ISSN 2186-5647

6-11

Rainbow-Band-Separation 攻撃における連立代数方程式の性質

日大生産工　○中村 周平

1 導入

連立代数方程式とは, 次のような多項式により表される幾つかの変数の間の関係式の組のことである.

$$\begin{cases} 4x_3+3x_2+2x_3^2+x_2x_3+x_1x_3 & =1 \\ 2x_3+3x_2+2x_1+4x_3^2+2x_2x_3+2x_1x_3 & =2 \\ x_1+x_3^2+3x_2x_3+3x_1x_3 & =3 \end{cases}$$

また, 連立代数方程式を解くということは, ここではこの関係式たちを満たす変数の組を求めることであり, そのようなものが存在しない場合は空集合を返すこととする. 例えば, 各多項式の次数が 1 次の場合の連立代数方程式問題は, 行列に対応させることにより, 行に関する掃き出しを行うことで解を求める方法が一般に知れらている. しかしながら, 一般の次数に関する連立代数方程式求解問題は難しく, 次数 2 の場合でさえ, 有限体上で NP 完全性を有することが知られている.

連立代数方程式の求解問題は, その素朴さから数学の様々なところで重要となるが, 暗号においても重要な対象として考えられている. 現在, 身の回りで多く用いられている暗号は, 素因数分解問題や離散対数問題などの数学の問題に関連したものを基に設計され, 問題の効率的な解法がないことがその暗号の安全性を保証している. しかしながら, これらの数学の問題は量子計算機を用いて多項式時間で求解可能であることが知られるようになり, その量子計算機の急速な開発の発展から, 耐量子暗号と呼ばれる量子計算機の攻撃に耐性のある暗号を設計することが要請されている. 先ほどの連立代数方程式の求解問題はこのような量子計算機による計算にも耐性があるものと期待され, この問題を基にした多変数多項式暗号 ([2]) は耐量子暗号の候補となっている.

2 多変数暗号

ここでは, 基本的な記号や記法を導入し, 多変数多項式暗号の定式化を行う.

体 k において k 上の n 変数の多項式のなす集合の全体を $k[x_1,\dots,x_n]$ で表す. また, 多項式環の m 個の直和 $(k[x_1,\dots,x_n])^m$ の元 $F=(f_1,\dots,f_m)$ は, k 上 n 次元線形空間 k^n から k 上 m 次元線形空間 k^m への写像 $k^n \to k^m$ を次のようにして定める:

$$(a_1,\dots,a_n) \mapsto (f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n))$$

このように定まる写像は多項式写像と呼ばれる. このとき, 多変数多項式暗号は次の 3 つのアルゴリズムを用いて機能する ([2]).

1. セキュリティパラメータ sk に対して, 秘密鍵 S,F,T が生成される. ただし, S,T は全単射な線形変換である.
2. $a \in k^n$ に対して, $P(a)$ を計算する. ただし, $P=(p_1,\dots,p_n)=T\circ F\circ S$ である.
3. $b=(b_1,\dots,b_m)\in k^m$ に対して, $P^{-1}(b)=T^{-1}(F^{-1}(S^{-1}(b)))$ を計算する.

暗号化方式の場合, 2 は暗号化, 3 は復号のプロセスに対応する. また, 署名方式であれば, 3 は署名, 2 は検証のプロセスに対応するものとなる. これらの方式において, 暗号文 (もしくは平文) として $b\in k^m$ が与えられたとき $P^{-1}(b)$ から平文 (もしくは署名文) を得る攻撃は, 次の連立代数方程式の求解に対応する.

$$\begin{cases} p_1(x_1,\dots,x_n)=b_1 \\ \vdots \\ p_m(x_1,\dots,x_n)=b_m \end{cases}$$

Properties of the dominant polynomial system in the Rainbow-Band-Separation attack

Shuhei NAKAMURA

ここで, この暗号から生じる連立代数方程式は一般に幾つかの条件を含んでいることに注意したい. 例えば, 体 k として利用されるのは有限体であり, 連立代数方程式の解はその体上で求める. また, 暗号は構成の仕方から, 必ず付随する連立代数方程式が解をもつことも判る. さらに重要な点として, 暗号への応用から公開鍵のサイズを抑えるため $\deg p_i = 2$ であることが要求される. この場合においても, 連立代数方程式の解を求めることが困難とされる理由は次の問題の NP 完全性にある:

問 1. 位数 2 の有限体 $\mathbb{F}_2$ と任意の自然数 m, n に対して $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ とする. このとき, $p_1(x_1, \ldots, x_n) = 0, \ldots, p_m(x_1, \ldots, x_n) = 0$ の解を求めよ.

