

NFALSE:

多項式環に基づくより高速な公開鍵暗号

2009/01/22
[SCIS 2009 3F2-5]

草川恵太/田中圭介（東京工業大学）

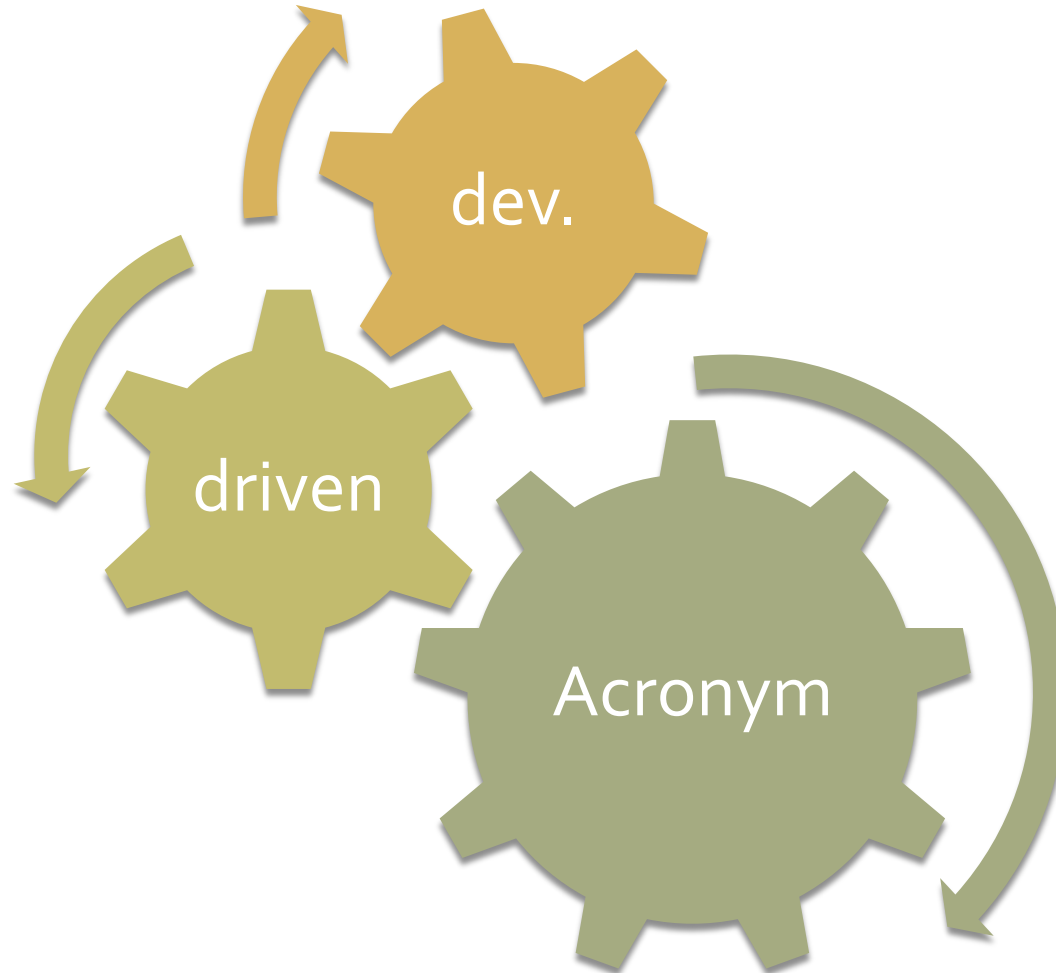
略称駆動開発

2



ADD (Acronym Driven Development)

3



既存の方式

4

NTRU

既存の読み方

5

NTRUE

新提案

6

NFALSE

名前だけ決まった

NTRU

7

- Hoffstein, Pipher, Silverman (ANTS 1998)
 - 速い $\tilde{O}(n^2)$
 - 多項式環ベース
- NTRUの変種
 - CTRU (Gaborit, Ohler, Solé [GOSo2])
 - MaTRU (Coglianese, Goi [CGo5])
 - etc.

