NTRU暗号に関するゼロ知識証明

2009/01/22
[SCIS 2009 3F2-4]

草川恵太/田中圭介（東京工業大学）

NTRU

- Hoffstein, Pipher, Silverman (ANTS 1998)
  - 多項式環ベース
  - 速い
  - 40本以上の関連論文

NTRUとプロトコル

- NTRU暗号の関係を扱ったプロトコルはない
  - R={(pk, sk) }
  - R={((pk, c),(m, r)) : E(pk, m, r) = c}

- RSAやDL関係はプロトコルあり
  - Ex: R={(y, x): y = g^x}
- 格子暗号もプロトコルあり

結果

- NTRUについて
  - R={(pk, sk)}
  - R={((pk, c),(m, r))}
- についてのゼロ知識証明を提案
- 認証にも使える

NTRU #1

- 記法
  - $*$: $\mathbb{Z}[\alpha]/(\alpha^n-1)$上の積
  - $\mathcal{B}(d)$ = {1がd個, 0がn-d個の多項式}

- 鍵生成
  - $\mathbf{f} \leftarrow \mathcal{B}(d)$, $\mathbf{g} \leftarrow \mathcal{B}(d)$
  - pk: $\mathbf{h} = \mathbf{f}^{-1} * \mathbf{g} \bmod q$
  - sk: $\mathbf{f}$

NTRU #2

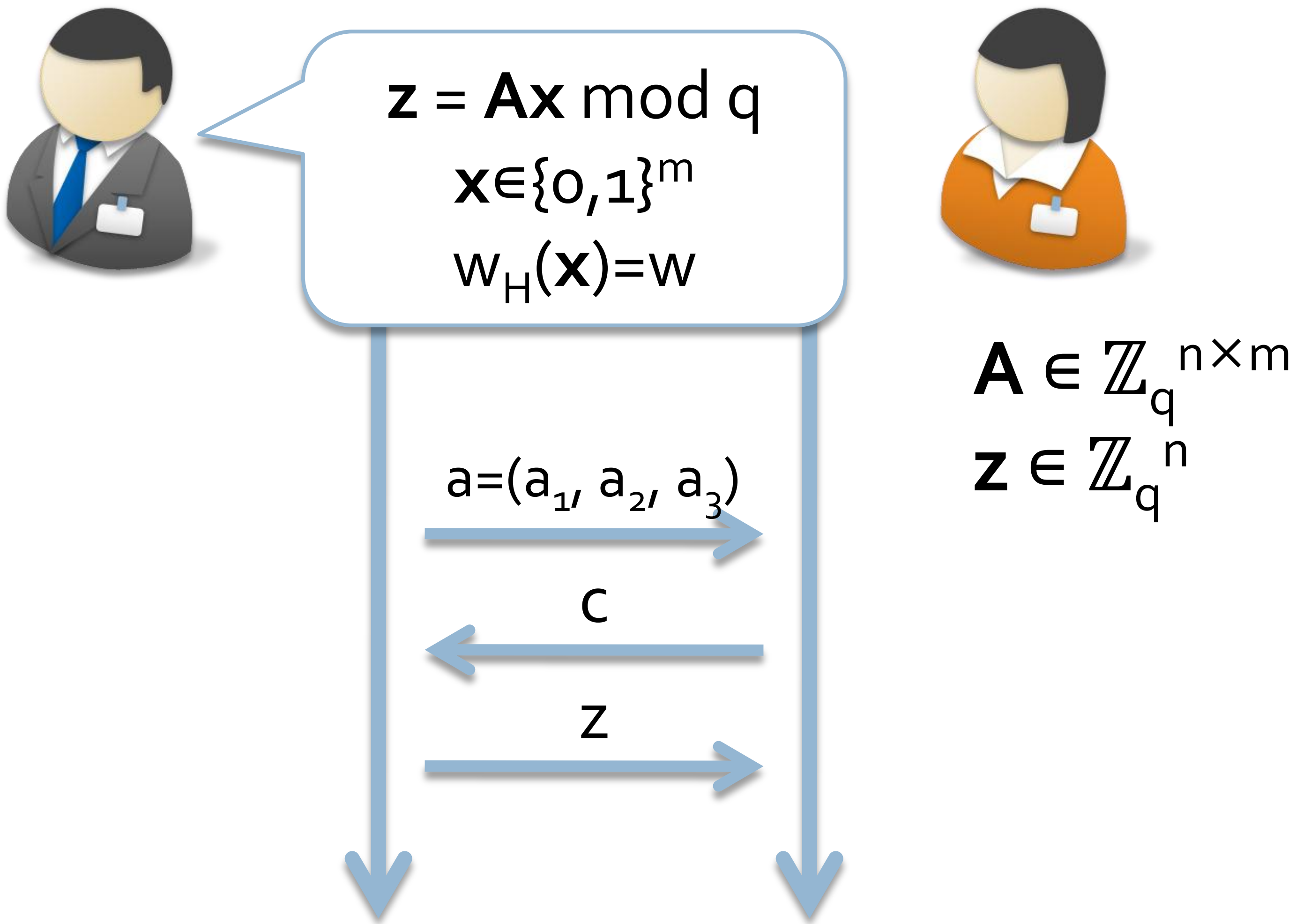
- 暗号化
  - $\mathbf{m} \in \mathcal{B}(d)$, $\mathbf{r} \leftarrow \mathcal{B}(d)$
  - $\mathbf{c} = p*\mathbf{h}*\mathbf{r} + \mathbf{m} \bmod q$
- 復号
  - $\mathbf{a}' \leftarrow \mathbf{f}*\mathbf{c}$
  - $\mathbf{a} \leftarrow p*\mathbf{g}*\mathbf{r} + \mathbf{f}*\mathbf{m}$ over $\mathbb{Z}$
  - $\mathbf{m} \leftarrow \mathbf{F}_p*\mathbf{a} \bmod p$, where $\mathbf{F}_p*\mathbf{f} = 1 \bmod p$

