Hidden Pair of Bijection Signature Scheme

Masahito Gotaishi and Shigeo Tsujii

Research and Development Initiative, Chuo University, 1-13-27 Kasuga, Tokyo, Japan, 112-8551 gotaishi@tamacc.chuo-u.ac.jp http://www.chuo-u.ac.jp/chuo-u/rdi/index_j.html

Abstract. A new signature system of multivariate public key cryptosystem is proposed. The new system, Hidden Pair of Bijection (HPB), is the advanced version of the Complementary STS system. This system realized both high security and quick signing. Experiments showed that the cryptanalysis of HPB by Gröbner bases has no less complexity than the random polynomial systems. It is secure against other way of cryptanalysis effective for Complementary STS.

On the other hand, since it is based on bijections, signatures exist for any message, unlike other cryptosystems based on non-bijections such as HFE or Unbalanced Oil and Vinegar.

Keywords: Multivariate Public Key Cryptosystem, Digital Signature, Bijection, Rainbow

1 Introduction

1.1 Multivariate Public Key Cryptosystem

Multivariate Public Key Cryptosystem (MPKC) is one of the important subjects of post-quantum cryptosystems. Its one-wayness is based on the knowledge that solving a set of multivariate polynomial equations over a finite field is NP-hard [10].

Among post-quantum cryptosystems, it would have the highest number of variants, with about 30 to 40 schemes proposed in the past. Although, according to the classification proposed by Wolf, et al. [24], the number of basic trapdoors of MPKCs is only four. Most of the MPKCs are created by modifying the basic trapdoors, such as by eliminating polynomials or adding some noise, to improve the security against attacks.

1.2 Central Map and Public Key of MPKC

An MPKC cryptosystem is created by building a polynomial system with trapdoor structure, whose inverse mapping is easily computed. Since it is well possible to analyze the structure of this polynomial system, the system cannot be directly used as the public key. Let $\mathbf{P}' \in \mathbf{F}_q[\mathbf{x}]^m$ be the polynomial system with the trapdoor. When a plain text $\mathbf{x} \in \mathbf{F}_q^n$ is encrypted, usually \mathbf{x} is transformed by affine

transform S beforehands. Thus obtained intermediate variable $v \in F_q^n$ is assigned to the polynomial system P'. Resulting vector $w \in F_q^m$ is transformed again by another affine transform T. The composite mapping $P := T \circ P' \circ S$ is used as the public key. The polynomial system P' is called "central map." The relationship among affine transformations, central map, and the public key is illustrated in the Figure 1.

In the signature scheme, \boldsymbol{y} is the document and the signature \boldsymbol{x} , which satisfies the equation $\boldsymbol{P}(\boldsymbol{x}) = \boldsymbol{y}$, is computed by the signer.

$$P := T \circ P' \circ S \in F_q[x]^m \quad \text{Public Key}$$

$$x \in F_q^n \xrightarrow{\mathbf{S} \in F_q[x]^n} \mathbf{v} \in F_q^n \xrightarrow{\mathbf{P}' \in F_q[v]^m} \mathbf{w} \in F_q^m \xrightarrow{\mathbf{T} \in F_q[w]^m} \mathbf{y} \in F_q^m$$

$$x \in \mathbf{F}_q^n \xrightarrow{\mathbf{S} \in F_q[x]^n} \mathbf{v} \in F_q^n$$

$$x \in \mathbf{F}_q^n \xrightarrow{\mathbf{S} \in F_q[x]^n} \mathbf{v} \in F_q^n$$

Fig. 1. Multivariate Public Key Cryptosystem

1.3 MPKC Trapdoors

According to the classification of Wolf [24], the basic trapdoors of MPKC are:

- 1. Unbalanced Oil and Vinegar (UOV)
- 2. Stepwise Triangular System (STS)
- 3. Matsumoto-Imai (MI)
- 4. Hidden Field Equation (HFE)

Among the above four trapdoors, STS and Matsumoto-Imai are bijections. The property of bijectiveness has been made full use of by various scientists including Tsujii et al [22]. Here Matsumoto-Imai and STS are explained as examples.

Matsumoto-Imai One of the most well-known MPKC trapdoors would be the Matsumoto-Imai (MI) Cryptosystem [12]. This scheme is regarded as a very basic among MPKCs and several variants have been proposed. Its construction is explained concisely in the textbook of Ding et al. [6]:

Let \mathbf{F}_q be a finite field of characteristic q, and take $i(x) \in \mathbf{F}_q[x]$ to be any irreducible polynomial of degree n. Then \mathbf{F}_{q^n} is a quotient field defined as $\mathbf{F}_q[x]/i(x)$, a degree n extension of \mathbf{F}_q . Let $\phi : \mathbf{F}_{q^n} \to \mathbf{F}_q^n$ be the standard \mathbf{F}_q -linear isomorphism between \mathbf{F}_{q^n} and \mathbf{F}_q^n given by

$$\phi(a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) := (a_0, a_1, \ldots, a_{n-1}).$$