NTRU #1

8

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

- パラメータ例:
 - 128bit: $n=449, d=134$
 - 256bit: $n=853, d=268$

NTRU #2

9

- 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

10

□ 暗号化

- $m \in \mathcal{B}(d), r \leftarrow \mathcal{B}(d)$

- $c = p * h * r + m \text{ mod } q$

□ 復号

- $a' \leftarrow f * c$

- $a \leftarrow p * g * r + f * m \text{ over } \mathbb{Z}$

- $m \leftarrow F_p * a \text{ mod } p, \text{ where } F_p * f = 1 \text{ mod } p$

□ 計算速度

- $O(n^2 \log^2 q)$

発想

11

| | |
|--------|--|
| NTRU | $\mathbb{Z}_q[\alpha]/(\alpha^n-1)$ |
| CTRU | $(\text{GF}(2)[T])[\alpha]/(\alpha^n-1)$ |
| MaTRU | $M_{k,k}(\mathbb{Z}_q[\alpha]/(\alpha^n-1))$ |
| NFALSE | ??? |

発想

12

NTRU

$$\mathbb{Z}_q[\alpha]/(\alpha^n - 1)$$

CTRU

TRUE or FALSEを
-1 or +1と解釈

MaTRU

$$\mathbb{Z}_q[\alpha]/(\alpha^n - 1)$$

NFALSE

$$\mathbb{Z}_q[\alpha]/(\alpha^n + 1)$$

α^n+1 の性質 #1

13

- $n=2^k$ のとき
- \mathbb{Z} 上既約
- \mathbb{Z}_q 上可約
 - q :素数かつ $2n|q-1 \Rightarrow \mathbb{Z}_q$ 上可約
 - w :位数 $2n$ の \mathbb{Z}_q の要素
 - $\alpha^n+1 = (\alpha-w^1)(\alpha-w^3)\dots(\alpha-w^{2^n-1})$ over \mathbb{Z}_q

α^{n+1} の性質 #2

14

- FFTと同様に $f * g$ を $O(n \log n \log^2 q)$ で計算できる
→ほぼ線形時間で暗号化・復号が可能!
- NTRUだと $O(n^2 \log^2 q)$

長所が見つかった

高速化のポイント

15

- 数学的構造
 - w : 位数 $2n$ の \mathbb{Z}_q の要素
 - $\alpha^n + 1 = (\alpha - w^1)(\alpha - w^3)\dots(\alpha - w^{2^n-1})$
 - $\mathbb{Z}_q[\alpha]/(\alpha^n + 1) = \mathbb{Z}_q[\alpha]/(\alpha - w^1) \times \dots \times \mathbb{Z}_q[\alpha]/(\alpha - w^{2^n-1})$
 - $\theta_{n,w}(\mathbf{f}) = (\mathbf{f}(w^1), \dots, \mathbf{f}(w^{2^n-1}))$
- 行列で書いてみる

行列表示

16

$$\theta_{n,w}(f) = \begin{pmatrix} w^0 & w^1 & w^2 & w^3 & w^4 & w^5 & w^6 & w^7 \\ w^0 & w^3 & w^6 & w^9 & w^{12} & w^{15} & w^2 & w^5 \\ w^0 & w^5 & w^{10} & w^{15} & w^4 & w^9 & w^{14} & w^3 \\ w^0 & w^7 & w^{14} & w^5 & w^{12} & w^3 & w^{10} & w^1 \\ w^0 & w^9 & w^2 & w^{11} & w^4 & w^{13} & w^6 & w^{15} \\ w^0 & w^{11} & w^6 & w^1 & w^{12} & w^7 & w^2 & w^{13} \\ w^0 & w^{13} & w^{10} & w^7 & w^4 & w^1 & w^{14} & w^{11} \\ w^0 & w^{15} & w^{14} & w^{13} & w^{12} & w^{11} & w^{10} & w^9 \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{pmatrix}$$

行列表示

17

$$\theta_{n,w}(f) = \begin{pmatrix} w^0 & w^1 & w^2 & w^3 & w^4 & w^5 & w^6 & w^7 \\ w^0 & w^3 & w^6 & w^9 & w^{12} & w^{15} & w^2 & w^5 \\ w^0 & w^5 & w^{10} & w^{15} & w^4 & w^9 & w^{14} & w^3 \\ w^0 & w^7 & w^{14} & w^5 & w^{12} & w^3 & w^{10} & w^1 \\ w^0 & w^9 & w^2 & w^{11} & w^4 & w^{13} & w^6 & w^{15} \\ w^0 & w^{11} & w^6 & w^1 & w^{12} & w^7 & w^2 & w^{13} \\ w^0 & w^{13} & w^{10} & w^7 & w^4 & w^1 & w^{14} & w^{11} \\ w^0 & w^{15} & w^{14} & w^{13} & w^{12} & w^{11} & w^{10} & w^9 \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{pmatrix}$$