NTRUの関係

- 公開鍵と秘密鍵
  - $\mathbf{f} \in \mathcal{B}(d)$, $\mathbf{g} \in \mathcal{B}(d)$
  - $\mathbf{h} = \mathbf{f}^{-1} * \mathbf{g} \bmod q$

- 暗号文
  - $\mathbf{m} \in \mathcal{B}(d)$, $\mathbf{r} \in \mathcal{B}(d)$
  - $\mathbf{c} = p * \mathbf{h} * \mathbf{r} + \mathbf{m} \bmod q$

Sternのプロトコル [Ste96]



Random/Masked/Permuted

$\mathbf{z} = \mathbf{A}\mathbf{x} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w_H(\mathbf{x}) = w$

$\pi \longleftarrow S_m,\ \mathbf{s} \longleftarrow \mathbb{Z}_q^m$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{A}\mathbf{s})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{s}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{x}+\mathbf{s}))$

$z \longleftarrow \mathrm{Res}(c, \mathbf{A}, \mathbf{x}, \mathbf{s}, \pi)$

$a = (a_1, a_2, a_3) \longrightarrow$

$c \longleftarrow \{0,1,2\}$

$\longleftarrow c$

$z \longrightarrow$

$1/0 \longleftarrow V(\mathbf{A}, \mathbf{z}, a, c, z)$

Random/Masked/Permuted

$$\mathbf{z} = \mathbf{Ax} \bmod q$$
$$\mathbf{x} \in \{0,1\}^m$$
$$w_H(\mathbf{x}) = w$$

$\pi \longleftarrow S_m,\ \mathbf{s} \longleftarrow \mathbb{Z}_q^{\,m}$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{As})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{s}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{x}+\mathbf{s}))$

$\xrightarrow{a=(a_1,\ a_2,\ a_3)}$

$c \longleftarrow \{0,1,2\}$

$\xleftarrow{0}$

$z_0 \longleftarrow (\pi, \mathbf{s})$

$\xrightarrow{z_0}$

Check "random"

Random/**Masked**/Permuted

$\mathbf{z} = \mathbf{Ax} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w_H(\mathbf{x}) = w$

$\pi \longleftarrow S_m,\ \mathbf{s} \longleftarrow \mathbb{Z}_q^{\ m}$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{As})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{s}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{x}+\mathbf{s}))$

$z_1 \longleftarrow (\pi, \mathbf{x}+\mathbf{s})$

$a=(a_1, a_2, a_3)$ →

← 1

z_1 →

$c \longleftarrow \{0,1,2\}$

Check "masked"

Random/Masked/**Permuted**

$\mathbf{z} = \mathbf{A}\mathbf{x} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w_H(\mathbf{x}) = w$

$\pi \longleftarrow S_m,\ \mathbf{s} \longleftarrow \mathbb{Z}_q^m$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{A}\mathbf{s})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{s}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{x}+\mathbf{s}))$

$z_2 \longleftarrow (\pi(\mathbf{s}), \pi(\mathbf{x}+\mathbf{s}))$

$a=(a_1, a_2, a_3)$

$c \longleftarrow \{0,1,2\}$

2

z_2

Check "permuted"

