P-5

正標数の wild 多項式自己同型と鍵共有方式

A wild polynomial automorphism in positive characteristic and a key exchange protocol

○中村周平 [1], 伊藤勝 [2], 秋山浩一郎 [3], 平田典子 [2]

*Shuhei Nakamura[1], Masaru Ito[2], Koichiro Akiyama[3], Noriko Hirata-Kohno[2]

Abstract: The aim of the present article is to create suitably secure bijective maps in a key exchange protocol in the cryptography. We consider so-called wild polynomial automorphisms and show auxiliary properties to construct such automorphisms over a domain of positive characteristic. [4]

1. Polynomial automorphisms

Rを整域とする．$\mathbf{x} = (x_1, \ldots, x_n)$とおく．$R[\mathbf{x}]^n$ の元 $\varphi = (\varphi_1, \ldots, \varphi_n)$ は R^n から R^n への写像を定める．この写像を多項式写像と称する．

$$\varphi\colon\ (a_1, \ldots, a_n) \mapsto (\varphi_1(a_1, \ldots, a_n), \ldots, \varphi_n(a_1, \ldots, a_n)), \quad R^n \to R^n.$$

$\varphi = (\varphi_1, \ldots, \varphi_n), g = (g_1, \ldots, g_n) \in R[\mathbf{x}]^n$ に対して合成 $\circ$ を

$$\varphi \circ g = (\varphi_1(g_1, \ldots g_n), \ldots, \varphi_n(g_1, \ldots, g_n))$$

で定める．多項式写像 $\varphi \in R[\mathbf{x}]^n$ に対し $\varphi \circ g = (x_1, \ldots, x_n)$ を満たす $g \in R[\mathbf{x}]^n$ が存在するとき，即ち合成して恒等写像になるような多項式写像が存在するときに，φ は *invertible* と呼ばれる．さて多項式写像 $\varphi \in R[\mathbf{x}]^n$ は R 代数 $R[\mathbf{x}]$ の自己準同型とみなすことができる．

$$\varphi : f \mapsto \varphi(f) = f \circ \varphi, \quad R[\mathbf{x}] \to R[\mathbf{x}].$$

多項式写像 φ が invertible となることと，自己準同型 φ が自己同型となることは同値である．$\psi \in R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ に対して，基本自己同型 (elementary automorphism) と呼ばれる同型写像

$$(x_1, \ldots, x_{i-1}, x_i + \psi, x_{i+1}, \ldots, x_n) \in R[\mathbf{x}]^n$$

は，invertible な多項式写像になる．また invertible となる $\varphi \in R[\mathbf{x}]^n$ が $\deg \varphi_j \leq 1\ (1 \leq j \leq n)$ を満たすならば，*affine* と呼ばれる．affine および elementary な自己同型とその合成のみで表される自己同型は *tame* と呼ばれ, その全体は $\mathrm{T}(R, \{x_1, \ldots, x_n\})$ で表される．一方，$\mathrm{T}(R, \{x_1, \ldots, x_n\})$ に含まれない多項式写像は *wild* と呼ばれる．

本稿では黒田茂による考察に基づいた wild な多項式写像の構成法と，それを用いた共通鍵暗号を考察する．

2. Our key exchange protocol

$\mathbb{F}_p$ 上において下記の鍵共有方式を提案する．

1. $\sigma \in \mathbb{F}_p^n$ および $\tilde{f} \in \mathbb{F}_p[\mathbf{x}]$ に対し , Alice は $f := \tilde{f} - \tilde{f}(\sigma)$ を構成して Bob に送る．
2. Bob は $g, c \in \mathbb{F}_p[\mathbf{x}]^n$ を Alice へ送る: $\Psi, g, r \in R[\mathbf{x}]^n$ のうち Ψ, g が invertible であり $\deg g_i \leq 1\ (1 \leq i \leq n)$ となるもの選ぶ．$c := \Psi \circ g + f \cdot r$ とおく．
3. このとき, Alice は $u = c(\sigma)$ と共通鍵 $s = g(\sigma)$ を計算することができる．Alice は u を Bob へ送る．
4. Bob は次のようにして s を計算することができるので，上記は共通鍵方式として成立する．

$$\Psi^{-1}(u) = \Psi^{-1}(c(\sigma)) = \Psi^{-1}(\Psi \circ g(\sigma) + f(\sigma) \cdot r(\sigma)) = g(\sigma) = s.$$

このような鍵共有方式の共通鍵を求める安全性を，多項式の連立方程式の求解の困難性に帰着させて，安全の根拠を以下に担保することを考える:

命題 1. 上の鍵共有方式において, 通信路を通る情報 $f, g, c, c(\sigma)$ から共通鍵 s を求める問題は次の連立方程式の解を求める問題へ多項式時間で帰着される *:*

$$\begin{cases} c_1(x_1, \ldots, x_n) & = c_1(\sigma) \\ \qquad\vdots & \\ c_n(x_1, \ldots, x_n) & = c_n(\sigma) \\ f(x_1, \ldots, x_n) & = 0 \end{cases}$$

[1] 日大理工・院 (後)・数学
[2] 日大理工・教員・数学
[3] 株式会社東芝　研究開発センター
[4] 本研究は JSPS 科学研究費基盤研究 (C), 課題番号 26520208 の補助を受けております．