3 Rainbow 暗号に対する Rainbow-Band-Separation 攻撃

与えられた正整数 v, o_1, o_2 に対して $n := v+o_1+o_2$, $m := o_1 + o_2$ とおく. 多変数多項式暗号である Rainbow 暗号 ([2]) の中心写像 $F = (f_1, \ldots, f_m)$ は最高斉次部分が次の対称行列に対応する二次多項式系として定義される:

$$M_{f_i} = \begin{cases} \begin{pmatrix} A_{v\times v} & A_{v\times o_1} & O_{v\times o_2} \\ A_{v\times v} & O_{v\times o_1} & O_{v\times o_2} \\ O_{v\times v} & O_{v\times o_1} & O_{v\times o_2} \end{pmatrix} & \text{if } 1 \le i \le o_1 \\ \begin{pmatrix} A_{v\times v} & A_{v\times o_1} & A_{v\times o_2} \\ A_{v\times v} & A_{v\times o_1} & A_{v\times o_2} \\ A_{v\times v} & A_{v\times o_1} & O_{v\times o_2} \end{pmatrix} & \text{if } o_1+1 \le i \le o_1+o_2 \end{cases}$$

ただし, $A_{i\times j}$ は $\mathrm{Mat}_{i\times j}(k)$ から選ばれたランダムな元であり, $O_{i\times j}$ は $\mathrm{Mat}_{i\times j}(k)$ での零行列を意味する.

Rainbow-Band-Separation 攻撃 Rainbow 暗号に対する Rainbow-Band-Separation 攻撃は次のプロセスからなる秘密鍵を復元するアルゴリズムである ([3]):

第 i プロセス $(1 \le i \le o_2)$

座標変換 $x_1 = x'_1 - \lambda_1 x'_{n-i+1}, \ldots, x_{v+o_1} = x'_{v+o_1} - \lambda_{v+o_1} x'_{n-i+1}$ により $p_1, \ldots, p_m$ から $p'_1, \ldots, p'_m$ を得る. $p'_1, \ldots, p'_m$ における $x'_{n-j+1}x'_{n-i+1}$ $(1 \le \forall j \le i)$ の係数と $p_i - \lambda_{v+o_1+1}p'_{o_1+1} - \cdots - \lambda_{v+o_1+o_2}p'_{o_1+o_2}$ に含まれる $x'_l x'_{n-i+1}$ $(1 \le \forall l \le n-1)$ の係数は 0 となる必要があるため, $i\times m+n-1$ 本の n 変数代数方程式を得る. この連立代数方程式を解いた後, その解を代入した $p'_1, \ldots, p'_m$ を改めて $p_1, \ldots, p_m$ で表す.

第 i プロセス $(o_2+1 \le i \le o_2+o_1)$

変数変換 $x_1 = x'_1 - \lambda_1 x'_{n-i+1}, \ldots, x_v = x'_v - \lambda_v x'_{n-i+1}$ により $p_1, \ldots, p_m$ から $p'_1, \ldots, p'_m$ を得る. $p'_1, \ldots, p'_m$ に含まれる $x'_{n-j+1}x'_{n-i+1}$ $(1 \le \forall j \le i)$ の係数は 0 となる必要があるため, $i \times o_1$ 本の v 変数代数方程式を得る. この連立代数方程式を解いた後, その解を代入した $p'_1, \ldots, p'_m$ を改めて $p_1, \ldots, p_m$ で表す.

本研究の結果 文献 [4] において, この攻撃の計算時間は第 1 プロセスで解く $n+m-1$ 本の n 変数 2 次多項式からなる連立代数方程式により支配されることが実験的に示されている. また, 彼らは対応する多項式系が準正則 (semi-regular) であることを仮定し, degree of regularity d_{reg}([1]) を用いて計算量が与えられているが, 実験的にほとんどの多項式系は準正則ではないことが観ることができる. このような準正則でない多項式系に対しては, first fall degree と呼ばれる計算量を見積もる次数で測ることが一般的であり ([2]), 本研究では次の主張を示す:

定理 1. Rainbow-Band-Separation 攻撃において第 1 プロセスで解く多項式系の first fall degree は 3 以下となる.

さらに講演では, この主張の系として, 暗号で有用とされる Rainbow 暗号のパラメータに対して第 1 プロセスで解く多項式系が準正則列とならないことを理論的に示す.

参考文献

[1] M. Bardet, J-C. Faugére and B. Salvy, On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, ICPPSS International Conference on Polynomial System Solving, 2004

[2] J. Ding, J. E. Gower and D. S. Schmidt, Multivariate Public Key Cryptosystems, Springer, New York, 2006

[3] J. Ding, J., B.-Y. Yang, C.-H. O. Chen, M.-S. Chen and C.-M. Cheng. New differential-algebraic attacks and reparametrization of Rainbow. In ACNS, volume 5037 of Lecture Notes in Computer Science, pages 242–257. Springer, 2008.

[4] A. Petzoldt, S. Bulygin and J. Buchmann. Selecting Parameters for the Rainbow Signature Scheme. In PQCrypto, volume 6061 of Lecture Notes in Computer Science, pages 218 - 240. Springer, 2010.