M_031

順序解法を原方式に持つ非線形持駒方式の安全性に関する一考察

On the security of Piece In Hand Concept based on Sequential Solution Method

福島 啓友† 伊藤 大介† 金子 敏信†
Yoshitomo FUKUSHIMA Daisuke ITO Toshinobu KANEKO

1 はじめに

多次元多変数型公開鍵暗号は1980年代初頭から研究が進められてきた。そのひとつとして1986年に辻井らによって提案された順序解法による公開鍵暗号方式がある。

順序解法を原方式に持つ線形持駒方式 [1] は2003年に辻井らによって提案された多次元多変数型公開鍵暗号を強化する手法である。また、2004年に辻井らは、持駒行列を非線形行列にした構成を提案し [2]、2006年にさらに改良した構成法を提案した [3]。非線形持駒方式は持駒行列と呼ばれる秘密鍵の行列を使用して、多次元多変数型公開鍵暗号方式を強化する手法である。

我々は順序解法を原方式に持つ線形持駒行列に対する攻撃を既に示したが [4]、本稿では順序解法を原方式に持つ非線形持駒方式 [3] の安全性について考察する。

2 順序解法型非線形持駒暗号方式

辻井らが提案している非線形持駒方式を、順序解法型構造に適用したものを以下に説明する。

2.1 順序解法型構造

非線形連立方程式を適切な中間変数 $\boldsymbol{u} = (u_1, \ldots, u_k)$、$\boldsymbol{w} = (w_1, \ldots, w_k)$ を使って式 (1) のように整理し、これらの式を u_k から $u_{k-1} \cdots u_1$ の順に解くことができる場合、元の非線形連立方程式は順序解法型構造を持つという。

$$\begin{aligned} w_1 &= h_1(u_1, u_2, \ldots, u_k) \\ w_2 &= h_2(u_2, u_3, \ldots, u_k) \\ &\vdots \\ w_{k-1} &= h_{k-1}(u_{k-1}, u_k) \\ w_k &= h_k(u_k) \end{aligned} \tag{1}$$

辻井らの論文では、簡単に解ける式として1次式を用いている。即ち $w_k = h_k(u_k)$ は u_k の1次式であり、それを解いて u_k を求め、求めた値を $h_{k-1}(u_{k-1}, u_k)$ に代入することにより、u_{k-1} を求める。この繰り返しで中間変数 $u_k \cdots u_1$ が簡単に解けることを利用した非線形連立方程式型公開鍵暗号を順序解法型公開鍵暗号という。

辻井らは持駒方式を、任意の非線形連立方程式型の公開鍵暗号を強化する方式として位置づけているが、本稿では順序解法型公開鍵暗号を原方式とする持駒暗号方式を対象とする。

2.2 非線形持駒方式

辻井らが提案する多次元多変数型公開鍵暗号は $\mathbf{F}_q$ 上の暗号方式である。その暗号方式において、平文ベクトルは $\boldsymbol{x} = (x_1, x_2 \ldots, x_k)$、暗号文ベクトルは $\boldsymbol{y} = (y_1, y_2 \ldots, y_n)$ $(x_i, y_i \in \mathbf{F}_q \ \ and \ \ n > k)$ で表されている。

非線形持駒方式の暗号文ベクトルは公開鍵ベクトル $\tilde{E}(\boldsymbol{x})$ で表すと次式のように表される。

$$\boldsymbol{y} = \tilde{E}(x) = B \begin{pmatrix} \bar{E}(\boldsymbol{x}) \\ C(\boldsymbol{x}) \end{pmatrix} \tag{2}$$

行列 B は正則行列である。$C(\boldsymbol{x})$ は2次以下の多項式ベクトルである。以下に本方式で使用する数式を挙げる。$\bar{E}(\boldsymbol{x})$ は式 (3)(4)(5) より求まる。式 (6) は復号に使用する。本方式での公開鍵は $\tilde{E}(\boldsymbol{x})$ と q であり、秘密鍵は B、M、S、R、T、$\boldsymbol{u}$、$E(\boldsymbol{x})$ である。

$$MS = I, MR = 0 \tag{3}$$

$$F(\boldsymbol{x}) = E(\boldsymbol{x}) - TC(\boldsymbol{x}) - \boldsymbol{u} \tag{4}$$

$$\bar{E}(\boldsymbol{x}) = S \begin{pmatrix} 1 \\ F(\boldsymbol{x}) \end{pmatrix} + R\bar{X} \tag{5}$$

$$\tilde{M}(\boldsymbol{x}) = \begin{pmatrix} TC(\boldsymbol{x}) + \boldsymbol{u} & I \end{pmatrix} M \tag{6}$$

$$\bar{X} = (x_1^2, x_1 x_2, \ldots, x_k^2, x_1, \ldots, x_k, 1)^T \tag{7}$$

行列 M、S、R は式 (3) を満たすように定める。$E(\boldsymbol{x})$ は原方式における公開鍵である。行列 T とベクトル $\boldsymbol{u}$ は任意に定める。行列 I は単位行列である。詳しくは文献 [3] を参照。

2.3 非線形持駒方式における暗号化と復号

2.3.1 暗号化

公開鍵ベクトル $\tilde{E}(\boldsymbol{x})$ は x についての2次式ベクトルであり、各項の係数が公開されている。ここで E_k は公開鍵係数行列である。

$$\boldsymbol{y} = \tilde{E}(\boldsymbol{x}) = E_k \bar{X} \tag{8}$$

暗号化においては平文ベクトルから単項式ベクトル $\bar{X}$ を計算し、式 (8) で暗号文ベクトル $\boldsymbol{y}$ を得る。

† 東京理科大学

2.3.2 復号

正当な受信者は秘密鍵情報を持っているので以下のように復号する。B^{-1} を乗算し、$\bar{E}(\boldsymbol{x})$ および $C(\boldsymbol{x})$ を得る。

$$B^{-1}\tilde{E}(\boldsymbol{x}) = \begin{pmatrix} \bar{E}(\boldsymbol{x}) \\ C(\boldsymbol{x}) \end{pmatrix} \tag{9}$$

