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？

<table>
<thead>
<tr>
<th></th>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,...,MR07, GPVo8]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mico4,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>OW-TDFs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8,Peio9]</td>
<td>[Reg05,GPVo8, Peio9,CHKP10]</td>
<td>✔</td>
<td>[CHKP10]</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
説明は？

<table>
<thead>
<tr>
<th></th>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,...,MRo7, GPVo8]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアール</td>
<td>[Mico4,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE, HIBE</td>
<td>IBI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8,Peio9]</td>
<td>[Reg05,GPVo8, Peio9,CHKP10]</td>
<td>✔️</td>
<td>[CHKP10]</td>
</tr>
<tr>
<td>イデアール</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
格子

- $B = [b_1, \ldots, b_n] \in \mathbb{Q}^{n \times n}$
- $L(B) := \{ \Sigma_i \alpha_i b_i \mid \alpha_i \in \mathbb{Z} \text{ for all } i \} \subseteq \mathbb{Q}^n$
- $\lambda(\Lambda) : \Lambda$中の最短ベクトルの長さ
格子定数2

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

\[ B = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \]
双対格子

- \( B = [b_1, \ldots, b_n] \in \mathbb{Q}^{n \times n} \)
- \( L(B) := \{ \sum_i \alpha_i b_i \mid \alpha_i \in \mathbb{Z} \text{ for all } i \} \subseteq \mathbb{Q}^n \)
- \( \Lambda^* = \{ x \mid \langle x, v \rangle \in \mathbb{Z} \text{ for all } v \text{ in } \Lambda \} \)
- \( \Lambda^* = L(B^{-T}) \)
双対格子: 例

\[ B = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \]

\[ B^{-1} = \begin{pmatrix} -1/2 & 1/2 \\ 1 & 0 \end{pmatrix} \]

\[ B^{\top} = \begin{pmatrix} -1/2 & 1 \\ 1/2 & 0 \end{pmatrix} \]
双対格子: 例

\[ B = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \]

\[ B^{-1} = \begin{pmatrix} -1/2 & 1/2 \\ 1 & 0 \end{pmatrix} \]

\[ B^{-T} = \begin{pmatrix} -1/2 & 1 \\ 1/2 & 0 \end{pmatrix} \]
特殊な格子

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

- $\Lambda_q^\perp(A) = \{ e \in \mathbb{Z}_m^m | Ae = 0 \bmod q \}$
- $\Lambda_q(A) = \{ y \in \mathbb{Z}_m^m | y = A^T s \bmod q \}$
For $A \in \mathbb{Z}_q^{n \times m}$

- $\Lambda_q^\perp (A) = \{ e \in \mathbb{Z}_q^m \mid Ae = o \ \text{mod} \ q \}$
- $\Lambda_q (A) = \{ y \in \mathbb{Z}_q^m \mid y = A^T s \ \text{mod} \ q \}$

$$(\Lambda_q (A))^* = (1/q) \Lambda_q^\perp (A)$$
Given $B$ of $\Lambda$
find $v \in \Lambda - \{0\}$ s.t. $\|v\| = \lambda(\Lambda)$
近似版最短ベクトル問題 (SVP$_\gamma$)

Given $B$ of $\Lambda$, find $v \in \Lambda - \{o\}$ s.t. $\|v\| \leq \gamma \lambda(\Lambda)$
近似版最短線形独立ベクトル集合問題（SIVPγ）

Given $B$ of $\Lambda$, find $S \subseteq \Lambda$ s.t. $\|S\| \leq \gamma \lambda_n(\Lambda)$
<table>
<thead>
<tr>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE HIBE</td>
<td>IBI</td>
<td>Sig (w/o ROM)</td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8, Pei09]</td>
<td>[Reg05, GPVo8, Pei09, CHKP10]</td>
<td>✔️</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97, ..., MR07, GPVo8]</td>
<td>[MV03, Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04, LMo6, PR06]</td>
<td>[Lyu08, KTXo8, Lyu09]</td>
<td>✔️</td>
</tr>
</tbody>
</table>
格子ハッシュ [Ajt96,...,MR07,GPV08]

\[ H_n = \{ h_A : D_n \to \mathbb{Z}_q^n \mid A \in \mathbb{Z}_q^{n \times m} \} \]

\[ h_A(e) = A e \mod q \]

\[ D_n = \{ e \in \mathbb{Z}_m^m \mid ||e|| \leq d \} \]
短い整数解問題 (SIS_{q,m,\beta})

