Linear Piece In Hand matrix method and plus method

Kohtaro Tadaki

Research and Development Initiative, Chuo University
JST CREST
Tokyo, Japan

The Second CREST-SBM International Conference
Harmony of Gröbner Bases and the Modern Industrial Society
June 28 – July 02, 2010, Osaka, Japan

Abstract

In 2007, we proposed the linear Piece In Hand (PH, for short) matrix method with random variables. It is a general prescription which can be applicable to any type of multivariate public-key cryptosystems (MPKCs, for short) for the purpose of enhancing their security.

In 1998 Patarin, Goubin, and Courtois introduced the plus method as a general prescription which aims to enhance the security of any given MPKC, just like the linear PH matrix method with random variables.

In this talk, we show that the linear PH matrix method with random variables has an advantage over the plus method with respect to the security enhancement.

Scheme of MPKCs

A **multivariate public key cryptosystem (MPKC, for short)** can be considered to comply with the following scheme:

- Plain Text: a column vector $\boldsymbol{p} = (p_1, \ldots, p_k)^T \in \mathbf{F}_q{}^k$.
- Cipher Text: a column vector $\boldsymbol{c} = (c_1, \ldots, c_n)^T \in \mathbf{F}_q{}^n$.
- Public Key: a polynomial column vector $\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$.

  Encryption: the transformation from $\boldsymbol{p}$ to $\boldsymbol{c}$ by the sender, Alice:

  $$\boldsymbol{c} = \boldsymbol{E}(\boldsymbol{p}).$$

- Secret Key: an efficient method to solve the system $\boldsymbol{E} = \boldsymbol{c}$ of polynomial equations on $(x_1, \ldots, x_k)$ for any given $\boldsymbol{c} \in \mathbf{F}_q{}^n$.

  Decryption: the execution of this method by the legitimate receiver, Bob, for the cipher text $\boldsymbol{c}$ sent from the sender to recover the plain text $\boldsymbol{p}$.

Therefore, $\boldsymbol{E}$ has to be constructed so that, without the knowledge about this method, it is difficult to find $\boldsymbol{p}$ for any given $\boldsymbol{c}$ in polynomial-time.

Linear PH Matrix Methods

In our former works, we proposed the linear Piece In Hand (PH, for short) matrix methods. They are a general prescription which can be applicable to any type of MPKCs for the purpose of enhancing their security as follows.

Let $\mathcal{K}$ be an arbitrary MPKC whose public key is given by $\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$. By the application of linear PH matrix method to the original public key $\boldsymbol{E}$, a new MPKC $\widetilde{\mathcal{K}}$ can be constructed for the purpose of enhancing the security.

$\mathcal{K}$ $\Rightarrow$ $\widetilde{\mathcal{K}}$

Any MPKC (Possibly) Enhanced MPKC

Linear PH Matrix Method

Primitive Linear PH Matrix Method

Primitive Linear PH Matrix Method (1)

The primitive linear PH matrix method is introduced by our previous work [S. Tsujii, K. Tadaki, and R. Fujita, Cryptology ePrint Archive, Report 2004/366, Dec. 2004] to explain the notion of the linear PH matrix methods in general in an illustrative manner and not for a practical use to enhance the security of any given MPKC.

A public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \ldots, x_k]^l$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $\boldsymbol{E}$ of $\mathcal{K}$ by the transformation:

$$\widetilde{\boldsymbol{E}} := S\boldsymbol{E} + R\boldsymbol{X}.$$

Here,

- $\boldsymbol{X}$: a polynomial column vector whose components are all monomials in $\mathbf{F}_q[x_1, \ldots, x_k]$ of total degree at most two, namely,

$$\boldsymbol{X} := (x_1x_1, x_1x_2, \ldots, x_{k-1}x_k, x_kx_k, x_1, x_2, \ldots, x_k, 1)^T.$$

- S: a matrix in ${\mathbf{F}_q}^{l \times n}$ with $l > n$.
- R: a matrix in ${\mathbf{F}_q}^{l \times t}$, where t is the number of components of $\boldsymbol{X}$.

The term $R\boldsymbol{X}$ plays a role in randomizing $\widetilde{\boldsymbol{E}}$.

Primitive Linear PH Matrix Method (2)

- In addition to S and R, the PH matrix $M \in \mathbf{F}_q{}^{n \times l}$ is introduced as a secret key of $\widetilde{\mathcal{K}}$.

In the key-generation stage, the matrices S, R, and M are chosen so as to satisfy the following condition.