行列表示

18

$$\theta_{n,w}(f) = \begin{pmatrix} w^0 & w^2 & w^4 & w^6 & w^1 & w^3 & w^5 & w^7 \\ w^0 & w^6 & w^{12} & w^2 & w^3 & w^9 & w^{15} & w^5 \\ w^0 & w^{10} & w^4 & w^{14} & w^5 & w^{15} & w^9 & w^3 \\ w^0 & w^{14} & w^{12} & w^{10} & w^7 & w^5 & w^3 & w^1 \\ w^0 & w^2 & w^4 & w^6 & w^9 & w^{11} & w^{13} & w^{15} \\ w^0 & w^6 & w^{12} & w^2 & w^{11} & w^1 & w^7 & w^{13} \\ w^0 & w^{10} & w^4 & w^{14} & w^{13} & w^7 & w^1 & w^{11} \\ w^0 & w^{14} & w^{12} & w^{10} & w^{15} & w^{13} & w^{11} & w^9 \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_2 \\ f_4 \\ f_6 \\ f_1 \\ f_3 \\ f_5 \\ f_7 \end{pmatrix}$$

行列表示

19

$$\theta_{n,w}(f) = \begin{pmatrix} w^0 & w^2 & w^4 & w^6 & w^1 & w^3 & w^5 & w^7 \\ w^0 & w^6 & w^{12} & w^2 & w^3 & w^9 & w^{15} & w^5 \\ w^0 & w^{10} & w^4 & w^{14} & w^5 & w^{15} & w^9 & w^3 \\ w^0 & w^{14} & w^{12} & w^{10} & w^7 & w^5 & w^3 & w^1 \\ w^0 & w^2 & w^4 & w^6 & w^9 & w^{11} & w^{13} & w^{15} \\ w^0 & w^6 & w^{12} & w^2 & w^{11} & w^1 & w^7 & w^{13} \\ w^0 & w^{10} & w^4 & w^{14} & w^{13} & w^7 & w^1 & w^{11} \\ w^0 & w^{14} & w^{12} & w^{10} & w^{15} & w^{13} & w^{11} & w^9 \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_2 \\ f_4 \\ f_6 \\ f_1 \\ f_3 \\ f_5 \\ f_7 \end{pmatrix}$$

行列表示

20

$$\theta_{n,w}(f) = \begin{pmatrix} w^0 & w^2 & w^4 & w^6 & w^1 & w^3 & w^5 & w^7 \\ w^0 & w^6 & w^{12} & w^2 & w^3 & w^9 & w^{15} & w^5 \\ w^0 & w^{10} & w^4 & w^{14} & w^5 & w^{15} & w^9 & w^3 \\ w^0 & w^{14} & w^{12} & w^{10} & w^7 & w^5 & w^3 & w^1 \\ w^0 & w^2 & w^4 & w^6 & w^9 & w^{11} & w^{13} & w^{15} \\ w^0 & w^6 & w^{12} & w^2 & w^{11} & w^1 & w^7 & w^{13} \\ w^0 & w^{10} & w^4 & w^{14} & w^{13} & w^7 & w^1 & w^{11} \\ w^0 & w^{14} & w^{12} & w^{10} & w^{15} & w^{13} & w^{11} & w^9 \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_2 \\ f_4 \\ f_6 \\ f_1 \\ f_3 \\ f_5 \\ f_7 \end{pmatrix}$$

