非可換群を用いたNTRU方式の拡張

安田 貴徳† グザヴィエ ダハン† 櫻井 幸一‡,†

† 九州先端科学技術研究所
814–0001 福岡市早良区百道浜 2-1-22
yasuda, dahan, sakurai @isit.or.jp

‡ 九州大学 大学院システム情報科学研究院
819–0395 福岡県福岡市西区元岡 744 番地

あらまし 格子ベース暗号の暗号方式の一つであるNTRUは、巡回群に対する群環を利用した方式と見ることができる。本稿では、この考え方を一般化し、任意の群環に対するNTRUの拡張方式を考察する。特に具体的な幾つかの群の例について実現方式と安全性について考察する。

Extension of NTRU using non-commutative group

Takanori Yasuda†Xavier Dahan Kouichi Sakurai‡,†

†Institute of Systems, Information Technologies and Nanotechnologies
Momochihama 2–1–22, Sawara-ku, Fukuoka-shi, Fukuoka,
814–0001 Japan
yasuda, dahan, sakurai @isit.or.jp

‡Department of Informatics, Kyushu University
Motooka 744, Nishi-ku, Fukuoka-shi, Fukuoka, 819–0395 Japan

Abstract An encryption scheme NTRU, which belongs to lattice-based cryptography, can be regarded as a scheme using the group ring with respective to cyclic groups. In this paper, we generalize this idea to propose an extension of NTRU using general group ring. In particular, we observe the realization and security of the extension scheme for several examples.

1 はじめに

NTRUはJ. Hoffsteinらが1996年に提案したと格子ベース暗号の暗号方式である [1]. 今のところ，致命的となる攻撃方法は知られていない. NTRUは（代数的な）環を利用した暗号であるが，どんな環でも利用できるというわけではなく，NTRUで用いられている環 $\mathbb{Z}[x]/(x^N-1)$ のようなある特性を持った環でなければ，同じような方式を作ることはできない．実際，一般の環でNTRUを構成すると，ほとんどの場合で復号化可能となるメッセージ領域が十分には確保できず，安全な暗号方式にはならない．ここで言う“ある特性”を $\mathbb{Z}[x]/(x^N-1)$ で説明すると，$\mathbb{Z}[x]/(x^N-1)$ 内の（簡約された）単項式 ax^i, bx^j が十分小さい係数を持つならば，その積

$$ax^i * bx^j = abx^{i+j \bmod N} \tag{1}$$

も十分小さい係数を持つというものである．補足するならば，積がまた単項式であることと，係数に余計なスカラー倍が係っていないという点がポイントである.

一方，(有限）群 G に対し，群環と呼ばれる環 $\mathbb{Z}[G]$ が作られる．$\mathbb{Z}[G]$ 内の単項式 $a[g], b[h]$ に対して，それらの積は

$$a[g] * b[h] = ab[gh] \tag{2}$$

と与えられ，(1) と近い計算規則を持っている．実際，$\mathbb{Z}[x]/(x^N-1)$ は N 元からなる巡回群 C_N

による群環 $\mathbb{Z}[C_N]$ と同型である．(2) の規則は一般の有限群に対する群環が，NTRU の構成に必要な環の“特徴”を持っていることを示しており，群環が NTRU と非常に相性の良い環であることが分かる．

本発表では，群環を用いた NTRU の拡張（GR-NTRU）を提案し，その安全性について議論する．但し，今回は一般的な群環に対する安全性評価はせず，群が 2 面体群，フロベニウス群の場合のみを扱い，その結果から，一般の場合の GR-NTRU の安全性を推測する．将来的に，一般の場合の GR-NTRU の安全性が決定できたならば，より安全性の高い群に対する GR-NTRU を選択し，使用することができるようになる．安全性の観点から見て，GR-NTRU 全体においてオリジナル NTRU がどの位置にあるかという点について今のところ不明であるが，興味深い問題である．

2 群環を用いた NTRU の拡張方式

NTRU の方式は環 $\mathbb{Z}[x]/(x^N-1)$ を用いて記述されるが，この環を単純に $\mathbb{Z}[C_N]$ に変えても何の問題もなく方式が実行できる．さらに，この C_N の部分を一般の有限群 G に拡張することができる．この $\mathbb{Z}[G]$ を用いた NTRU の拡張を GR-NTRU と呼ぶことにする．GR-NTRU に関しては NTRU にはない次の 2 つが問題となる．

1. 有限群 G に対して $\mathbb{Z}[G]$ をどのように実現するか．
2. GR-NTRU の安全性はどの程度か．

この 2 点は実は密接に関係がある．このことについて 2 つの例を用いて説明する．

3 二面体群の場合

2 面体群 $D_n = C_n \rtimes \mathbb{Z}/2\mathbb{Z}$ は位数 $2n$ の非可換群である．D_n は n 次対称群 $\mathfrak{S}_n$ の部分群として実現することができる．実際，C_n の生成元を巡回置換 $(2,3,\ldots,n,1)$ と $\mathbb{Z}/2\mathbb{Z}$ の非自明元を

