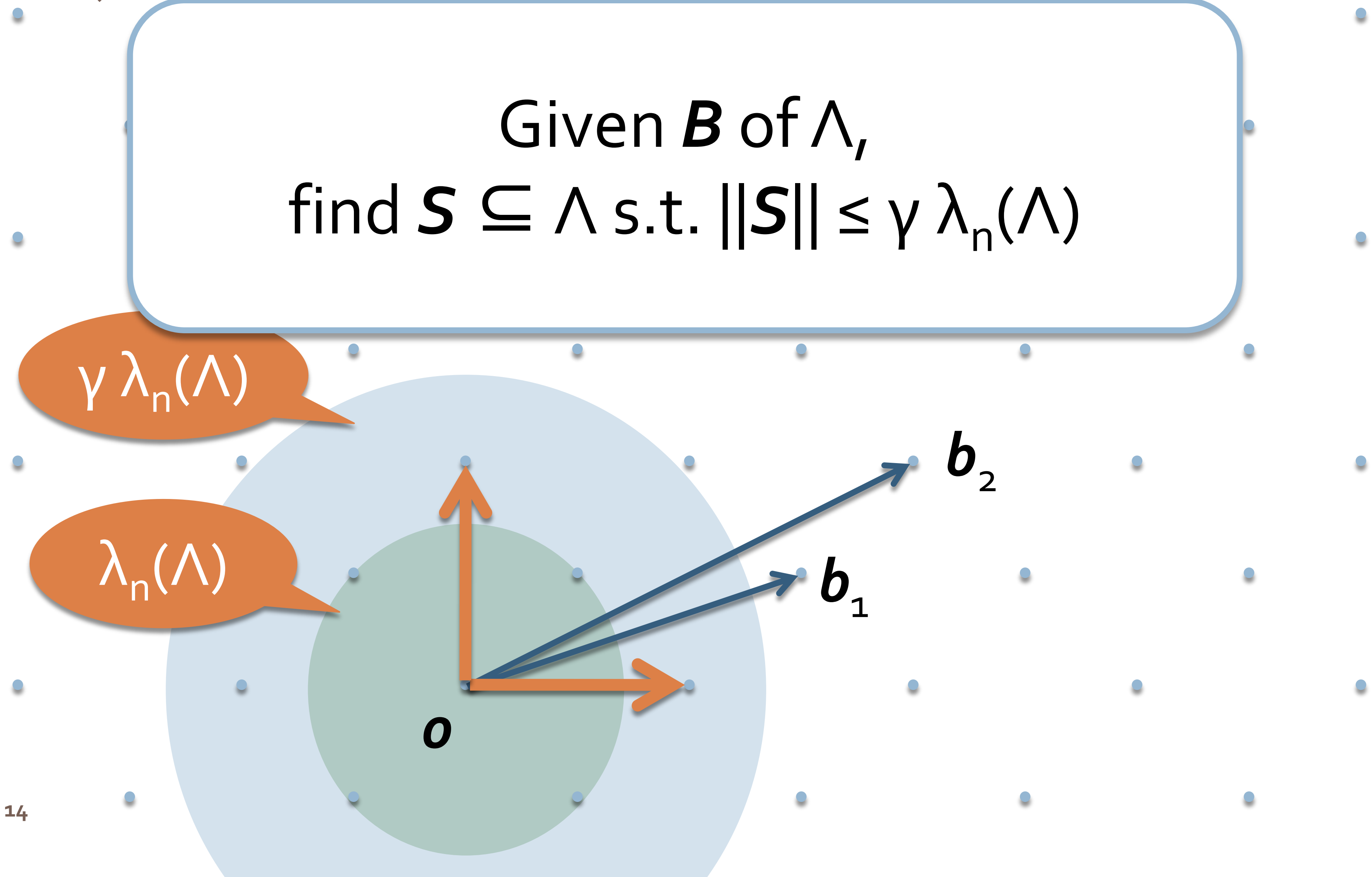
Given $\boldsymbol{B}$ of Λ,
find $\boldsymbol{v} \in \Lambda - \{\boldsymbol{o}\}$ s.t. $\|\boldsymbol{v}\| \le \gamma\,\lambda(\Lambda)$



近似版最短線形独立ベクトル集合問題 (SIVPγ)

Given $\boldsymbol{B}$ of Λ,

find $\boldsymbol{S} \subseteq \Lambda$ s.t. $\|\boldsymbol{S}\| \leq \gamma\, \lambda_n(\Lambda)$



	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	**[Ajt97,...,MR07, GPV08]**	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

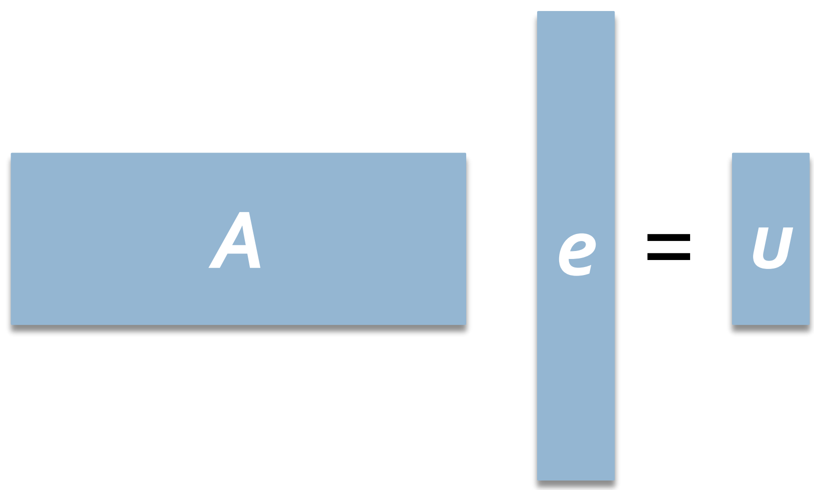
	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

格子ハッシュ [Ajt96,…,MR07,GPV08]

$$H_n = \{h_{\boldsymbol{A}} : D_n \longrightarrow \mathbb{Z}_q^n \mid \boldsymbol{A} \in \mathbb{Z}_q^{n \times m}\}$$

$$h_{\boldsymbol{A}}(\boldsymbol{e}) = \boldsymbol{A}\boldsymbol{e} \bmod q$$

$$D_n = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \|\boldsymbol{e}\| \le d\}$$



短い整数解問題 ($\mathrm{SIS}_{q,m,\beta}$)

Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}$,
find $\boldsymbol{e} \in \mathbb{Z}^m$ s.t. $\|\boldsymbol{e}\| \leq \beta$, $\boldsymbol{Ae} = \boldsymbol{o} \bmod q$

格子$\Lambda_q^{\perp}(\boldsymbol{A})$の
短い非ゼロベクトルを
探索

$\mathrm{Col}(H) \geq \mathrm{SIS}_{q,m,2d}$ [GGH96]

$$H_n = \{h_{\boldsymbol{A}}: D_n \longrightarrow \mathbb{Z}_q^n \mid \boldsymbol{A} \in \mathbb{Z}_q^{n\times m}\}$$

$$h_{\boldsymbol{A}}(\boldsymbol{e}) = \boldsymbol{Ae} \bmod q$$

$$D_n = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \|\boldsymbol{e}\| \leq d\}$$

Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}$,

find $\boldsymbol{e} \in \mathbb{Z}^m$ s.t. $\|\boldsymbol{e}\| \leq \beta$, $\boldsymbol{Ae} = \boldsymbol{0} \bmod q$

$\mathrm{SIS}_{q,m,\beta} \geq_{a/w} \mathrm{SIVP}_{\tilde{O}(\beta\sqrt{n})}$ [Ajt96,GGH96,CN07, Mic04,MR07,GPV08]

Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}$,
find $\boldsymbol{e} \in \mathbb{Z}^m$ s.t. $\|\boldsymbol{e}\| \leq \beta$, $\boldsymbol{A}\boldsymbol{e} = \boldsymbol{0} \bmod q$

Given $\boldsymbol{B}$ of Λ,
find $\boldsymbol{S} \subseteq \Lambda$ s.t. $\|\boldsymbol{S}\| \leq \gamma\, \lambda_n(\Lambda)$

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,...,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	**[Mic04,LM06, PR06]**	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