$$\bar{w} = w^2$$

行列表示

$$\theta_{n,w}(f) = \begin{pmatrix} \bar{w}^0 & \bar{w}^1 & \bar{w}^2 & \bar{w}^3 \\ \bar{w}^0 & \bar{w}^3 & \bar{w}^6 & \bar{w}^1 \\ \bar{w}^0 & \bar{w}^5 & \bar{w}^2 & \bar{w}^7 \\ \bar{w}^0 & \bar{w}^7 & \bar{w}^6 & \bar{w}^5 \\ \bar{w}^0 & \bar{w}^1 & \bar{w}^2 & \bar{w}^3 \\ \bar{w}^0 & \bar{w}^3 & \bar{w}^6 & \bar{w}^1 \\ \bar{w}^0 & \bar{w}^5 & \bar{w}^2 & \bar{w}^7 \\ \bar{w}^0 & \bar{w}^7 & \bar{w}^6 & \bar{w}^5 \end{pmatrix} \begin{pmatrix} w^1 \cdot \bar{w}^0 & w^1 \cdot \bar{w}^1 & w^1 \cdot \bar{w}^2 & w^1 \cdot \bar{w}^3 \\ w^3 \cdot \bar{w}^0 & w^3 \cdot \bar{w}^3 & w^3 \cdot \bar{w}^6 & w^3 \cdot \bar{w}^1 \\ w^5 \cdot \bar{w}^0 & w^5 \cdot \bar{w}^5 & w^5 \cdot \bar{w}^2 & w^5 \cdot \bar{w}^7 \\ w^7 \cdot \bar{w}^0 & w^7 \cdot \bar{w}^7 & w^7 \cdot \bar{w}^6 & w^7 \cdot \bar{w}^5 \\ -w^1 \cdot \bar{w}^0 & -w^1 \cdot \bar{w}^1 & -w^1 \cdot \bar{w}^2 & -w^1 \cdot \bar{w}^3 \\ -w^3 \cdot \bar{w}^0 & -w^3 \cdot \bar{w}^3 & -w^3 \cdot \bar{w}^6 & -w^3 \cdot \bar{w}^1 \\ -w^5 \cdot \bar{w}^0 & -w^5 \cdot \bar{w}^5 & -w^5 \cdot \bar{w}^2 & -w^5 \cdot \bar{w}^7 \\ -w^7 \cdot \bar{w}^0 & -w^7 \cdot \bar{w}^7 & -w^7 \cdot \bar{w}^6 & -w^7 \cdot \bar{w}^5 \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_2 \\ f_4 \\ f_6 \\ f_1 \\ f_3 \\ f_5 \\ f_7 \end{pmatrix}$$

$$\bar{w} = w^2$$

行列表示

$$\theta_{n,w}(f) = \begin{pmatrix} \theta_{n/2,w^2}(f_e) + (w^1, \dots, w^7) \theta_{n/2,w^2}(f_o) \\ \theta_{n/2,w^2}(f_e) - (w^1, \dots, w^7) \theta_{n/2,w^2}(f_o) \end{pmatrix}$$

ほとんどFFTと同じ
再帰的な計算で、 $\tilde{O}(n \log q)$

NTRUとFFT

23

なぜNTRUではFFTを使わないのか?

[Sil99] NTRU-FFTを考察

[Geno1] 低次元格子を用いて攻撃

NTRU格子 - 準備

24

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

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

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

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

NTRU格子 [CS97]

25

- Coppersmith and Shamir
 - $R_h = \{(\mathbf{x}, \mathbf{y}) : \mathbf{h} * \mathbf{x} = \mathbf{y} \pmod{q}\}$
 - $(\mathbf{f}, \mathbf{g}) \in R_h$
 - $\|(\mathbf{f}, \mathbf{g})\| \leq \sqrt{2d}$

$$\mathbf{B}_h = \begin{pmatrix} \text{Rot}(\mathbf{1}) & \text{Rot}(\mathbf{0}) \\ \text{Rot}(\mathbf{h}) & \text{Rot}(\mathbf{q}) \end{pmatrix}$$

$$L_h = L(\mathbf{B}_h)$$

Gentryの攻撃—アイデア

26

- $b|n$ のとき,
- $\mathbb{Z}[\alpha]/(\alpha^n-1)$ から $\mathbb{Z}[\alpha]/(\alpha^b-1)$ に環準同型
- $\mathbf{a} = (a_0, \dots, a_{n-1}) \in \mathbb{Z}[\alpha]/(\alpha^n-1)$ について
$$\theta_b(\mathbf{a}) = (\sum_{i=0 \bmod b} a_i, \dots, \sum_{i=b-1 \bmod b} a_i) \in \mathbb{Z}[\alpha]/\langle \alpha^b-1 \rangle$$
- ポイント
 - θ_b はノルムを高々 n/b 倍にしかなない
 - $\|(\theta_b(\mathbf{f}), \theta_b(\mathbf{g}))\| \leq (n/b)\sqrt{2d}$
 - $(\theta_b(\mathbf{f}), \theta_b(\mathbf{g}))$ から (\mathbf{f}, \mathbf{g}) に戻せる (省略)

Gentryの攻撃を防ぐ

27

- α^{n+1} は \mathbb{Z} 上既約
 - これで防げた
- \mathbb{Z}_q 上可約
 - 現時点では攻撃できるようないい環がない?
 - 今のところNFALSEでは大丈夫

略称の意味

28

NFALSE

略称の意味

29

New

Fast and

Almost

Linear-time

Secure (?)

Encryption

最後に

30

NFALSEは
皆さんの攻撃を
お待ちしております