Given \( A \leftarrow \mathbb{Z}_q^{n \times m} \),
find \( e \in \mathbb{Z}^m \) s.t. \( ||e|| \leq \beta \), \( Ae = 0 \mod q \)

格子\( \Lambda_{q}^{\perp}(A) \)の
短い非ゼロベクトルを
探索
Col(H) ≥ SIS_{q,m,2d} \quad [GGH96]

\[ H_n = \{ h_A : D_n \rightarrow \mathbb{Z}_q^n | A \in \mathbb{Z}_q^{n \times m} \} \]
\[ h_A(e) = Ae \mod q \]
\[ D_n = \{ e \in \mathbb{Z}_q^m | \|e\| \leq d \} \]

Given \( A \leftarrow \mathbb{Z}_q^{n \times m} \),
find \( e \in \mathbb{Z}_q^m \) s.t. \( \|e\| \leq \beta \), \( Ae = 0 \mod q \)
Given $A \leftarrow \mathbb{Z}_q^{n \times m}$, find $e \in \mathbb{Z}_m^m$ s.t. $\|e\| \leq \beta$, $Ae = 0 \mod q$

Given $B$ of $\Lambda$, find $S \subseteq \Lambda$ s.t. $\|S\| \leq \gamma \lambda_n(\Lambda)$
<table>
<thead>
<tr>
<th></th>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97, ..., MR07, GPVo8]</td>
<td>[MVo3, Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04, LM06, PR06]</td>
<td>[Lyu08, KTXo8, Lyu09]</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE</td>
<td>HIBE</td>
<td>IBI</td>
<td>Sig (w/o ROM)</td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8, Pei09]</td>
<td>[Reg05, GPVo8, Pei09, CHKP10]</td>
<td>✔️</td>
<td>[CHKP10]</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
イデアル格子版の準備

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

\[ x(x) = 1+x+x^3 \quad \longleftrightarrow \quad \text{Rot}_f(x) = \begin{pmatrix} 1 & -1 & 0 & -1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \]

\[ y(x) = 1+2x^2 \quad \longleftrightarrow \quad \text{Rot}_f(y) = \begin{pmatrix} 0 & 0 & -2 & -1 \\ 1 & 0 & 0 & -2 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \end{pmatrix} \]

\[ x \otimes y = -1-3x+3x^2+2x^3 \quad \longleftrightarrow \quad \text{Rot}_f(x) \text{Rot}_f(y) = \begin{pmatrix} -1 & -2 & -3 & 3 \\ -3 & -1 & -2 & -3 \\ 3 & -3 & -1 & -2 \\ 2 & 3 & -3 & -1 \end{pmatrix} \]
イデアル格子とイデアル格子問題

\[ R = \mathbb{Z}[x]/\langle f \rangle, \quad \text{e.g.,} \quad f = x^{n+1} \]
\[ I \subseteq R \iff \Lambda_I \subseteq \mathbb{Z}^n \]

\( f \)-SVP\(_\gamma\):

Given \( B \) of \( \Lambda_I \),

find \( \mathbf{v} \in \Lambda_I - \{ \mathbf{0} \} \) s.t.
\[ \|\mathbf{v}\| \leq \gamma \lambda(\Lambda_I) \]
イデアル格子ハッシュ [Mic07, LMo6, PR06, PR07]

\[ H_n = \{ h_\alpha : D_n \to R_q \mid \alpha \in R^m_q \} \]

\[ h_\alpha(e) = \alpha \cdot e \mod q = \sum_i a_i e_i \]

\[ D_n = \{ e \in R^m \mid \| e \| \leq d \} \]

\[ \text{Rot}_f(a_1) \quad \text{Rot}_f(a_m) \]

\[ e = U \]
\( \text{f-Col}(H) \geq \text{f-SIS}_{q,m,2d} \)

\[
H_n = \{ h_a : D_n \rightarrow R_q \mid a \in R_q^m \}
\]

\[ h_a(e) = a \cdot e \mod q = \sum_i a_i e_i \]

\[ D_n = \{ e \in R^m \mid \|e\| \leq d \} \]