イデアル格子版の準備

$$R = \mathbb{Z}[x]/(1+x^4) \longleftrightarrow D \subseteq M_4(\mathbb{Z})$$

$$\mathbf{x}(x) = 1+x+x^3 \longleftrightarrow \mathrm{Rot}_f(\mathbf{x}) = \begin{pmatrix} 1 & -1 & 0 & -1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\mathbf{y}(x) = 1+2x^2 \longleftrightarrow \mathrm{Rot}_f(\mathbf{y}) = \begin{pmatrix} 0 & 0 & -2 & -1 \\ 1 & 0 & 0 & -2 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \end{pmatrix}$$

$$\mathbf{x} \otimes \mathbf{y} = -1-3x+3x^2+2x^3 \longleftrightarrow \mathrm{Rot}_f(\mathbf{x})\mathrm{Rot}_f(\mathbf{y}) = \begin{pmatrix} -1 & -2 & -3 & 3 \\ -3 & -1 & -2 & -3 \\ 3 & -3 & -1 & -2 \\ 2 & 3 & -3 & -1 \end{pmatrix}$$

イデアル格子とイデアル格子問題

$$R = \mathbb{Z}[x]/\langle \mathbf{f} \rangle, \text{ e.g., } \mathbf{f} = x^n + 1$$

$$I \subseteq R \Leftrightarrow \Lambda_I \subseteq \mathbb{Z}^n$$

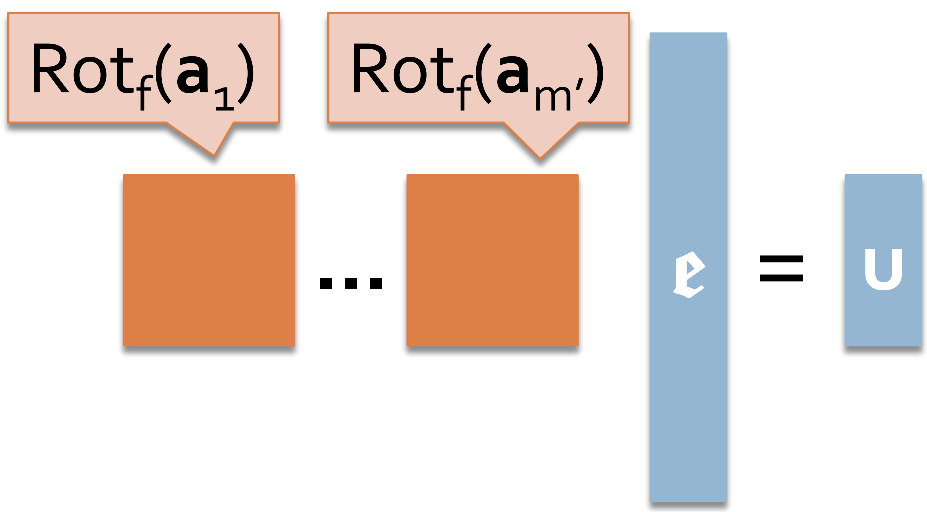
$\mathbf{f}$-SVP$_\gamma$:

Given $\boldsymbol{B}$ of Λ_I,

find $\boldsymbol{v} \in \Lambda_I - \{\boldsymbol{o}\}$ s.t. $\|\boldsymbol{v}\| \leqq \gamma\, \lambda(\Lambda_I)$

イデアル格子ハッシュ [Mic07,LM06,PR06,PR07]

$$H_n = \{h_{\mathfrak{a}} : D_n \longrightarrow R_q \mid \mathfrak{a} \in R_q^m\}$$
$$h_{\mathfrak{a}}(\mathfrak{e}) = \mathfrak{a}\,\mathfrak{e} \bmod q = \Sigma_i\, \mathbf{a}_i \mathbf{e}_i$$
$$D_n = \{\mathfrak{e} \in R^m \mid \|\mathfrak{e}\| \leq d\}$$



$\mathbf{f}$-Col(H) ≥ $\mathbf{f}$-SIS$_{q,m,2d}$

$$H_n = \{h_{\mathfrak{a}} : D_n \longrightarrow R_q \mid \mathfrak{a} \in R_q^m\}$$

$$h_{\mathfrak{a}}(\mathfrak{e}) = \mathfrak{a}\,\mathfrak{e} \bmod q = \Sigma_i\, \mathbf{a}_i \mathbf{e}_i$$

$$D_n = \{\mathfrak{e} \in R^m \mid \|\mathfrak{e}\| \le d\}$$

Given $\mathfrak{a} \leftarrow R_q^m$,

find $\mathfrak{e} \in R^m$ s.t. $\|\mathfrak{e}\| \le \beta$, $\mathfrak{a}\,\mathfrak{e} = \mathbf{0} \bmod q$

$\mathbf{f}\text{-SIS}_{q,m,\beta} \geq_{a/w} \mathbf{f}\text{-SVP}_{\tilde{O}(\beta\sqrt{n})}$ [Mic07,LM06,PR06, PR07,SSTX09,LPR10]

Given $\mathfrak{a} \leftarrow R_q^m$,
find $\mathfrak{e} \in R^m$ s.t. $||\mathfrak{e}|| \leq \beta$, $\mathfrak{a}\,\mathfrak{e} = \boldsymbol{o} \bmod q$

$\mathbf{f}\text{-SVP}_\gamma$:
Given $\boldsymbol{B}$ of Λ_I,
find $\boldsymbol{v} \in \Lambda_I\text{-}\{\boldsymbol{o}\}$ s.t. $||\boldsymbol{v}|| \leqq \gamma\, \lambda(\Lambda_I)$

注:$\mathbf{f}\text{-SIS}_{q,m,\beta}^{\infty} \geq_{a/w} \mathbf{f}\text{-SVP}_{\tilde{O}(\beta)}^{\infty}$

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,…,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

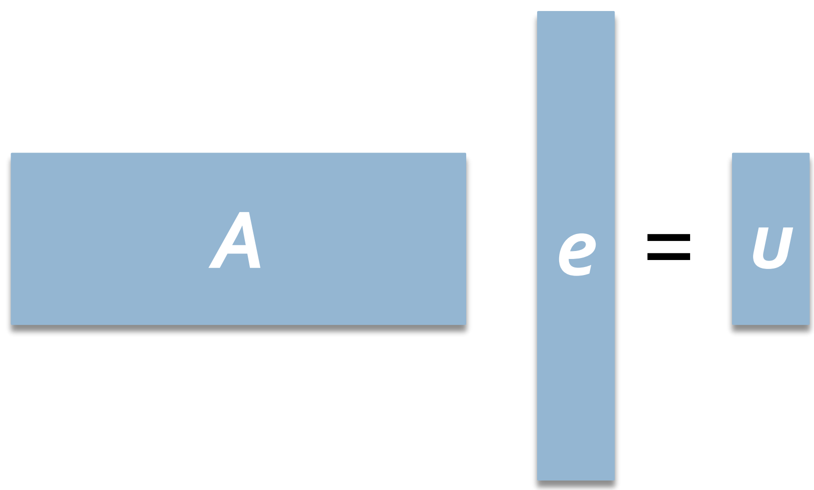
	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

格子ハッシュ [Ajt96,…,MR07,GPV08]

$$H_n = \{h_{\boldsymbol{A}} : D_n \longrightarrow \mathbb{Z}_q^n \mid \boldsymbol{A} \in \mathbb{Z}_q^{n \times m}\}$$

$$h_{\boldsymbol{A}}(\boldsymbol{e}) = \boldsymbol{A}\boldsymbol{e} \bmod q$$

$$D_n = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \|\boldsymbol{e}\| \leq d\}$$



落とし戸 [Ajt99, GPV08, AP09]

$$\boldsymbol{A} \quad \boldsymbol{T} \quad = \quad \boldsymbol{O}$$

$(\boldsymbol{A}, \boldsymbol{T}) \leftarrow \mathrm{Gen}(1^n)$

$\boldsymbol{T} \in \mathbb{Z}^{m \times m}$ s.t.