次に式 (6) と $C(\boldsymbol{x})$ から $\tilde{M}(\boldsymbol{x})$ を得る。そして、次の式から $E(\boldsymbol{x})$ を得る。

$$E(\boldsymbol{x}) = \tilde{M}(\boldsymbol{x})\bar{E}(\boldsymbol{x}) \tag{10}$$

この $E(\boldsymbol{x})$ を順序解法で解き、平文を得る。

3 解読原理

本稿で述べる解読手法は、順序解法を原方式に持つ非線形持駒方式が以下の 3 つの性質を持つことを利用している。

【性質】

性質 1 $\tilde{E}(\boldsymbol{x})$ の係数行列 E_k の行空間に $E(\boldsymbol{x})$ の係数行列の行ベクトルが含まれる。

性質 2 公開鍵係数行列 E_k に 2 次項係数を消去するような適切な行基本操作を行えば、簡単な式 (1 次式) が少なくとも 1 本出てくる。

性質 3 順序解法の構造より、簡単な式を解いた値を他の式に代入し、適切な行基本操作を行えば次に解くべき簡単な式が順次現れる。

【証明】

証明 1 (9) 式より $\tilde{E}(\boldsymbol{x})$ の係数行列 E_k の各行の線形結合で $\bar{E}(\boldsymbol{x})$、$C(\boldsymbol{x})$ の係数行列を表すことができる。(5) 式より $F(\boldsymbol{x})$ の係数行列は $\bar{E}(\boldsymbol{x})$ の係数行列の各行の線形結合で表すことができる。(4) 式より $E(\boldsymbol{x})$ の係数行列は $F(\boldsymbol{x})$ と $C(\boldsymbol{x})$ の係数行列の各行の線形結合で表すことができる。よって $E(\boldsymbol{x})$ の係数行列は $\tilde{E}(\boldsymbol{x})$ の係数行列 E_k の各行の線形結合で表すことができる。よって $\tilde{E}(\boldsymbol{x})$ の係数行列 E_k の部分空間に $E(\boldsymbol{x})$ の係数行列の行ベクトルが含まれる。

証明 2 $E(\boldsymbol{x})$ は順序解法を原方式に持つので、$E(\boldsymbol{x})$ に適切な行基本操作を行うと簡単な式 (1 次式) が出てくる。性質 1 より $\tilde{E}(\boldsymbol{x})$ に適切な行基本操作を行っても簡単な式が出てくる。よって、2 次項以上を消去するような行基本操作を $\tilde{E}(\boldsymbol{x})$ に行えば、簡単な式が少なくとも 1 本は出てくるはずである。もし 1 本も出てこないのなら、$\tilde{E}(\boldsymbol{x})$ の部分空間には簡単な式が含まれていないことになり、$E(\boldsymbol{x})$ の行基本操作を行っても簡単な式が出てこないことになる。これは $E(\boldsymbol{x})$ が順序解法で解けるということに矛盾するので、少なくとも 1 本は簡単な式が出てくる。

証明 3 2.1 節の説明より、k 変数、k 本の順序解法型非線形連立方程式において、簡単に解ける式の解を他の $k-1$ 本の式に代入すれば残りは $k-1$ 本の順序解法型非線形連立方程式になる。このことと性質 2 の考えをあわせれば明らかである。

4 解読手順

前節で述べた解読原理を解読手順としてまとめると以下のようになる。

step1 公開鍵係数行列 E_k を行基操作により既約台形正準形に変形する。ここでは 2 次項係数を消去するよう、行基本操作を適用する。

step2 既約台形正準形の行ベクトル内の簡単な式 (1 次式) を探す。

step3 得られた簡単な式が順序解法で解くべき最初の式である。その式の値を既知定数と考え、式に含まれる 1 平文要素を他の式に代入し、変数の 1 つ少ない公開鍵係数行列 E_{k-1} を作る。既に得られた簡単な式の本数が k 本未満の場合は step1 へ。

step4 step3 で得られた k 本の式を解くことで、平文を得ることができる。

5 まとめ

順序解法を原方式に持つ非線形持駒方式に対して、順序解法構造の特徴を利用した攻撃を提案した。この攻撃を用いることにより公開鍵情報から解読ができることを示した。

参考文献

[1] Shigeo Tsujii, Ryou Fujita, and Kohtaro Tadaki. "Proposal of MOCHIGOMA (Piece in hand) concept for multivariate type public key cryptosystem" , IEICE Technical Report, ISEC 2004-74, September 2004.

[2] Shigeo Tsujii, Kohtaro Tadaki, Ryou Fujita, "Piece In Hand Concept for Enhancing the Security of Multivariate Type Public Key Cryptosystems: Public Key Without Containing All the Information of Secret Key", Cryptology ePrint Archive, Report 2004/266, December 2004. http://eprint.iacr.org/2004.366

[3] 辻井重男, 只木孝太郎, 藤田亮、" 持駒行列の提案 その2 -多変数多項式型公開鍵暗号の安全性強化のための汎用的手法－" SCIS 2006, Jan. 17-20, 2006.

[4] 伊藤大介, 福島啓友, 金子敏信, " 順序解法を原方式に持つ線形持駒方式の安全性に関する一考察" ISEC2006, July.20,2006. (発表予定)