イデアル版LWE仮定に基づくIND-CCA2安全な暗号方式

2009/01/24
[SCIS 2009 4A2-5]

草川恵太/田中圭介（東京工業大学）

最近の格子暗号業界 #1

- [LMPR08] SWIFFT (FSE2008)
- [LM08] One-time Sig from f-SVP (TCC2008)
- [PSW08] GGH Sigの改良 (PKC2008)
- [Lyu08a] ID from GapSVP (PKC2008)
- [PW08] IND-CCA2 PKE from LWE(STOC2008)
- [GPV08] Sig from GapSVP, IBE from LWE (STOC08)
- [PVW08] UCOT from LWE (CRYPTO2008)
- [PV08] NISZK for lattice problems (CRYPTO2008)

最近の格子暗号業界 #2

- [ADL+08] SWIFFTX (SHA-3)
- [GV08] IND-CCA2 PKE from LWE (Personal Com.)
- [Pei08] IND-CCA2 PKE from GapSVP (ePrint2008)
- [Lyu08b] uSVP ≧ LWE (≧ GapSVP) (ePrint2008)
- [KTX08] ID from GapSVP (ASIACRYPTO2008)
- [MR08] Survey (Book:PQC)
- [AGV09] Hardcore function for LWE (TCC2009)

格子暗号とIND-CCA2

- 標準モデルでIND-CCA2な格子暗号
  - Peikert and Waters [PW08]
  - Lossy trapdoor functionによる構成

- 2008年11月頃
  - Peikert [Pei08]
  - Goldwasser and Vaikuntanathan [GV08]

  - ともにRosen and Segev [RS09]に基づく構成

動機

- [PWo8], [Peio8], [GVo8]は一般の格子問題ベース
  - $|pk| = \tilde{O}(n^3)$

イデアル格子問題ベースにしよう

目標: $|pk| = \tilde{O}(n^2)$

[Pei08,GV08]の方針

- Rosen and Segev [RS09]の構成を利用
- Correlated Product TDFs + One-time Sig

  ⇒IND-CCA2PKE
- Correlated Product TDFs
  - g_{ai}(・)はTDF
  - k個並べてf(s)=(g_{a1}(s),g_{a2}(s),…,g_{ak}(s))も一方向

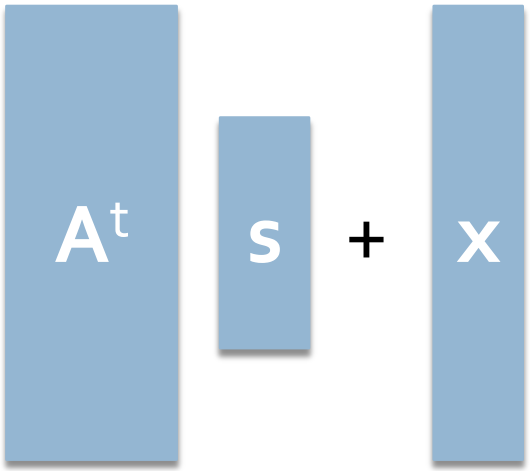
格子ベースのCorrelated product TDFs

LWE

- $LWE_{q,\chi}$
  - $A_{\mathbf{s},\chi}$
    - 1. $\mathbf{a} \longleftarrow \mathbb{Z}_q^n$, $x \longleftarrow \chi$
    - 2. output $(\mathbf{a}, \mathbf{a}^t \mathbf{s} + x)$
  - $A_{\mathbf{s},\chi}$からのサンプルを見ても, **s**が求められない