$\boldsymbol{T}$:a basis of $\Lambda_q^{\perp}(\mathbf{A})$, $\|\mathrm{GS}(\boldsymbol{T})\| \leqq L$

注: $L = \tilde{O}(\sqrt{n} \log q)$

落とし戸 [Ajt99, GPV08, AP09]

$$H_n = \{h_{\boldsymbol{A}}: D_n \longrightarrow \mathbb{Z}_q^n \mid \boldsymbol{A} \in \mathbb{Z}_q^{n \times m}\}$$
$$h_{\boldsymbol{A}}(\boldsymbol{e}) = \boldsymbol{A}\boldsymbol{e} \bmod q$$
$$D_n = \{\boldsymbol{e} \in \mathbb{Z}^m \mid \|\boldsymbol{e}\| \leq d\}$$

*T*があれば,
$h_{\boldsymbol{A}}(\boldsymbol{e})=\boldsymbol{u}$になる$\boldsymbol{e}$を取れる
(ただし$\|\boldsymbol{e}\| \leqq L\sqrt{m}\cdot\omega(\sqrt{\log m})$)

ガウス分布

- ガウス分布関数:

  $\nu_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|(\boldsymbol{x}-\boldsymbol{c})/s\|^2)/s^n$

- 離散ガウス分布関数:

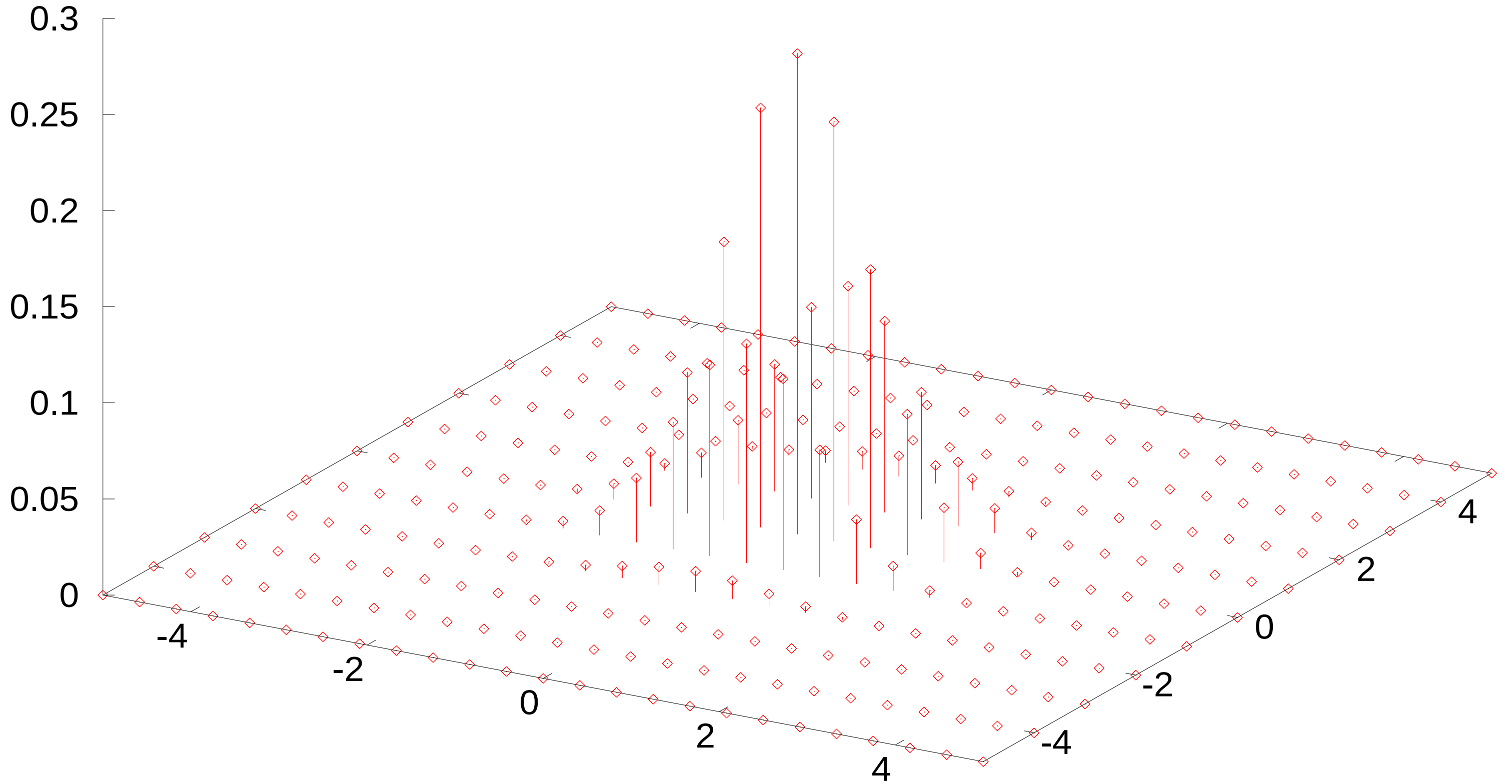
  $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\nu_{s,\boldsymbol{c}}(\boldsymbol{x})/\nu_{s,\boldsymbol{c}}(\Lambda)$

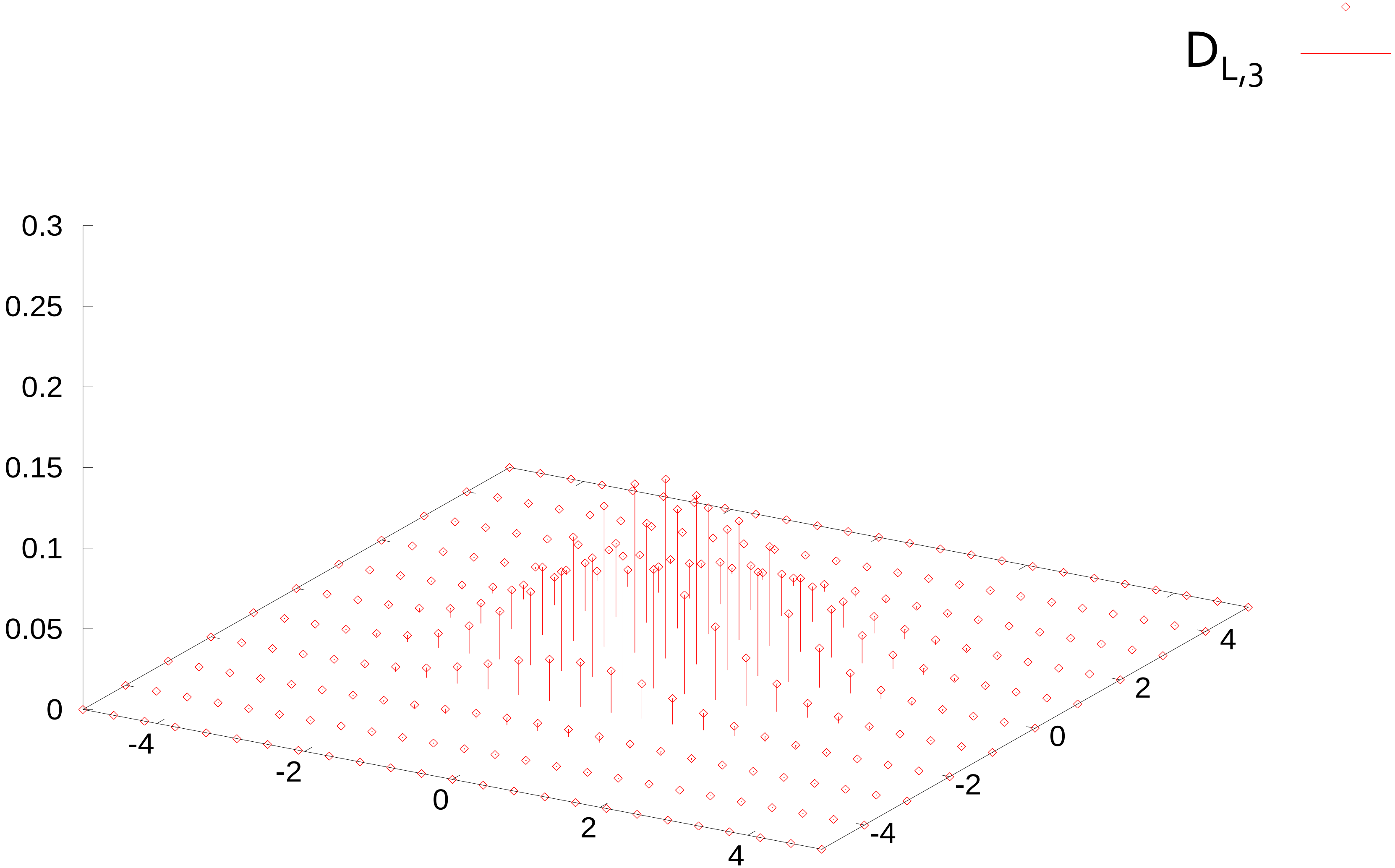
- $s \geq \lambda_n(\Lambda)\ \omega(\sqrt{\log n})$なら,

  $\Pr_{\boldsymbol{x}\leftarrow D}[\|\boldsymbol{x}\| > s\sqrt{n}] < \mathrm{negl}(n)$

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




$D_{L,3}$
0.3
0.25
0.2
0.15
0.1
0.05
0
-4
-2
0
2
4
-4
-2
0
2
4

Klein-GPV Sampling [Kle01?, GPV08,Pei10]

$\mathbf{T}$: a basis of Λ, $\|GS(\boldsymbol{T})\| \leq L$,

$s \geq L\ \omega(\sqrt{\log n})$,

$\Rightarrow \text{SampleD}(\boldsymbol{T}, s, \boldsymbol{c}) \sim_s D_{\Lambda,s,\boldsymbol{c}}$

Klein-GPV Sampling [Kle01?, GPV08,Pei10]

$\mathbf{T}$: a basis of Λ, $||GS(\boldsymbol{T})|| \leq L$,

$s \geq L\,\omega(\sqrt{\log n})$,

$\Rightarrow \text{SampleD}(\boldsymbol{T}, s, \boldsymbol{c}) \sim_s D_{\Lambda, s, \boldsymbol{c}}$

$(\boldsymbol{A}, \boldsymbol{T}) \leftarrow \text{Gen}(1^n)$

$\boldsymbol{T} \in \mathbb{Z}^{m \times m}$ s.t.