Given \( a \leftarrow R_q^m \),
find \( e \in R^m \) s.t. \( \|e\| \leq \beta \), \( a \cdot e = 0 \mod q \)
Given \( \mathbf{a} \leftarrow R_q^m \),
find \( \mathbf{e} \in R^m \) s.t. \( ||\mathbf{e}|| \leq \beta \), \( \mathbf{a} \mathbf{e} = \mathbf{0} \mod q \)

**f-SVP**

**f-SVP** \( _{\gamma} \):
Given \( \mathbf{B} \) of \( \Lambda_1 \),
find \( \mathbf{v} \in \Lambda_1 - \{\mathbf{0}\} \) s.t. \( ||\mathbf{v}|| \leq \gamma \lambda(\Lambda_1) \)

注：\( f\text{-SIS}_{q,m,\beta} \geq_{a/w} f\text{-SVP} \tilde{O}(\beta) \)
<table>
<thead>
<tr>
<th>Hash ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97, MRo7, GPVo8]</td>
<td>[MVo3, Lyuo8, KTXo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04, LMo6, PRo6]</td>
<td>[Lyuo8, KTXo8, Lyuo9]</td>
</tr>
</tbody>
</table>

### OW-TDFs

<table>
<thead>
<tr>
<th>OW-TDFs</th>
<th>PKE, IBE</th>
<th>IBI</th>
<th>Sig (w/o ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[GPVo8, Peio9]</td>
<td>[Reg05, GPVo8, Peio9, CHKP10]</td>
<td>✔</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hash ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
格子ハッシュ  [Ajt96,...,MR07,GPV08]

\[ H_n = \{ h_A : D_n \rightarrow \mathbb{Z}_q^n \mid A \in \mathbb{Z}_q^{n \times m} \} \]
\[ h_A(e) = A e \mod q \]
\[ D_n = \{ e \in \mathbb{Z}_m^m \mid ||e|| \leq d \} \]
(A, T)←Gen(1^n)

T ∈ ℤ^{m×m} s.t.

T: a basis of Λ_q^⊥(A), ||GS(T)|| ≤ L

注: L = Õ(√n log q)
落とし戸 [Ajt99, GPVo8, APo9]

\[ H_n = \{ h_A : D_n \rightarrow \mathbb{Z}_q^n \mid A \in \mathbb{Z}_q^{n \times m} \} \]
\[ h_A(e) = Ae \mod q \]
\[ D_n = \{ e \in \mathbb{Z}_q^m \mid ||e|| \leq d \} \]

注: \( L = \Omega(\sqrt{n \log q}) \)

\( T \)があれば、
\( h_A(e) = u \)になる \( e \)を取りれる
(ただし \( ||e|| \leq L \sqrt{m} \cdot \omega(\sqrt{\log m}) \))
ガウス分布

□ ガウス分布関数:

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

□ 離散ガウス分布関数:

\[ D_{\Lambda,s,c}(x) = \nu_{s,c}(x)/\nu_{s,c}(\Lambda) \]

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

\[ \Pr_{x \leftarrow D[\| x \| > s \sqrt{n}]} < \text{negl}(n) \]
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
$D_{L,3}$
Klein-GPV Sampling [Kle01?, GPV08, Pei10]

$T$: a basis of $\Lambda$, $||GS(T)|| \leq L$, 
$s \geq L \omega(\sqrt{\log n})$, 
$\Rightarrow \text{SampleD}(T, s, c) \sim_s D_{\Lambda, s, c}$
Klein-GPV Sampling [Kleo1?, GPV08, Pei10]

\( T \): a basis of \( \Lambda \), \( \| \text{GS}(T) \| \leq L \), 
\( s \geq L \omega(\sqrt{\log n}) \),
\( \Rightarrow \text{SampleD}(T, s, c) \sim_S D_{\Lambda, s, c} \)

\[ (A, T) \leftarrow \text{Gen}(1^n) \]
\[ T \in \mathbb{Z}^{m \times m} \text{ s.t. } \]
\[ T: \text{a basis of } \Lambda_q^\perp(A), \| \text{GS}(T) \| \leq L \]