Condition $MR = 0$ and $MS = I_n$, where I_n is the identity matrix in $\mathbf{F}_q{}^{n \times n}$. □

This choice can be efficiently possible.

$$M\widetilde{\boldsymbol{E}} = \boldsymbol{E} \qquad \text{(by the above } \textbf{Condition}\text{)}.$$

Primitive Linear PH Matrix Method (3)

- A plain text of $\widetilde{\mathcal{K}}$: a column vector $\boldsymbol{p} \in {\mathbf{F}_q}^k$ (the same as in $\mathcal{K}$).
- A cipher text of $\widetilde{\mathcal{K}}$: a column vector $\tilde{\boldsymbol{c}} \in {\mathbf{F}_q}^l$ calculated by $\tilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}(\boldsymbol{p})$.

- Public Key of $\widetilde{\mathcal{K}}$: $\widetilde{\boldsymbol{E}}$.
- Secret Key of $\widetilde{\mathcal{K}}$: The PH matrix M, together with the secret key of $\mathcal{K}$ corresponding to the public key $\boldsymbol{E}$ of $\mathcal{K}$.

The decryption of $\widetilde{\mathcal{K}}$ proceeds as follows:

[1] Based on the relation $M\widetilde{\boldsymbol{E}} = \boldsymbol{E}$, on receiving the cipher text $\tilde{\boldsymbol{c}} := \widetilde{\boldsymbol{E}}(\boldsymbol{p})$ for a plain text $\boldsymbol{p}$, Bob can efficiently calculate the cipher text $\boldsymbol{c}$ $(= \boldsymbol{E}(\boldsymbol{p}) = M\tilde{\boldsymbol{c}})$ of the original MPKC $\mathcal{K}$.

[2] According to the decryption procedure of $\mathcal{K}$, Bob can recover the plain text $\boldsymbol{p}$ using the secret key of $\mathcal{K}$.

Gröbner Basis Attack

In 2003 Faugère and Joux showed in an experimental manner that computing a Gröbner basis of the public key is likely to be an efficient attack to HFE, which is one of the major variants of MPKCs.

The attack is simply to compute a Gröbner basis for the ideal generated by polynomial components in $\boldsymbol{E} - \boldsymbol{c}$, where $\boldsymbol{E}$ is a public key and $\boldsymbol{c}$ is a cipher text vector.

$\Rightarrow$

Because of the simplicity of this attack, it may be a threat to the primitive linear PH matrix method as well.

Countermeasure against the Gröbner Basis Attack

In the primitive linear PH matrix method, the public key $\widetilde{\boldsymbol{E}}$ of $\widetilde{\mathcal{K}}$ and the public key $\boldsymbol{E}$ of $\mathcal{K}$ satisfy the relation $M\widetilde{\boldsymbol{E}} = \boldsymbol{E}$. This fact may make the primitive linear PH matrix method vulnerable to the Gröbner basis attack.

$\Rightarrow$

A countermeasure against the vulnerability is to introduce additional variables $x_{k+1}, \ldots, x_m$ to the public key $\widetilde{\boldsymbol{E}}$ of $\widetilde{\mathcal{K}}$.

Under this countermeasure, solving the system $\widetilde{\boldsymbol{E}} - \widetilde{\boldsymbol{c}} = \boldsymbol{0}$ of polynomial equations on $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_m)$ seems to be more difficult than solving the system $\boldsymbol{E} - \boldsymbol{c} = \boldsymbol{0}$ of polynomial equations on $(x_1, \ldots, x_k)$.

This idea can be implemented properly by the linear PH matrix method with random variables [S. Tsujii, K. Tadaki, and R. Fujita, *IEICE Transactions on Fundamentals*, E90-A, No.5, pp. 992–999, 2007] as follows.

Linear PH Matrix Method with Random Variables

Linear PH Matrix Method with Random Variables

Let $\mathcal{K}$ be an arbitrary MPKC whose public key is given by $\boldsymbol{E} \in \mathbf{F}_q[x_1, \ldots, x_k]^n$. Then a new MPKC $\widetilde{\mathcal{K}}$ is constructed from $\mathcal{K}$ as follows.

Assume that $p < k < m$.

A public key $\widetilde{\boldsymbol{E}} \in \mathbf{F}_q[x_1, \ldots, x_m]^l$ of $\widetilde{\mathcal{K}}$ is constructed from $\boldsymbol{E}$ by

$$\widetilde{\boldsymbol{E}} := S\boldsymbol{E}\begin{pmatrix} \boldsymbol{x} \\ A\boldsymbol{z} \end{pmatrix} + R\boldsymbol{Z}.$$

Here,

- $\boldsymbol{x} = (x_1, \ldots, x_p)^T \in \mathbf{F}_q[x_1, \ldots, x_p]^p$ and $\boldsymbol{z} = (x_1, \ldots, x_m)^T \in \mathbf{F}_q[x_1, \ldots, x_m]^m$.
- $\boldsymbol{Z}$: a polynomial column vector whose components are all monomials in $\mathbf{F}_q[x_1, \ldots, x_m]$ of total degree at most two, namely, $\boldsymbol{Z} := (x_1x_1, x_1x_2, \ldots, x_{m-1}x_m, x_mx_m, x_1, x_2, \ldots, x_m, 1)^T$.