- サンプルをm個並べてみると

  $(\mathbf{A}, \mathbf{A}^t \mathbf{s} + \mathbf{x})$



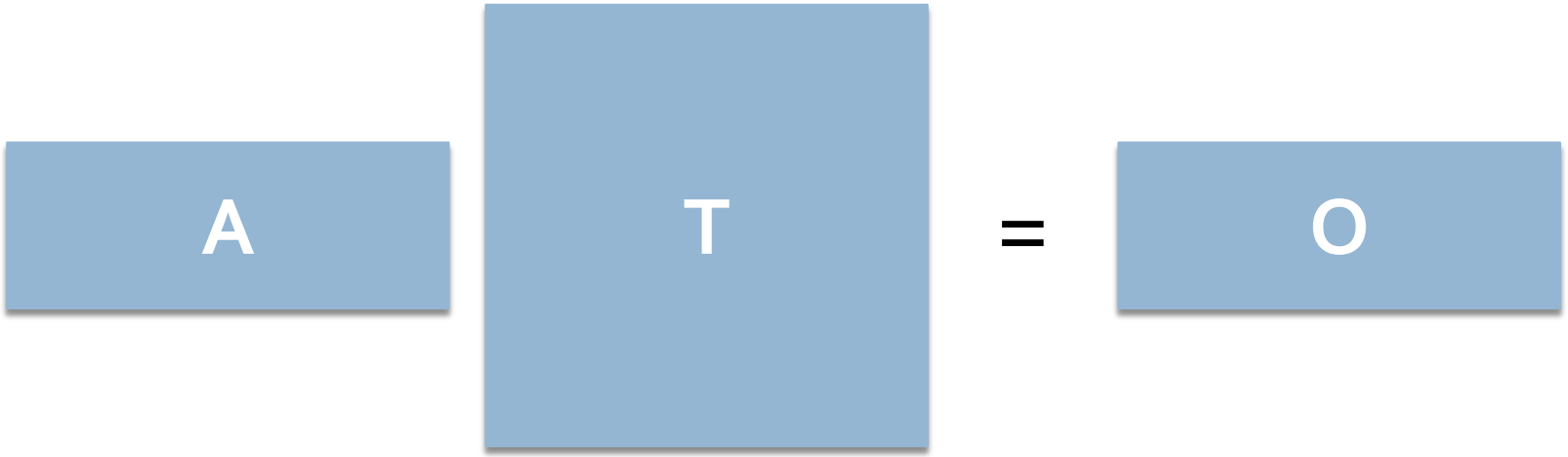
LWEとCorrelated Product TDF

- $g_{\mathbf{A}}(\mathbf{s},\mathbf{x})=\mathbf{A}^t\mathbf{s}+\mathbf{x}$とする
  ⇒$\mathrm{LWE}_{q,\chi}$が困難なら, $g_{\mathbf{A}}(\mathbf{s},\mathbf{x})$は一方向
  ⇒$(g_{\mathbf{A}_1}(\mathbf{s},\mathbf{x}_1),\ldots,g_{\mathbf{A}_k}(\mathbf{s},\mathbf{x}_k))$も一方向
- Correlated Product one-wayは簡単に言える!

- $g_{\mathbf{A}}(\cdot,\cdot)$はTDFになってるのか?

[Pei08,GV08]の戻し方

- $g_A(\mathbf{s},\mathbf{x})=\mathbf{A}^t\,\mathbf{s}+\mathbf{x} \bmod q$
- KeyGen [Ajt99, AP09]
  - Output $\mathbf{T} \in \mathbb{Z}^{m\times m}$ and $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$



イデアル格子版の準備

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

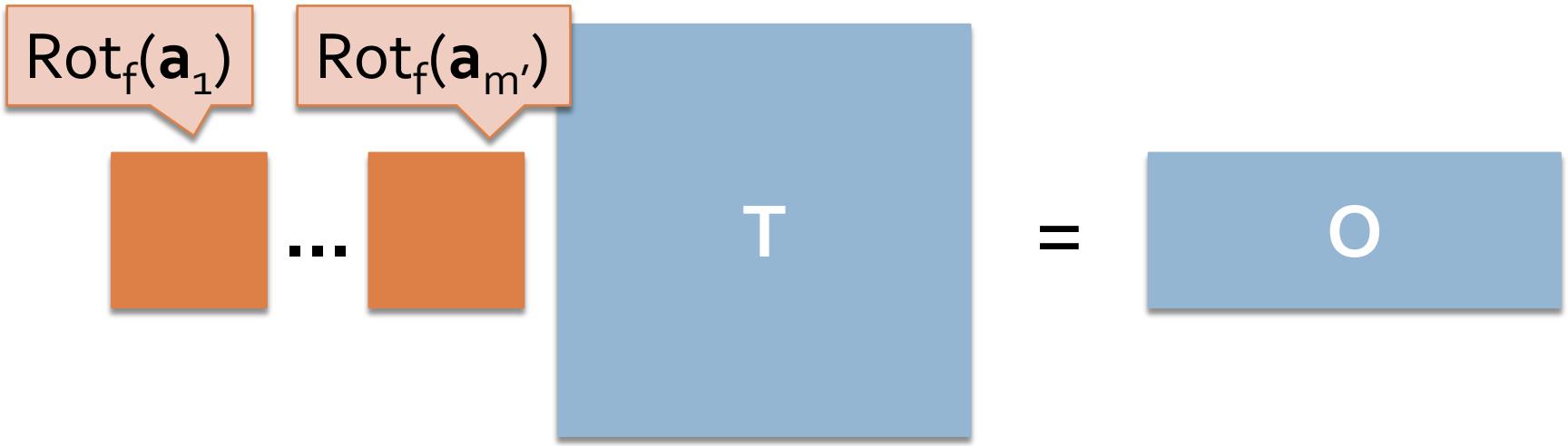
$$\mathbf{x}(\alpha)=1+\alpha+\alpha^3 \longleftrightarrow \mathrm{Rot}_f(\mathbf{x})=\begin{pmatrix} 1 & -1 & 0 & -1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