3. Derivations

Rを整域とする．加法に関する準同型 $D : R \to R$ が次の条件を満たすときに D を導分と呼ぶ．

$$D(ab) = D(a)b + aD(b) \ (^{\forall}a, b \in R).$$

$\mathrm{Ker}D = \{a \in R \mid D(a) = 0\}$ とする．任意の元 $a \in R$ に対して次の条件を満たす導分 D を局所冪零と言う．

$$D^i(a) = 0 \ (^{\exists}i \geq 1).$$

例えば $R[x_1, \ldots, x_n]$ の導分 D で各 i で $D(x_i) \in R[x_1, \ldots, x_{i-1}]$ となるようなものは局所冪零となるが，このような導分は三角導分と呼ばれる．ここで導分 D が局所冪零であれば fD ($f \in \mathrm{Ker}D$) も局所冪零導分となることに注意しよう．さて標数零の整域 R 上の局所冪零導分 D に対し，指数写像と呼ばれる次のような R の自己同型を定義する．

$$\exp D(g) := \sum_{i \geq 0} \frac{1}{i!} D^i(g) \ (^{\forall}g \in R).$$

4. Wild polynomial maps

I. P. Shestakov と U. U. Umirbaev は，標数零の体 k に対し，次を示した [4,5].

$$\mathrm{T}(k, \{x_1, x_2, x_3\}) \cap \mathrm{Aut}(k[x_1, x_2, x_3]/k[x_1]) = \mathrm{T}(k[x_1], \{x_2, x_3\})$$

ただし，$\mathrm{Aut}(k[x_1, x_2, x_3]/k[x_1])$ は x_1 を不変にする $k[x_1, x_2, x_3]$ の自己同型全体である．また黒田は整域 R に対し $V(R) := \{\frac{\alpha}{\beta} \in Q(R) \mid \alpha R + \beta R = R\}$ を定め，以下を証明した．

定理 1 (Theorem 2.2 in Chapter 3[6])．Rを標数零の整域とする．$R[y_1, y_2]$ の導分 D として $D(y_1) = a \neq 0, D(y_2) = \sum_{i=0}^{l} b_i y_1^i$ ($b_i \in R,\ b_l \neq 0$). を満たすものを考える．$f \in \mathrm{Ker}D \setminus R$，$Q(R)^{\times} = V(R)$ に対し，次が成立する．

$$\exp fD \in \mathrm{T}(R, \{y_1, y_2\}) \Leftrightarrow b_i \in aR \ (^{\forall}i \geq 1).$$

この定理において $R = k[x_1]$ で $y_1 = x_2, y_2 = x_3$ とすれば Shestakov と Umirbaev の結果から次の 3 変数の場合の wild 性の判定条件が得られる．

定理 2 (Theorem 2.3 in Chapter 3 [6])．D は $k[x_1, x_2, x_3]$ の三角導分で $D(x_1) = 0$ かつ $D(x_i) \neq 0$ ($i = 2, 3$) となるものとする．$f \in \mathrm{Ker}D \setminus k[x_1]$ に対し，次が成立する．

$$\exp fD \in \mathrm{T}(k, \{x_1, x_2, x_3\}) \Longleftrightarrow \frac{\partial}{\partial x_2} D(x_3) \in D(x_2)k[x_1, x_2].$$

5. Our results

2 節で提案する鍵共有方式での Ψ として, wild な自己同型写像を採用するために, まず黒田の定理 1 の正標数における類似として，正標数の指数写像を定義する．

定義 1. R は標数 $p > 0$ の整域，D はその導分とする．$\mathrm{Exp}_p D := \sum_{i=0}^{p-1} \frac{1}{i!} D^i$ とおき，

$$\mathrm{Exp}D = (\mathrm{Exp}_p D(x_1), \ldots, \mathrm{Exp}_p D(x_n))$$

と定める．$\mathrm{Exp}D$ は環準同型になる．

我々は正標数の指数写像に対し，以下が成り立つことを証明した．

定理 3. Rを標数 $p > 0$ の整域とする．導分 D は $a := D(y_1)$, $D(y_2) = \sum_{i=0}^{p-2} b_i y_1^i$ ($b_i \in R$) という形を持つと仮定する．$D(y_i) \neq 0$ とする．$f \in R[h_D] \setminus R$ に対し，次が成立する．

$$b_i \notin aR \ (^{\exists}i \geq 1) \ \Rightarrow \ \mathrm{Exp}fD \notin \mathrm{T}(R, \{y_1, y_2\}).$$

ただし $h_D := ay_2 - \sum_i \frac{b_i}{i+1} y_1^{i+1}$ である．

References

[1] K. Akiyama and N. Hirata-Kohno, A Key Exchange Protocol using Polynomial Map, 2017 Symposium on Cryptography and Information Security, Naha, IECE (2017).

[2] I. P. Shestakov and U. U. Umirbaev, Poisson Brackets and Two-Generated Subalgebras of Rings of Polynomials, J. Amer. Math. Soc., **17**, No.1 (2003), 181–196.

[3] I. P. Shestakov and U. U. Umirbaev, The Tame and The Wild Automorphisms of Polynomial Rings in Three Variables, J. Amer. Math. Soc., **17**, No.1 (2003), 197–227.

[4] S. Kuroda, Wildness of polynomial automorphisms in three variables, arXiv: 1110.1466v1, (2011).

[5] S. Kuroda, Wildness of polynomial automorphisms : Applications of the Shestakov-Umirbaev theory and its generalization, RIMS Kokyuroku Bessatsu, Kyoto University, B. 24 (2011), 103–120.