$\boldsymbol{T}$:a basis of $\Lambda_q^{\perp}(\mathbf{A})$, $||GS(\boldsymbol{T})|| \leq L$

注: $L = O(\sqrt{n \log q})$

Klein-GPV Sampling [Kle01?, GPV08,Pei10]

T: a basis of Λ, $||GS(\boldsymbol{T})|| \leq L$,

$s \geq L\,\omega(\sqrt{\log n})$,

$\Rightarrow \mathrm{SampleD}(\boldsymbol{T},s,\boldsymbol{c}) \sim_s D_{\Lambda,s,\boldsymbol{c}}$

Tがあれば、

$h_A(\boldsymbol{e})=\boldsymbol{u}$になる$\boldsymbol{e}$を取れる

(ただし$||\boldsymbol{e}|| \leqq s\sqrt{m}$, $s = L\,\omega(\sqrt{\log m})$)

GPV署名 [GPV08]

1. $\boldsymbol{u} = H(w \| r)$
2. $\boldsymbol{e} \leftarrow h_{\boldsymbol{A}}^{-1}(\boldsymbol{u})$

1. $h_{\boldsymbol{A}}(\boldsymbol{e}) = H(w \| r)$
2. $\|\boldsymbol{e}\| \le s\sqrt{m}$?

w

w, ($\boldsymbol{e}$, r)

vk = $\boldsymbol{A}$

sk = $\boldsymbol{T}$

vk = $\boldsymbol{A}$

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,…,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

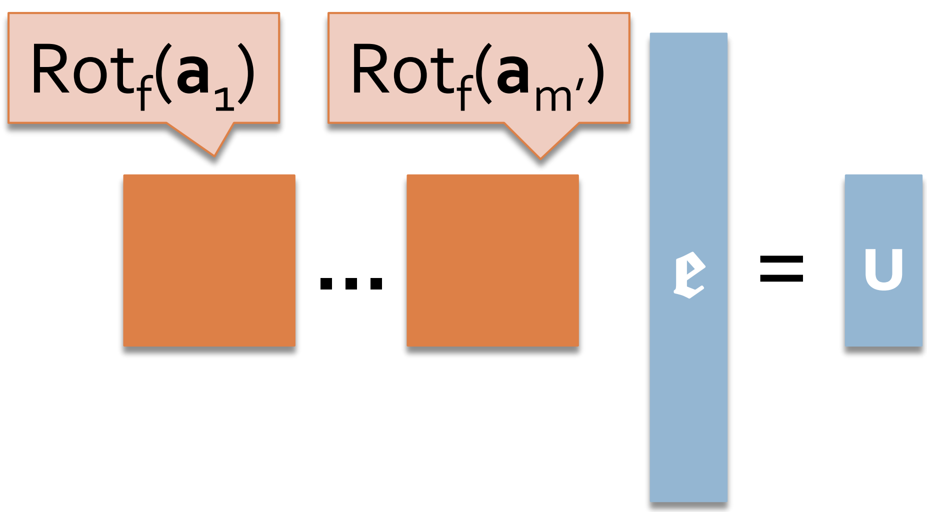
	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

イデアル格子ハッシュ [Mic07,LM06,PR06,PR07]

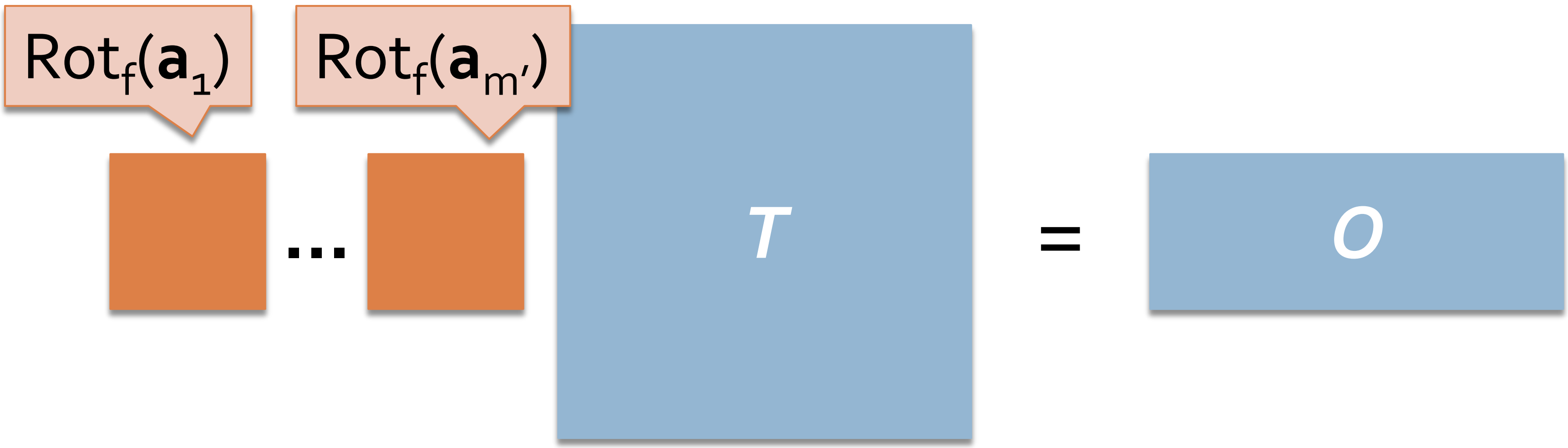
$$H_n = \{h_{\mathfrak{a}} : D_n \longrightarrow R_q \mid \mathfrak{a} \in R_q^m\}$$

$$h_{\mathfrak{a}}(\mathfrak{e}) = \mathfrak{a}\,\mathfrak{e} \bmod q = \Sigma_i\, \mathbf{a}_i \mathbf{e}_i$$

$$D_n = \{\mathfrak{e} \in R^m \mid \|\mathfrak{e}\| \le d\}$$



落とし戸 [SSTX09]



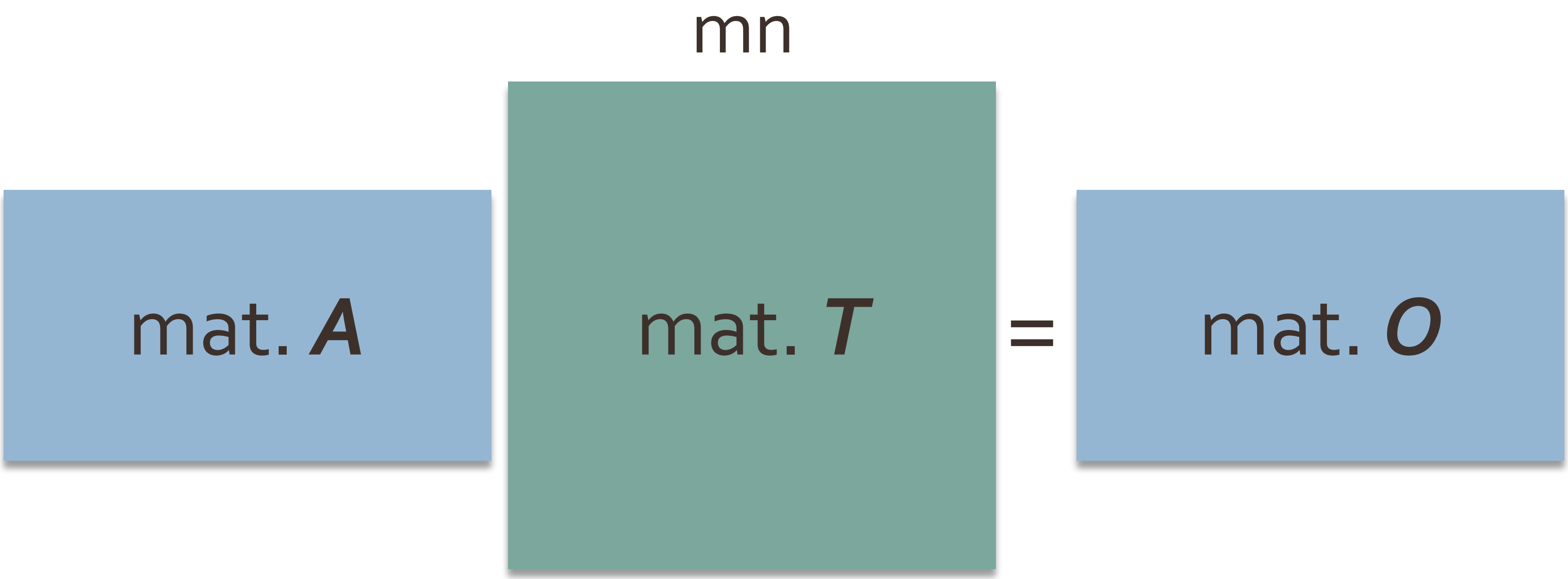
$$(\mathfrak{a} \in R_q^m, \boldsymbol{T}) \leftarrow \mathrm{Gen}(1^n)$$