注: \( L = O(\sqrt{n \log q}) \)
**Klein-GPV Sampling** [Kle01?, GPV08, Pei10]

\[ T: \text{a basis of } \Lambda, \| \text{GS}(T) \| \leq L, \]
\[ s \geq L \omega(\sqrt{\log n}), \]
\[ \Rightarrow \text{SampleD}(T, s, c) \sim S D_{\Lambda, s, c} \]

注: \( L = \tilde{O}(\sqrt{n \log q}) \)

\[ T \text{があれば,} \]
\[ h_A(e) = u \text{になる} e \text{を取れる} \]
\[ (\text{ただし} \| e \| \leq s \sqrt{m}, s = L \omega(\sqrt{\log m})) \]
GPV署名 [GPV08]

1. \( u = H(w || r) \)
2. \( e \leftarrow h_A^{-1}(u) \)

1. \( h_A(e) = H(w || r) \)
2. \( \|e\| \leq s \sqrt{m} \)?

\( \text{vk} = A \)
\( \text{sk} = T \)
<table>
<thead>
<tr>
<th></th>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,...,MRo7, GPVo8]</td>
<td>[MV03,Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE</td>
<td>HIBE</td>
<td>IBI</td>
<td>Sig (w/o ROM)</td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8,Peio9]</td>
<td>[Reg05,GPVo8, Peio9,CHKP10]</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
イデアル格子ハッシュ [Mico7,LMo6,PRo6,PRo7]

\[ H_n = \{ h_a : D_n \rightarrow R_q \mid a \in R_q^m \} \]

\[ h_a(e) = a \cdot e \mod q = \sum_i a_i e_i \]

\[ D_n = \{ e \in R_m \mid ||e|| \leq d \} \]
落とし戸 [SSTX09]

ロットフ(d₁)  ロットフ(dₘ')

\[ T \in \mathbb{Z}_{mn}^{mn} \text{ s.t.} \]

\[ T: \text{a basis of } \Lambda_q^\perp(\text{Rot}(a)) \text{, } \|\text{GS}(T)\| \leq L \]

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

\( m=O(\log q) \text{ で } L=\tilde{O}(n \log q) \)
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]
1. $u = H(w || r)$
2. $e \leftarrow h_{a^{-1}}(u)$

1. $h_a(e) = H(w || r)$
2. $||e|| \leq s \sqrt{mn}$?
<table>
<thead>
<tr>
<th>Hash ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,...,MR07, GPVo8]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
</tr>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE HIBE</td>
<td>IBI</td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8,Peio9]</td>
<td>[Rego5,GPVo8, Peio9,CHKP10]</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
LWE function \([\text{Reg09, GPVo8, Pei09}]\)

\[
A \in \mathbb{Z}_{q}^{n \times m}, \quad s \leftarrow \mathbb{Z}_{q}^{n}, \quad x \leftarrow \chi_{\alpha}^{m}
\]

\[
g_{A}(s, x) = A^{T}s + x \mod q
\]

\[
 A^{T} \quad s \quad + \quad x \quad = \quad p
\]
Find $s \leftarrow \mathbb{Z}_q^n$
given $A_{s,\alpha} \rightarrow (a, <a,s> + x)$
\[ A \in \mathbb{Z}_q^{n \times m}, \ s \leftarrow \mathbb{Z}_q^n, \ x \leftarrow \chi_\alpha^m \]
\[ g_A(s, x) = A^T s + x \mod q \]
\[ T: \text{a basis of } \Lambda_{q}^\perp(A) \]

\[ d = T^T p \mod q \ (= T^T x \mod q) \]
\[ c = T^{-T} d \ (\text{in } \mathbb{Q}) \ (= x \text{ with ow.prob}) \]
\[ \text{Extract } s \text{ from } \nu = p - c = (A^T s \mod q) \]

注: \[ |\langle t, x \rangle| \leq L\alpha \leq q/2 \Rightarrow a \leq q/2L \]なら \( c \)の行が成立
\[ q \geq 5L\sqrt{m}, \ 1/\alpha \leq L \ \omega(\sqrt{\log n}) \]とする
追記: LWE関数 [Reg09, GPVo8, Peio9]