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}$$

と対応させると D_n から $\mathfrak{S}_n$ への埋め込みが作れる．この埋め込みと置換行列を用いると

$$\Phi_1 : \mathbb{Z}[D_n] \to \mathbb{M}(n,\mathbb{Z})$$

なる環準同型が作られる．また，準同型 $D_n = C_n \rtimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ から，環準同型

$$\Phi_2 : \mathbb{Z}[D_n] \to \mathbb{Z}$$

が作られる．n が偶数のときは準同型 $D_n = C_n \rtimes \mathbb{Z}/2\mathbb{Z} \to (C_n \rtimes \mathbb{Z}/2\mathbb{Z})/(C_{n/2} \rtimes \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ があるから，これより

$$\Phi_3 : \mathbb{Z}[D_n] \to \mathbb{Z}$$

が作られる．このとき次が言える．

補題 1. 1) n が奇数のとき，$\Phi_1 \oplus \Phi_2 : \mathbb{Z}[D_n] \to \mathbb{M}(n,\mathbb{Z}) \oplus \mathbb{Z}$ は単射となる．

2) n が偶数のとき，$\Phi_1 \oplus \Phi_2 \oplus \Phi_3 : \mathbb{Z}[D_n] \to \mathbb{M}(n,\mathbb{Z}) \oplus \mathbb{Z} \oplus \mathbb{Z}$ は単射となる．

この補題により問題 1 は解決する．すなわち，n が奇数のとき，$\mathbb{Z}[D_n]$ は $\mathbb{M}(n,\mathbb{Z}) \oplus \mathbb{Z}$ で，偶数のときは $\mathbb{M}(n,\mathbb{Z}) \oplus \mathbb{Z} \oplus \mathbb{Z}$ で実現することができる．

次に GR-NTRU の安全性について考える．まず，NTRU の行列環類似方式 Matrix-NTRU[2] の安全性について述べておく．

補題 2 ([3])**.** 行列環 $\mathbb{M}(n,\mathbb{Z})$ を用いた NTRU の類似方式 Matrix-NTRU の安全性は，環 $\mathbb{Z}[x]/(x^n-1)$ を用いた NTRU の安全性と同等である．

補題 1 で $\mathbb{Z}[D_n]$ を実現し，GR-NTRU の方式を実行すると，実質，複数個の Matrix-NTRU の方式を実行することになる．実際，n が奇数の場合は $\mathbb{M}(n,\mathbb{Z})$ を用いた Matrix-NTRU 1 つと $\mathbb{Z} = \mathbb{M}(1,\mathbb{Z})$ を用いた Matrix-NTRU 1 つを実行することになり，n が偶数の場合は $\mathbb{M}(n,\mathbb{Z})$ を用いた Matrix-NTRU 1 つと $\mathbb{Z} = \mathbb{M}(1,\mathbb{Z})$ 2 つを用いた Matrix-NTRU を実行することになる．この事実から懸念されることは，$\mathbb{Z}[D_n]$ を用いた GR-NTRU の安全性が Matrix-NTRU の安全性に帰着されるのではないかということである．これに関しては次が言える．

補題 3. GR-NTRU に付随する格子問題の最短ベクトルは，補題 1 の準同型により，Matrix-NTRU に付随する格子問題の最短ベクトルに移る．

すなわち，懸念通り，GR-NTRU の安全性は Matrix-NTRU の安全性に帰着される．よって，補題 2 から次が言える．

定理 4. $\mathbb{Z}[D_n]$ を用いた GR-NTRU の安全性は環 $\mathbb{Z}[x]/(x^n-1)$ を用いた NTRU の安全性と同等である．

群の位数で比較すると D_n の位数が $2n$ で，C_N の位数が n であるから，$\mathbb{Z}[D_n]$ を用いた GR-NTRU を用いるよりも同じ安全性を持つ NTRU を用いた方が，鍵長などが小さくて済むことになる．

4 フロベニウス群の場合

フロベニウス群 $F_p = (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$（$p$: 素数）の場合も同様のことが言える．実際，$\mathbb{Z}[F_p]$ は $\mathbb{Z}[x]/(x^{p-1}-1) \oplus \mathbb{M}(p,\mathbb{Z})$ により実現することができ，次が言える．

定理 5. $\mathbb{Z}[F_p]$ を用いた GR-NTRU の安全性は環 $\mathbb{Z}[x]/(x^p-1)$ を用いた NTRU の安全性と同等である．

群の位数で比較すると F_p の位数が $p(p-1)$ で，C_p の位数が p であるから，$\mathbb{Z}[F_p]$ を用いた GR-NTRU を用いるよりも同じ安全性を持つ NTRU を用いた方が，鍵長などが小さくて済むことになる．

5 考察

２つの例から分かるように，GR-NTRU の安全性は $\mathbb{Z}[G]$ の実現方法と関係している．$\mathbb{Z}[G]$ の実現方法には G の表現が関わっている．よって，GR-NTRU の安全性は G の表現と関係があると考えられる．実際２つの例の場合，G の既約 $\mathbb{Q}$-表現の最大次数が安全性を決定している．

謝辞

この研究は総務省戦略的情報通信研究開発推進事業（SCOPE）平成 25 年度イノベーション創出型研究開発フェーズ II（no. 0159-0172）の支援を受け，また第 1 著者は科研費若手研究 B（課題番号 24740078）の支援を受けている．

参考文献

[1] J. Hoffstein, J. Pipher, and J.H. Silverman, “NTRU: a ring based public key cryptosystem”. ANTS-III, Springer LNCS vol. 1423, pp. 267–288, 1998.

[2] R. Nayak, C. Sastry, and J. Pradhan, “A matrix formulation for NTRU cryptosystem”, ICON’08, IEEE, pp.1–5, 2008.

[3] Y. Pan and Y. Deng, “A General NTRU-Like Framework for Constructing Lattice-Based Public-Key Cryptosystems”, WISE’11, Springer LNCS vol. 7115, pp. 109–120, 2012.