$$\boldsymbol{T} \in \mathbb{Z}^{mn \times mn} \text{ s.t.}$$

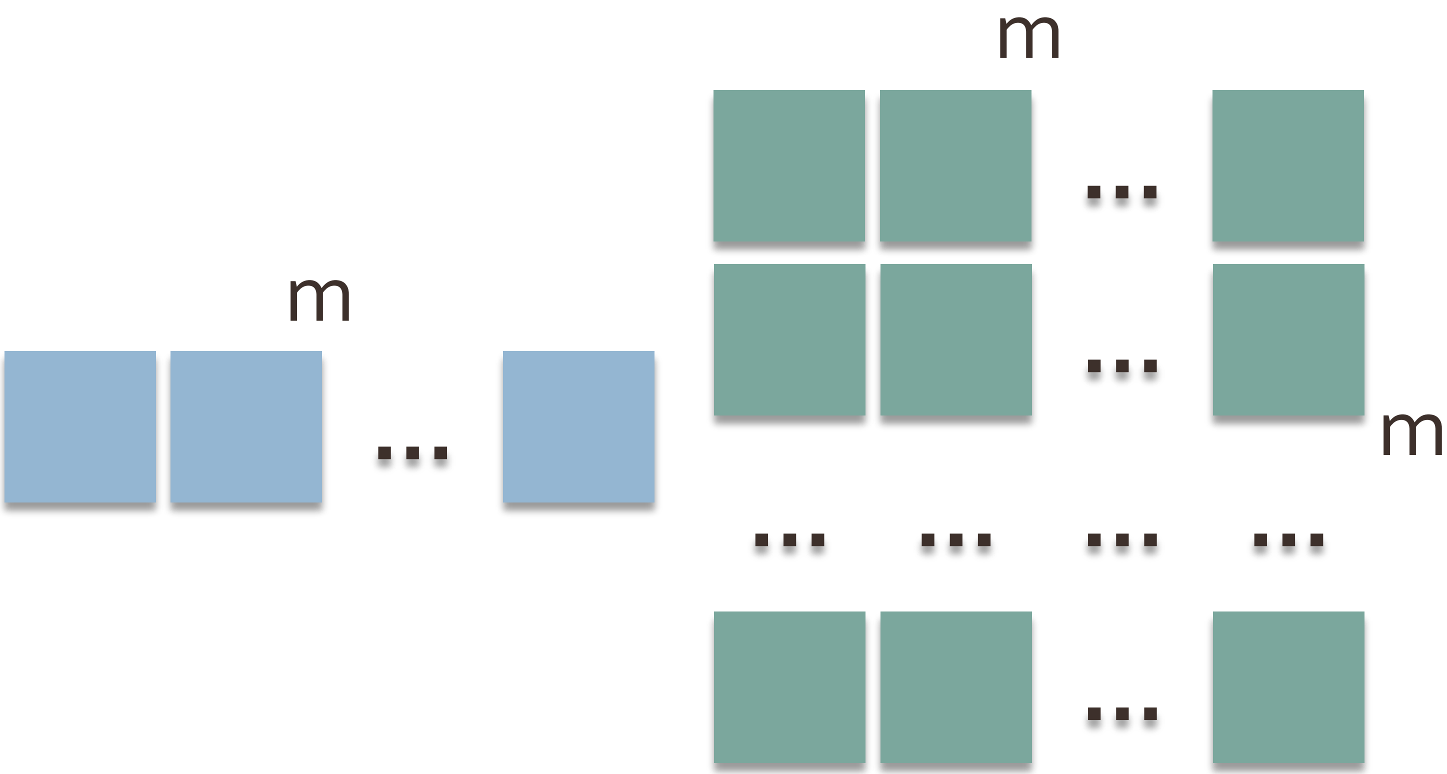
$$\boldsymbol{T}\text{:a basis of } \Lambda_q^{\perp}(\mathrm{Rot}(\mathfrak{a})),\ \|GS(\boldsymbol{T})\| \leqq L$$

注: $m=O(\log^2 q)$で$L=O(\sqrt{n}\log q)$
$m=O(\log q)$で$L=\tilde{O}(n \log q)$

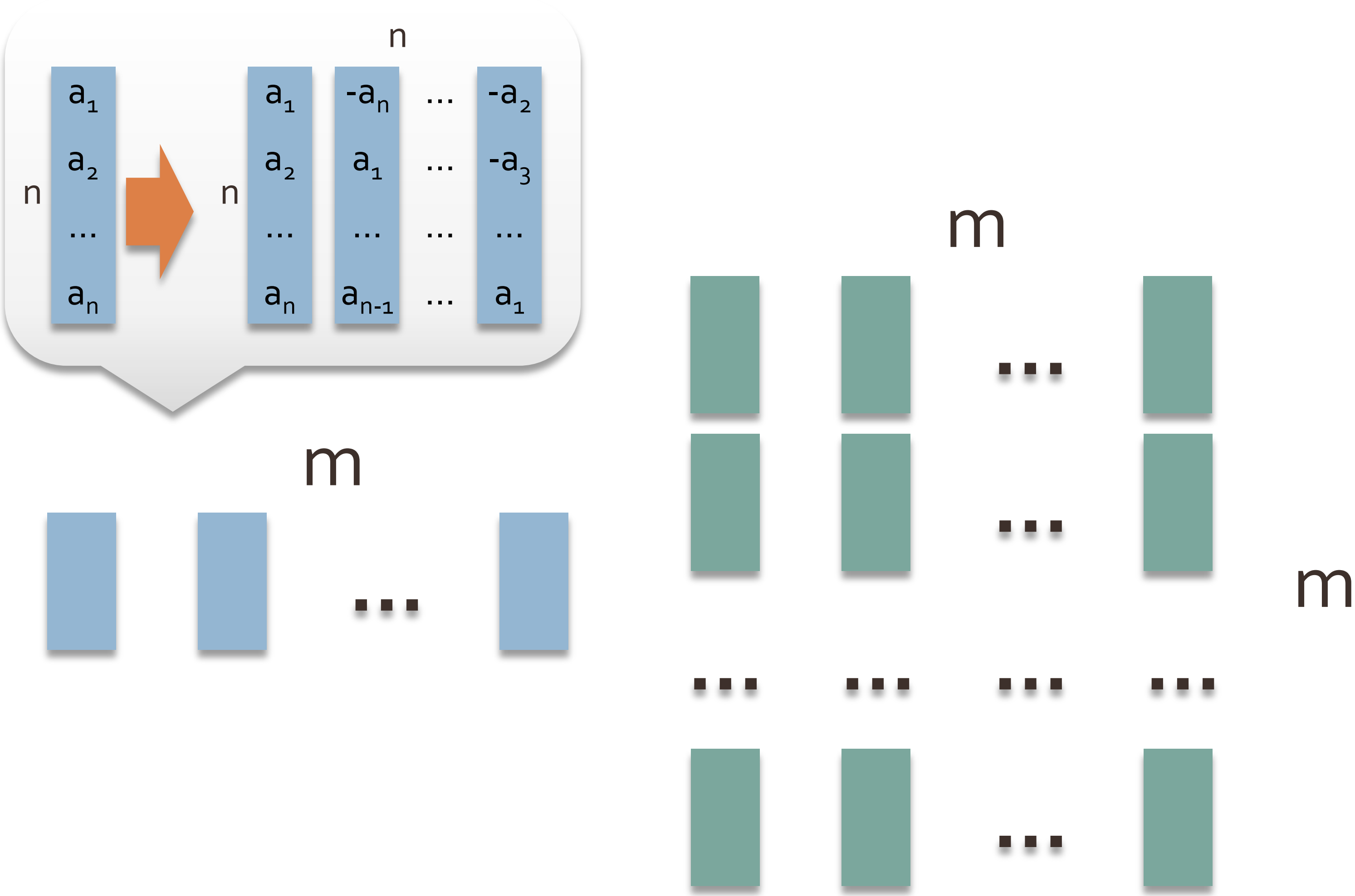
イデアル版鍵生成アルゴリズム [SSTX09]



イデアル版鍵生成アルゴリズム [SSTX09]