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

\[ g_A(s, x) = A^T s + x \mod q \]

\[(A, p) \sim c (A, U(\mathbb{Z}_q^m)) \]

も言える
Regevの帰着 [Reg09]

量子帰着 w/w
sLWE+古典帰着 w/w

BDD → Sampling
BDD → Sampling

SIVP $\tilde{O}(n/\alpha)$
<table>
<thead>
<tr>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,...,MR07, GPVo8]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mico4,LMo6, PR06]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OW-TDFs</th>
<th>PKE, IBE</th>
<th>HIBE</th>
<th>IBI</th>
<th>Sig (w/o ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[GPVo8,Pei09]</td>
<td>[Reg05,GPVo8, Pei09,CHKP10]</td>
<td>✔</td>
<td>[CHKP10]</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
イデアル格子版 $g_a(s, x)$

\[
a \in \mathbb{R}_q^m, s \leftarrow \mathbb{Z}_q^n, x \leftarrow \chi_\alpha^{mn}
\]

\[
g_a(s, x) = A^T s + x \mod q
\]

\[
A = \text{Rot}_f(a) = [\text{Rot}_f(a_1), \ldots, \text{Rot}_f(a_m)]
\]
Find $s \leftarrow \mathbb{Z}_q^n$, given $A_{s,\alpha} \rightarrow (a, \text{Rot}_f(a)^T s + x)$

1. $a \leftarrow R_q$, $x \leftarrow \chi_\alpha^n$
2. $b = \text{Rot}_f(a)^T s + x$
3. Output $(a, b)$
Regevの帰着

量子帰着 w/w
sLWE+古典帰着 w/w

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

$\Lambda = \Lambda_q(A)$とするととsLWEで$A^T s$が分かる
$(\Lambda_q(A))^* = (1/q) \Lambda_q(A)$の短いベクトルが分かる
$\Rightarrow SIS_{q, m, \beta}$が解ける
<table>
<thead>
<tr>
<th></th>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,…,MRo7, GPVo8]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mico4,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE, HIBE</td>
<td>IBI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>一般</td>
<td>[GPVo8,Peio9]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LWE-TDFs based KEM [Peio9]

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

1. $p = g_A(s, x)$
2. $v = g_U(s, x')$
3. $c = v + kq/2$

$(p, c)$

$ek = (A, U)$
$dk = T$

$(A, p) \sim c (A, U(Z_q^m))$を利用
<table>
<thead>
<tr>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,...,MRo7, GPV08]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
<td>[GPV08]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔</td>
</tr>
<tr>
<td>OW-TDFs</td>
<td>PKE, IBE</td>
<td>HIBE</td>
<td>IBI</td>
</tr>
<tr>
<td>一般</td>
<td>[GPV08,Peio9]</td>
<td>[Rego5,GPV08, Peio9,CHKP10]</td>
<td>✔</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
f-sLWE-TDFs based PKE [SSTX09]

1. $s \leftarrow p$
2. $w \leftarrow v \oplus H(s)$

$ek = a$
$dk = T$

$1. p = g_a(s, x)$
$2. v = w \oplus H(s)$

$(p, v)$

Note: $(a, p) \sim c (a, U(\mathbb{Z}_q^m))$ is unknown
まとめ - 色々やった

<table>
<thead>
<tr>
<th></th>
<th>Hash</th>
<th>ID</th>
<th>CR-PSFs</th>
<th>Sig (w/ ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[Ajt97,…,MRo7, GPVo8]</td>
<td>[MVo3,Lyu08, KTXo8]</td>
<td>[GPVo8]</td>
<td>[GPVo8]</td>
</tr>
<tr>
<td>イデアル</td>
<td>[Mic04,LMo6, PRo6]</td>
<td>[Lyu08,KTXo8, Lyu09]</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>OW-TDFs</th>
<th>PKE, IBE</th>
<th>IBI</th>
<th>Sig (w/o ROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般</td>
<td>[GPVo8,Pei09]</td>
<td>[Reg05,GPVo8, Pei09,CHKP10]</td>
<td>✔️</td>
<td>[CHKP10]</td>
</tr>
<tr>
<td>イデアル</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>