Random/Masked/**Permuted**

$\mathbf{z} = \mathbf{Ax} \bmod q$

$\mathbf{x} \in \{0,1\}^m$

$w_H(\mathbf{x}) = w$

$\pi \longleftarrow S_m,\ \mathbf{s} \longleftarrow \mathbb{Z}_q^{\ m}$

$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{As})$

$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{s}))$

$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{x}+\mathbf{s}))$

$z_2 \longleftarrow (\pi(\mathbf{s}), \pi(\mathbf{x}+\mathbf{s}))$

$a = (a_1, a_2, a_3) \longrightarrow$

$\longleftarrow 2$

$z_2 \longrightarrow$

C

$\pi(\mathbf{x}+\mathbf{s}) - \pi(\mathbf{s})$

$= \pi(\mathbf{s})\ ?\!\in \{0,1\}^m$

Check “permuted”

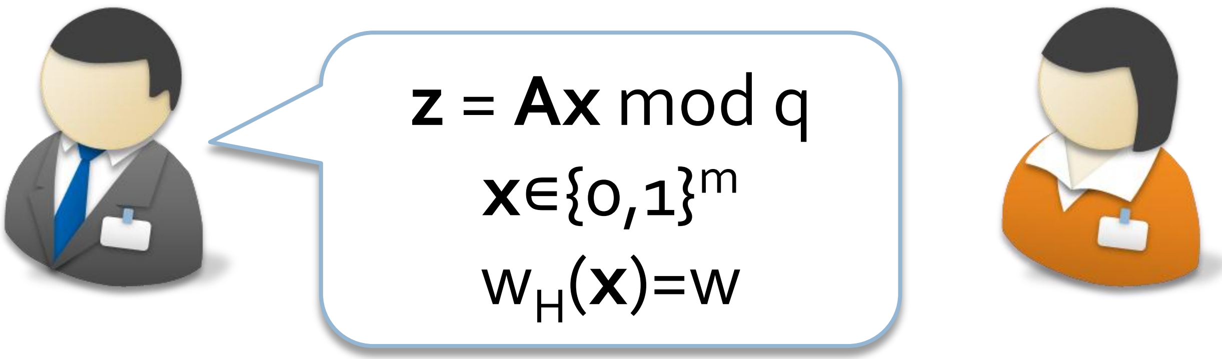
NTRUとSternのプロトコル

- R={ (h, (f,g)):

  $\mathbf{f} \in \mathcal{B}(d)$, $\mathbf{g} \in \mathcal{B}(d)$, $\mathbf{h} = \mathbf{f}^{-1} * \mathbf{g} \bmod q$}

- R={ ((h,c), (m,r)):

  $\mathbf{m} \in \mathcal{B}(d)$, $\mathbf{r} \in \mathcal{B}(d)$, $\mathbf{c} = p * \mathbf{h} * \mathbf{r} + \mathbf{m} \bmod q$}



NTRUとZKの準備

$$\mathbb{Z}[\alpha]/(\alpha^4-1) \longleftrightarrow C_4(\mathbb{Z})$$

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

$$\mathbf{y}(\alpha) = \alpha+2\alpha^2 \longleftrightarrow \mathbf{y} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}$$

$$\mathbf{x}*\mathbf{y} = 3+2\alpha+\alpha^2+\alpha^3 \longleftrightarrow \mathrm{Rot}(\mathbf{x})\,\mathbf{y} = \begin{pmatrix} 3 \\ 2 \\ 1 \\ 1 \end{pmatrix}$$

プロトコルの変形 #1-1

$$\mathbf{z} = \mathbf{A}\mathbf{x} \bmod q$$
$$\mathbf{x} \in \{0,1\}^m$$
$$w_H(\mathbf{x}) = w$$

- $\mathbf{A} = [\mathrm{Rot}(\mathbf{a})\ \mathrm{Rot}(\mathbf{b})]$とすると
- $\mathbf{z} = \mathbf{A}\,(\mathbf{x}, \mathbf{y}) = \mathrm{Rot}(\mathbf{a})\mathbf{x} + \mathrm{Rot}(\mathbf{b})\mathbf{y}$

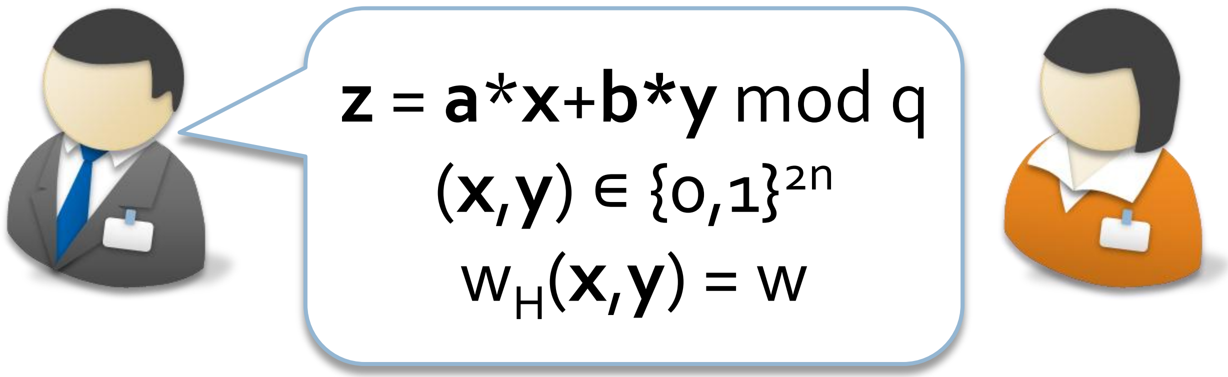
  $= \mathbf{a}*\mathbf{x} + \mathbf{b}*\mathbf{y} \bmod q$