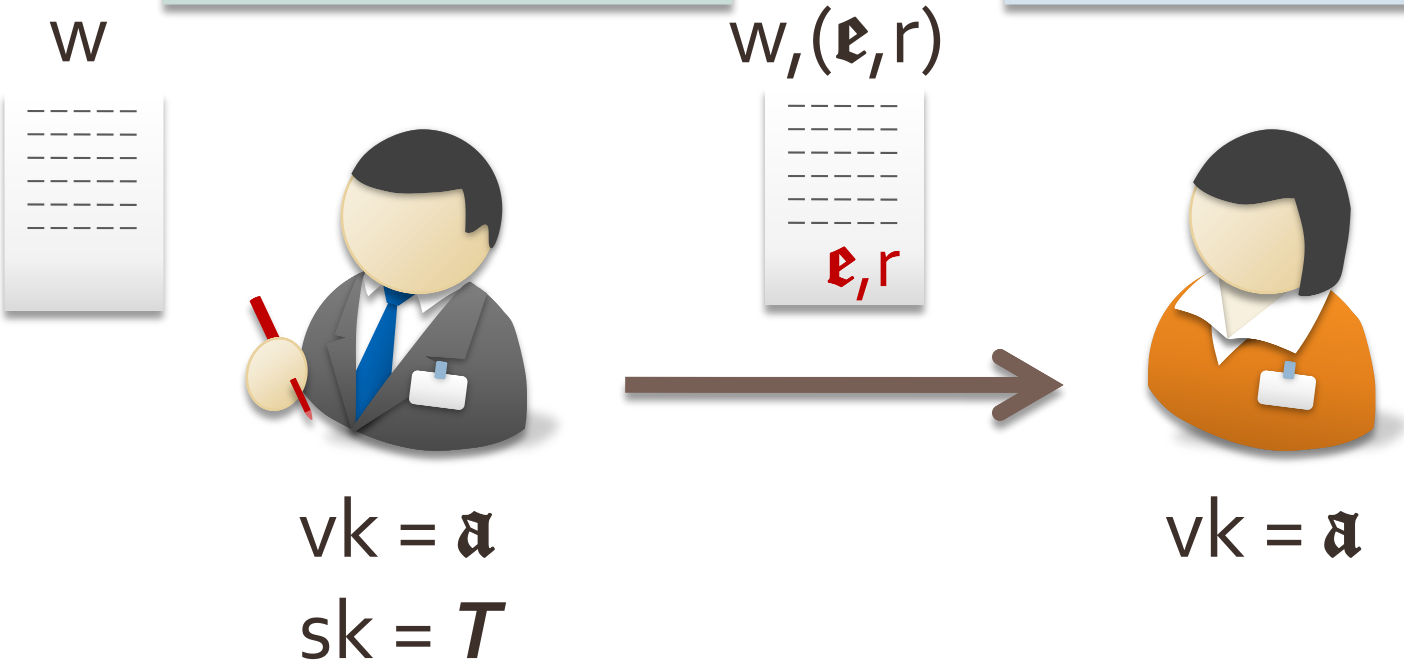
イデアル版鍵生成アルゴリズム [SSTX09]



SSTX署名 [SSTX09]

1. $\mathbf{u}=H(w||r)$
2. $\mathfrak{e}\leftarrow h_{\mathfrak{a}}^{-1}(\mathbf{u})$

1. $h_{\mathfrak{a}}(\mathfrak{e})=H(w||r)$
2. $||\mathfrak{e}|| \le s\sqrt{mn}$?



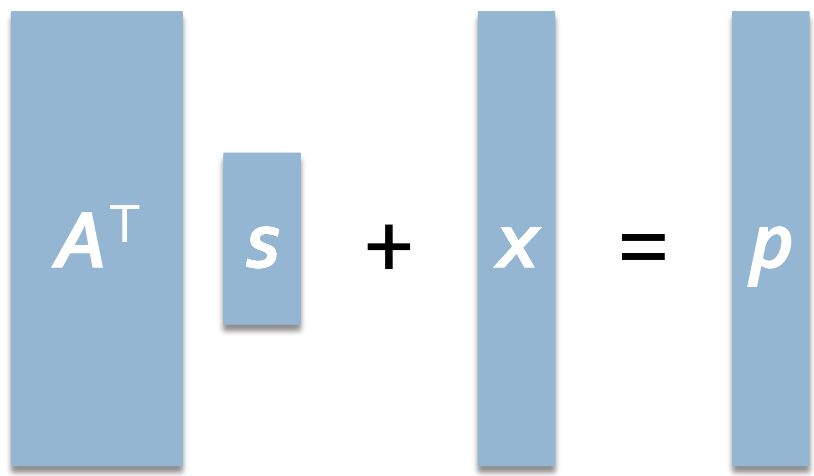
	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,...,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	**[GPV08,Pei09]**	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

LWE関数 [Reg09,GPV08,Pei09]

$$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m},\ \boldsymbol{s} \leftarrow \mathbb{Z}_q^n,\ \boldsymbol{x} \leftarrow \chi_\alpha^m$$

$$g_{\boldsymbol{A}}(\boldsymbol{s},\boldsymbol{x}) = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{x} \bmod q$$



$\mathrm{sLWE}_{q,\alpha}$

Find $\mathbf{s} \leftarrow \mathbb{Z}_q^n$

given $A_{\mathbf{s},\alpha} \rightarrow (\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + x)$

$A_{\mathbf{s},\alpha}$

Find **s**

$A_{\mathbf{s},\alpha}$

1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi_\alpha$
2. $b = \langle \mathbf{a}, \mathbf{s} \rangle + x$
3. Output $(\mathbf{a}, b)$

落とし戸 [Peio9?]

$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$, $\boldsymbol{x} \leftarrow \chi_\alpha^m$

$g_{\boldsymbol{A}}(\boldsymbol{s},\boldsymbol{x}) = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{x} \bmod q$

$\boldsymbol{T}$:a basis of $\Lambda_q^{\perp}(\mathbf{A})$

$\boldsymbol{d} = \boldsymbol{T}^{\mathrm{T}}\boldsymbol{p} \bmod q$ $(= \boldsymbol{T}^{\mathrm{T}}\boldsymbol{x} \bmod q)$

$\mathbf{c} = \boldsymbol{T}^{-\mathrm{T}}\,\boldsymbol{d}$ (in $\mathbb{Q}$) (= $\boldsymbol{x}$ with ow.prob)

Extract $\boldsymbol{s}$ from $\boldsymbol{v} = \boldsymbol{p} - \boldsymbol{c} = (\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} \bmod q)$

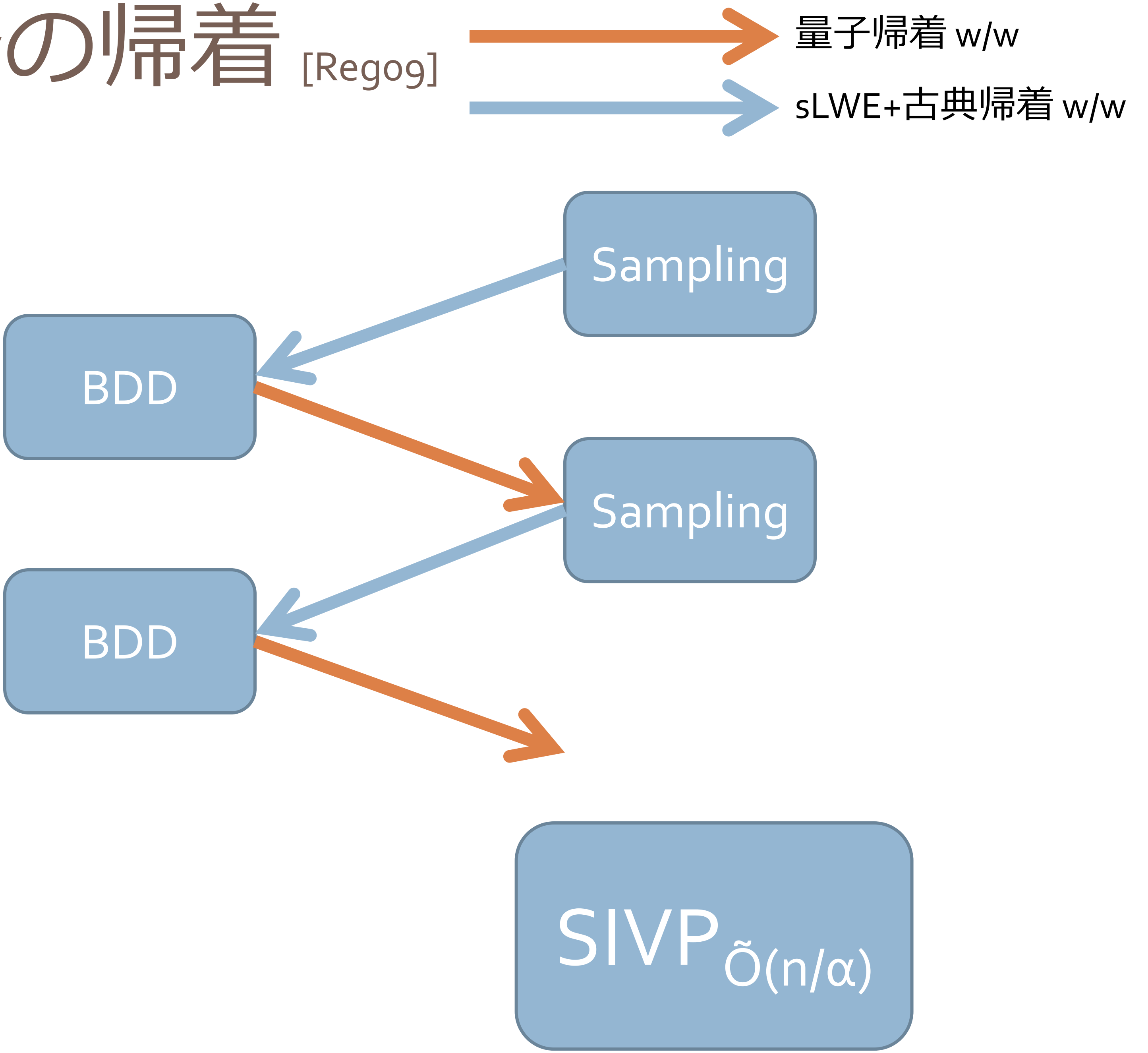
注: $|\langle \boldsymbol{t}_i, \boldsymbol{x}\rangle| \le La \le q/2 \Rightarrow a \le q/2L$なら$\boldsymbol{c}$の行が成立
$q \ge 5L\sqrt{m}$, $1/\alpha \le L\,\omega(\sqrt{\log n})$とする