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

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

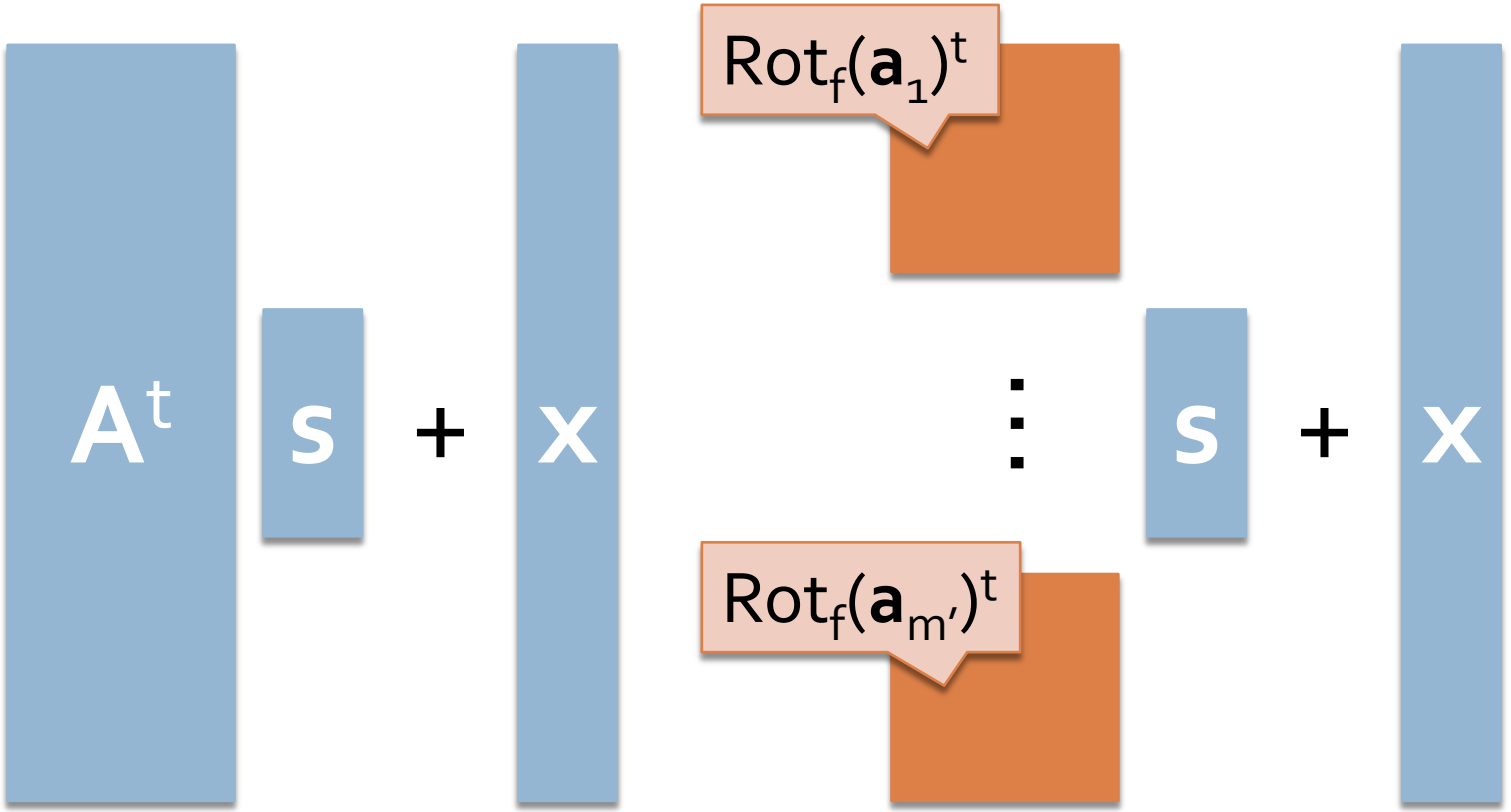
イデアル版鍵生成アルゴリズム

- 草川と田中 [XTo8], Steinfeld and Stehlé [SSo8]
- KeyGen [XTo8, SSo8]
  - Output $\mathbf{T} \in \mathbb{Z}^{m'n \times m'n}$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m'n}$



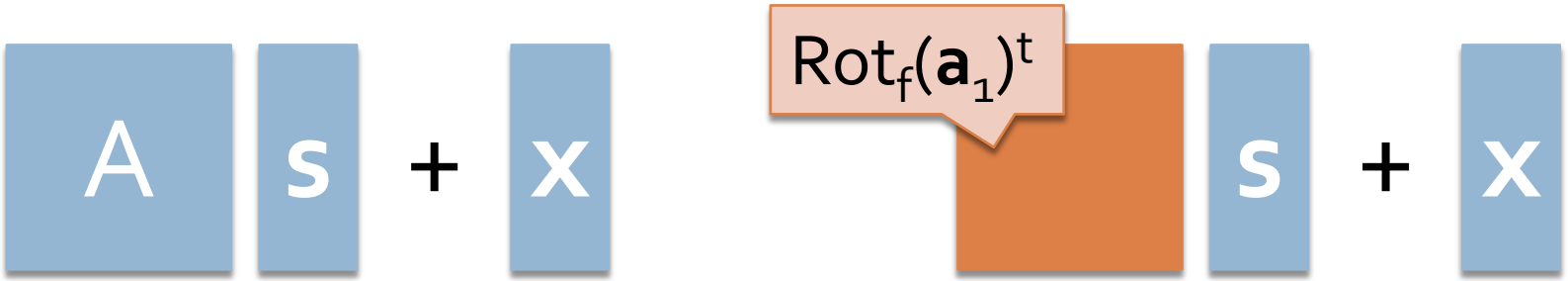
イデアル格子版 $g_A(\mathbf{s},\mathbf{x})$

- $g_A(\mathbf{s},\mathbf{x}) = \mathbf{A}^t\,\mathbf{s} + \mathbf{x}$
- $\mathbf{A}=[\mathrm{Rot}_f(\mathbf{a}_1), \ldots, \mathrm{Rot}_f(\mathbf{a}_{m'})]$なので



f-LWE問題

- $\text{f-LWE}_{q,\chi}$
  - $A_{s,\chi}$
    - 1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \chi^n$
    - 2. output $(\mathbf{a}, \text{Rot}_f(\mathbf{a})^t\,\mathbf{s} + \mathbf{x})$
  - $A_{s,\chi}$からのサンプルを見ても, **s**が求められない



まとめ

- f-LWE問題を定義
- [Pei08]を元にイデアル版のトラップドア関数
- [RS09]を元にIND-CCA2に持ち上げる
  - [Pei08]や[GV08]と同じ方針

- 未解決
  - f-LWE←f-GapSVPのような関係はあるのか?
  - 長いハードコア関数はないのか?
  - GPVのサンプリングの高速化は可能か?

参考文献

- [GGH96] (CRYPTO1996)
- [GV08] Goldwasser and Vaikuntanathan (Private)
- [Pei08] Peikert (ePrint2008)
- [SS08] Steinfeld and Stehlé (Private)
- [RS09] Rosen and Segev (TCC2009)
- [XT08] Xagawa and Tanaka (SCIS2008, AAAC2008)