The additional variables $x_{k+1}, \ldots, x_m$ are introduced in this manner.

- Note that $A\boldsymbol{z}$ is needed to prevent an eavesdropper from forging the PH matrix through the elimination of the variables $x_{p+1}, \ldots, x_k$.

The existence of the additional additional variables $x_{k+1}, \ldots, x_m$ might provide substantial robustness against the Gröbner basis attack, as is suggested by the experimental results shown below.

Strength against the Gröbner Basis Attack

Comparison between running-times for HFE and the enhanced HFE by the linear PH matrix method with random variables in the Gröbner bases attack.

cryptosystems	p	$k(=n)$	m	l	running-times in second
HFE ($q=2$)		10			<1
($128<d<513$)		25			686
$\mathcal{K}$		28			1404
the enhanced HFE	10	20	30	25	1364
by the PH method	10	20	35	25	5301
($d<513$)	10	20	37	25	8788
$\widetilde{\mathcal{K}}$	10	20	32	28	3437
	10	20	36	28	9903
rank $R=l-n$	10	20	38	28	15091

d: The degree of the univariate polynomial in the HFE scheme.

- HP workstation with Alpha EV68 processor at 1.25 GHz and 32GB of RAM.
- F_4 in Magma V2.12-14.

The table suggests that the increase of the number $m-k$ of additional random variables $x_{k+1},\ldots,x_m$ increases the running-time of the Gröbner bases.

Aim of This Talk

We show that the linear PH matrix method with random variables has an advantage over the plus method with respect to the security enhancement.

Plus Method

The plus method is introduced by Patarin, Goubin, and Courtois in 1998 as a general prescription which aims to enhance the security of any given MPKC, just like the linear PH matrix method with random variables.

A public key $\widetilde{\boldsymbol{E}}_+ \in \mathbf{F}_q[x_1, \ldots, x_k]^l$ of $\widetilde{\mathcal{K}}$ is constructed from the original public key $\boldsymbol{E}$ of $\mathcal{K}$ by the transformation:

$$\widetilde{\boldsymbol{E}}_+ := B \begin{pmatrix} \boldsymbol{E} \\ Q\boldsymbol{X} \end{pmatrix}.$$

Here $\boldsymbol{X}$ is the same as in the primitive linear PH matrix method. B is an invertible matrix. On the other hand, Q is a matrix and the term $Q\boldsymbol{X}$ plays a role in randomizing $\widetilde{\boldsymbol{E}}_+$.

Equivalence of Two Primitive Methods

Based on the following theorem, we can show that the Plus method is equivalent to the primitive linear PH matrix method.

Theorem For every matrices S, R and M, $MR = 0$ and $MS = I_n$ hold if and only if there exist a matrix $B \in \mathbf{F}_q{}^{l\times(l-n)}$ and a matrix $Q \in \mathbf{F}_q{}^{(l-n)\times t}$ such that
(i) the square matrix $(S|B) \in \mathbf{F}_q{}^{l\times l}$ is invertible,
(ii) $M = (I_n|O_{n,l-n})(S|B)^{-1}$, and
(iii) $R = BQ$,
where I_a is the $a \times a$ identity matrix and $O_{b,c}$ is the $b \times c$ zero matrix. □

The primitive linear PH matrix method: $\widetilde{\boldsymbol{E}} := S\boldsymbol{E} + R\boldsymbol{X}$.

The Plus method: $\widetilde{\boldsymbol{E}}_+ := (S|B)\begin{pmatrix} \boldsymbol{E} \\ Q\boldsymbol{X} \end{pmatrix}$.

Advantage over the Plus Method

- The linear PH matrix method with random variables has an advantage over the primitive linear PH matrix method with respect to the immunity from the Gröbner basis attack.

- The primitive linear PH matrix method is equivalent to the plus method.

Thus, we can conclude that the linear PH matrix method with random variables has an advantage over the plus method with respect to the immunity from the Gröbner basis attack.

Summary

The linear Piece In Hand (PH, for short) matrix method with random variables was proposed in our former work. It is a general prescription which can be applicable to any type of multivariate public-key cryptosystems (MPKCs, for short) for the purpose of enhancing their security.

Actually, we showed, in an experimental manner, that the linear PH matrix method with random variables can certainly enhance the security of HFE against the Gröbner basis attack, where HFE is one of the major variants of MPKCs.

In 1998 Patarin, Goubin, and Courtois introduced the plus method as a general prescription which aims to enhance the security of any given MPKC, just like the linear PH matrix method with random variables.

In this talk we have proven the equivalence between the plus method and the primitive linear PH matrix method, which is introduced by our previous work to explain the notion of the linear PH matrix methods in general in an illustrative manner.

Based on this equivalence, we have shown that the linear PH matrix method with random variables has an advantage over the plus method with respect to the security enhancement.