追記: LWE関数 [Reg09,GPV08,Pei09]

$$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m},\ \boldsymbol{s} \leftarrow \mathbb{Z}_q^n,\ \boldsymbol{x} \leftarrow \chi_\alpha^m$$
$$g_{\boldsymbol{A}}(\boldsymbol{s},\boldsymbol{x}) = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{x} \bmod q$$

$$(\boldsymbol{A},\boldsymbol{p}) \sim_c (\boldsymbol{A},U(\mathbb{Z}_q^m))$$
も言える

Regevの帰着 [Reg09]



	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,…,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

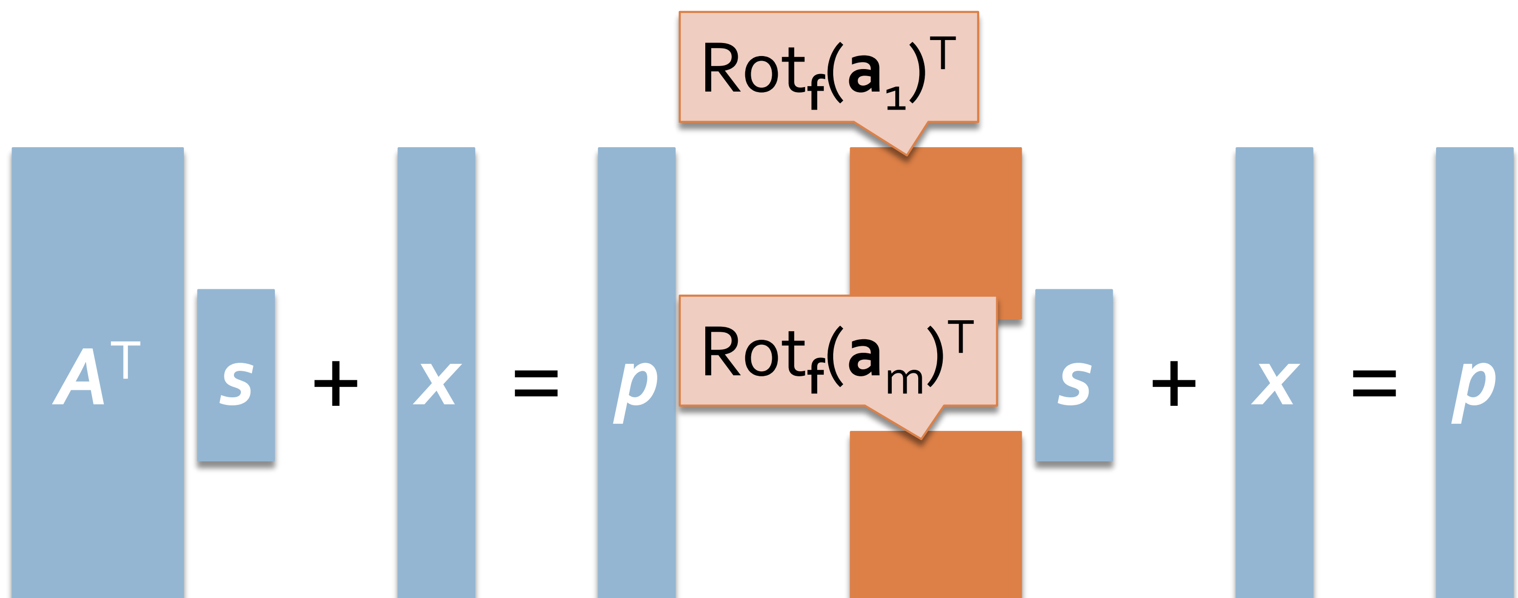
	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

イデアル格子版 $g_{\mathfrak{a}}(\boldsymbol{s}, \boldsymbol{x})$

$$\mathfrak{a} \in R_q^m,\ \boldsymbol{s} \leftarrow \mathbb{Z}_q^n,\ \boldsymbol{x} \leftarrow \chi_\alpha^{mn}$$

$$g_{\mathfrak{a}}(\boldsymbol{s},\boldsymbol{x}) = \boldsymbol{A}^{T}\boldsymbol{s} + \boldsymbol{x} \bmod q$$

$$\boldsymbol{A} = \mathrm{Rot}_{\mathbf{f}}(\mathfrak{a}) = [\mathrm{Rot}_{\mathbf{f}}(\mathbf{a}_1), \ldots, \mathrm{Rot}_{\mathbf{f}}(\mathbf{a}_m)]$$



$\mathbf{f}$-sLWE$_{q,\alpha}$

$\mathrm{Rot}_{\mathbf{f}}(\mathbf{a}_1)^T \; \boldsymbol{s} + \boldsymbol{x}$

Find $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$,

given $A_{\mathbf{s},\alpha} \rightarrow (\mathbf{a}, \mathrm{Rot}_{\mathbf{f}}(\mathbf{a})^T \boldsymbol{s} + \boldsymbol{x})$