プロトコルの改変 #1-2

- 公開鍵と秘密鍵
  - $\mathbf{A}$ = [Rot($\mathbf{h}$) Rot(-1)]
  - $\mathbf{h} = \mathbf{f}^{-1} * \mathbf{g} \bmod q \Rightarrow \mathbf{o} = \mathbf{h} * \mathbf{f} + (-1) * \mathbf{g} \bmod q$

- 暗号文
  - $\mathbf{A}$ = [Rot(p*$\mathbf{h}$) Rot(1)]
  - $\mathbf{c} = (p * \mathbf{h}) * \mathbf{r} + 1 * \mathbf{m} \bmod q$

問題 #1



- 公開鍵と秘密鍵
  - $\mathbf{o}=\mathbf{h}*\mathbf{f}-\mathbf{g} \bmod q$, $\mathbf{f} \in \mathcal{B}(d)$, $\mathbf{g} \in \mathcal{B}(d)$
- 暗号文
  - $\mathbf{c}=p*\mathbf{h}*\mathbf{r}+\mathbf{m} \bmod q$, $\mathbf{m} \in \mathcal{B}(d)$, $\mathbf{r} \in \mathcal{B}(d)$

プロトコルの改変 #2

$$\mathbf{z} = \mathbf{a}*\mathbf{x}+\mathbf{b}*\mathbf{y} \bmod q$$

$$(\mathbf{x},\mathbf{y}) \in \{0,1\}^{2n}$$

$$w_H(\mathbf{x},\mathbf{y})=2d$$

$$\pi \longleftarrow S_{2n},\ (\mathbf{s},\mathbf{t}) \longleftarrow \mathbb{Z}_q^{2n}$$

$$a_1 \longleftarrow \mathrm{Com}(\pi, \mathbf{a}*\mathbf{s}+\mathbf{b}*\mathbf{t})$$

$$a_2 \longleftarrow \mathrm{Com}(\pi(\mathbf{s},\mathbf{t}))$$

$$a_3 \longleftarrow \mathrm{Com}(\pi(\mathbf{x}+\mathbf{s},\mathbf{y}+\mathbf{t}))$$

$$z \longleftarrow \mathrm{Res}(c,\mathbf{a},\mathbf{b},\mathbf{x},\mathbf{y},\mathbf{s},\mathbf{t},\pi)$$

$$c \longleftarrow \{0,1,2\}$$

$$1/0 \longleftarrow V(\mathbf{A},\mathbf{z},a,c,z)$$

プロトコルの改変 #2

$\mathbf{z} = \mathbf{a}*\mathbf{x}+\mathbf{b}*\mathbf{y} \bmod q$

$(\mathbf{x},\mathbf{y}) \in \{0,1\}^{2n}$

$w_H(\mathbf{x})=d, w_H(\mathbf{y})=d$

$(\pi_s,\pi_t) \longleftarrow S_n^{\ 2},\ (\mathbf{s},\mathbf{t}) \longleftarrow \mathbb{Z}_q^{\ 2n}$

$a_1 \longleftarrow \mathrm{Com}(\pi_s,\pi_t,\mathbf{a}*\mathbf{s}+\mathbf{b}*\mathbf{t})$

$a_2 \longleftarrow \mathrm{Com}(\pi_s(\mathbf{s}),\pi_t(\mathbf{t}))$

$a_3 \longleftarrow \mathrm{Com}(\pi_s(\mathbf{x}+\mathbf{s}),\pi_t(\mathbf{y}+\mathbf{t}))$

$z \longleftarrow \mathrm{Res}(c,\mathbf{a},\mathbf{b},\mathbf{x},\mathbf{y},\mathbf{s},\mathbf{t},\pi_s,\pi_t)$

置換を分割
[KTX08]

$1/0 \longleftarrow V'(\mathbf{A},\mathbf{z},a,c,z)$

議論 #1

- NTRU暗号に関するゼロ知識証明
  - Sternのプロトコルを利用
  - CZK Proof or SZK Argument (ハッシュを仮定)

議論 #2

- 認証
  - NTRU仮定で受動的安全
  - コンカレント安全にするには
    - One-more NTRU仮定
    - 二重化テクニック
  - Sternのプロトコルと二重化は相性が悪い