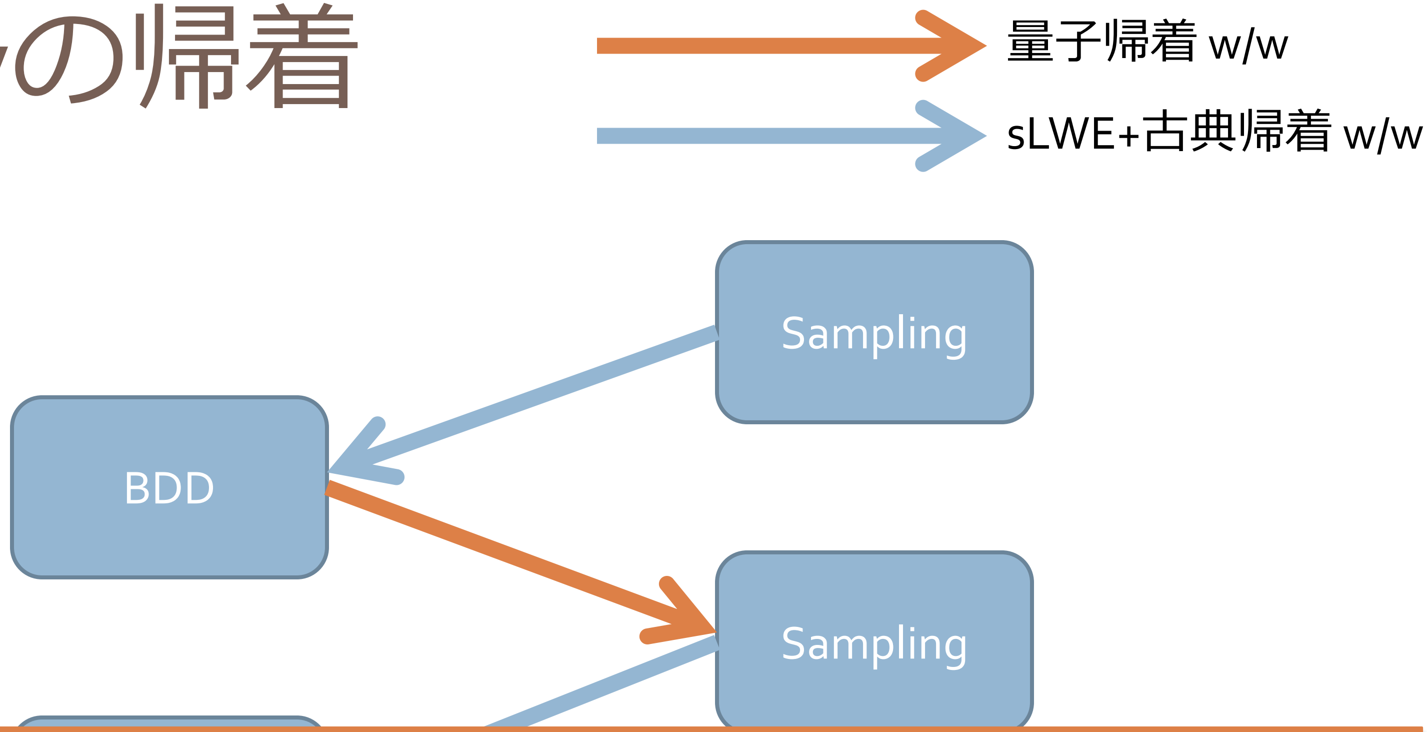
Find s

$A_{\mathbf{s},\alpha}$

$A_{\mathbf{s},\alpha}$

1. $\mathbf{a} \leftarrow R_q$, $\boldsymbol{x} \leftarrow \chi_\alpha^n$
2. $\boldsymbol{b} = \mathrm{Rot}_{\mathbf{f}}(\mathbf{a})^T \boldsymbol{s} + \boldsymbol{x}$
3. Output $(\mathbf{a}, \boldsymbol{b})$

Regevの帰着

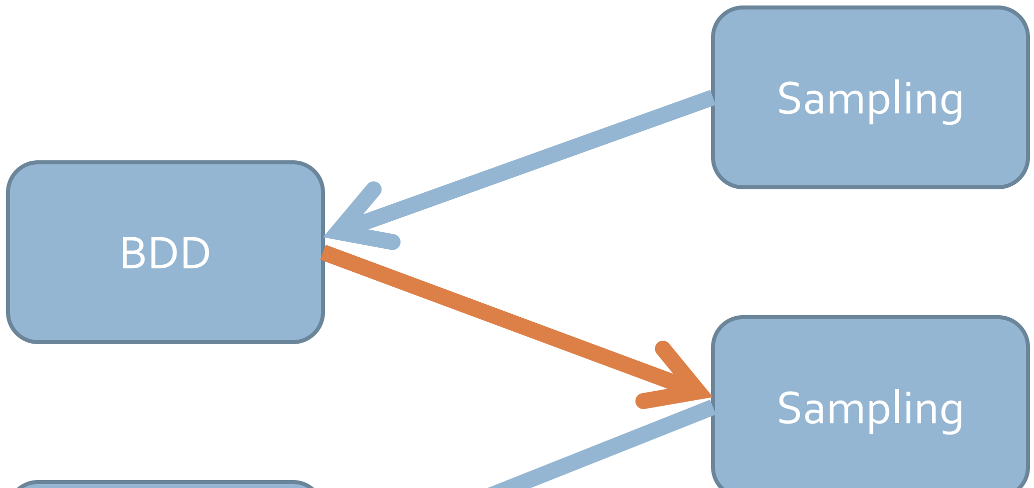


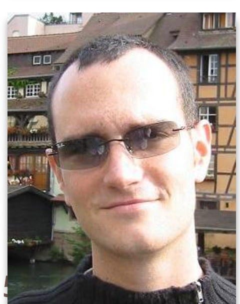
sLWE+古典帰着が
イデアル格子だと通らない

Regevの帰着

量子帰着 w/w

sLWE+古典帰着 w/w





sLWE+古典帰着を諦めて
量子帰着だけ使えばいいよ

[Reg09] の再解釈

→ 量子帰着 w/w

→ sLWE+古典帰着 w/w

BDD → Sampling

Given $\boldsymbol{B}$ of Λ^*,
If $R(\Lambda, \boldsymbol{p})$ finds $\boldsymbol{v}$ in Λ s.t. $\|\boldsymbol{v}-\boldsymbol{p}\| \leq d$,
$S^R(\boldsymbol{B})$ samples from $D_{\Lambda^*,s}$

$\Lambda = \Lambda_q(\boldsymbol{A})$とするとsLWEで$\boldsymbol{A}^T\boldsymbol{s}$が分かる
$(\Lambda_q(\boldsymbol{A}))^* = (1/q)\, \Lambda_q^{\perp}(\boldsymbol{A})$ の短いベクトルが分かる
$\Rightarrow SIS_{q,m,\beta}$が解ける

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,...,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

LWE-TDFs based KEM [Pei09]

1. $\boldsymbol{s} \leftarrow \boldsymbol{p}$
2. $\boldsymbol{k} \leftarrow \boldsymbol{c} - \boldsymbol{v}$

1. $\boldsymbol{p} = g_{\boldsymbol{A}}(\boldsymbol{s}, \boldsymbol{x})$
2. $\boldsymbol{v} = g_{\boldsymbol{U}}(\boldsymbol{s}, \boldsymbol{x}')$
3. $\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{k}q/2$

$(\boldsymbol{p}, \boldsymbol{c})$

ek = $(\boldsymbol{A}, \boldsymbol{U})$
dk = $\boldsymbol{T}$

ek = $(\boldsymbol{A}, \boldsymbol{U})$

$(\boldsymbol{A}, \boldsymbol{p}) \sim_c (\boldsymbol{A}, \mathrm{U}(\mathbb{Z}_q^m))$を利用

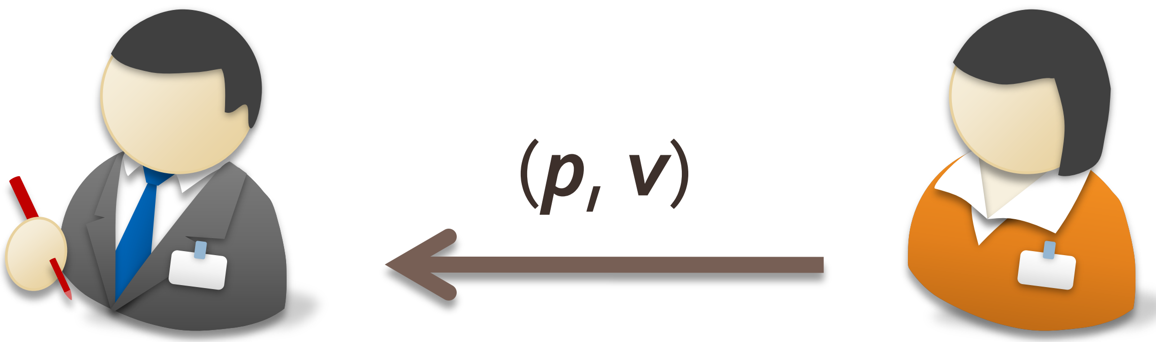
	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,…,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔

f-sLWE-TDFs based PKE [SSTX09]

1. $\boldsymbol{s} \leftarrow \boldsymbol{p}$
2. $\boldsymbol{w} \leftarrow \boldsymbol{v} \oplus \mathrm{H}(\boldsymbol{s})$

1. $\boldsymbol{p} = \mathrm{g}_{\mathfrak{a}}(\boldsymbol{s}, \boldsymbol{x})$
2. $\boldsymbol{v} = \boldsymbol{w} \oplus \mathrm{H}(\boldsymbol{s})$



ek = $\mathfrak{a}$

dk = $\boldsymbol{T}$

ek = $\mathfrak{a}$

注: $(\mathfrak{a}, \boldsymbol{p}) \sim_c (\mathfrak{a}, \mathrm{U}(\mathbb{Z}_q^m))$ は不明

まとめ – 色々やった

	Hash	ID	CR-PSFs	Sig (w/ ROM)
一般	[Ajt97,…,MR07, GPV08]	[MV03,Lyu08, KTX08]	[GPV08]	[GPV08]
イデアル	[Mic04,LM06, PR06]	[Lyu08,KTX08, Lyu09]	✔	✔

	OW-TDFs	PKE, IBE HIBE	IBI	Sig (w/o ROM)
一般	[GPV08,Pei09]	[Reg05,GPV08, Pei09,CHKP10]	✔	[CHKP10]
イデアル	✔	✔	✔	✔