Choose θ so that $0 < \theta < n$ and

$$\gcd(q^{\theta}+1, q^n-1) = 1.$$

Map G over \mathbf{F}_{q^n} is as follows:

$$G(X) = X^{1+q^{\theta}}.$$

Now if η is an integer such that

$$\eta(1+q^{\theta}) \equiv 1 \mod (q^n-1)$$

then $G^{-1}(X) = X^{\eta}$. Now let **P'** be the map over \mathbf{F}_q^{n} defined by

$$\mathbf{P'} = \phi \circ G \circ \phi^{-1}(x_1, \dots, x_n) = (g_1, \dots, g_n).$$

Afterwards its structure is disguised by affine transformations:

$$\boldsymbol{P} = \boldsymbol{T} \circ \boldsymbol{P'} \circ \boldsymbol{S}(x_1, \dots, x_n) = (e_1, \dots, e_n).$$

Matsumoto-Imai Cryptosystem was successfully cryptanalyzed by Patarin [14] in 1995. After Patarin published the cryptanalysis, their group proposed another trapdoor expanding the concept of MI. This is the Hidden Field Equation cryptosystem [15]

Stepwise Triangular System (STS) Another example is Stepwise Triangular System, whose basic concept was proposed by Tsujii [18][19] in 1986 and 1989 as an encryption system known as "Sequential Solution Method." Similar ideas were independently proposed by Shamir [17] in 1993 and T. T. Moh [13] in 1999 as signature systems.

The central map of the sequential solution method is shown in the formula (1).

$$w_{1} = g_{1}(v_{1}, v_{2}, \dots, v_{k-1}, v_{k})$$

$$w_{2} = g_{2}(v_{1}, v_{2}, \dots, v_{k-1})$$

$$\vdots$$

$$w_{k-1} = g_{k-1}(v_{1}, v_{2})$$

$$w_{k} = g_{k}(v_{1})$$
(1)

As shown above, the ciphertext $\mathbf{y} := (y_1, \ldots, y_k)$ is decrypted by solving the equation from the bottom. Since the polynomial $g_k(v_1) = y_k$ is univariate, it is easily solved and afterwards the root is assigned to the variable v_1 of the equation $g_{k-1}(v_1, v_2) = y_{k-1}$. In this way whole system of equations is solved by solving univariate equations one after another.

Kasahara et al. [11] proposed an encryption system based on this idea. His idea, Stepwise Triangular System (STS), uses the "step," subsequences of the

central map with r elements. r is a small number such as 4 or 5. Its structure is shown in the equation (2).

Step 1
$$\begin{cases} p_{1}(v_{1},...,v_{r},...,v_{ir},...,v_{(L-1)r},...,v_{Lr}) \\ \vdots & \vdots \\ p_{r}(v_{1},...,v_{r},...,v_{ir},...,v_{(L-1)r},...,v_{Lr}) \end{cases}$$
Step 2
$$\begin{cases} p_{r+1}(v_{1},...,v_{r},...,v_{ir},...,v_{(L-1)r}) \\ \vdots & \vdots \\ p_{2r}(v_{1},...,v_{r},...,v_{ir},...,v_{(L-1)r}) \end{cases}$$
(2)
Step i
$$\begin{cases} p_{(i-1)r+1}(v_{1},...,v_{r},...,v_{ir}) \\ \vdots & \vdots \\ p_{ir}(v_{1},...,v_{r},...,v_{ir}) \\ \vdots & \vdots \\ p_{ir}(v_{1},...,v_{r},...,v_{ir}) \\ \vdots & \vdots \\ p_{Lr}(v_{1},...,v_{r}) \end{cases}$$

The Step L, is an r-variate determined equation system. It is possible to decrypt the whole ciphertext by solving small equation systems, in the similar way as solving the univariate equation in the sequential solution method. Kasahara et al. proposed their cryptosystem, which they named RSSE(2)PKC. Afterwards they proposed its bijection version by the name of RSE(2)PKC.

1.4 Modifiers

Wolf et al. [24] proposed to classify the modifiers into 8 categories. One example of modifiers is the 'Internal Perturbation,' proposed by Ding, et al. [4]. Now the 'Internal Perturbation' is explained as an example of Modifiers.

Let z_1, \ldots, z_r be random linear polynomials of \boldsymbol{x} and $\boldsymbol{F}(\boldsymbol{x}) \in \boldsymbol{F}_q[\boldsymbol{x}]^m$ is a conventional MPKC public key such as MI or HFE. Now random r-variate polynomials q_1, \ldots, q_m are created and new public key $\boldsymbol{H}(\boldsymbol{x}) := \boldsymbol{F}(\boldsymbol{x}) + (q_1(z_1, \ldots, z_r), \ldots, q_m(z_1, \ldots, z_r))^T$ is generated. The resulting

polynomial vector $H(\mathbf{x})$ is "perturbed" from the original public key and complexity of Gröbner bases attack is higher than the original cryptosystem. According to Ding et al. [3], the relationship between time complexity of Gröbner bases attack and m is exponential if the trapdoor of $F(\mathbf{x})$ is Matsumoto-Imai and $r \geq 6$. Ding et al. have proposed new cryptosystems by modifying Matsumoto-Imai and HFE [4][7] with internal perturbation.

2 Background -Enhanced STS

Tsujii et al. proposed to apply the STS trapdoor, originally designed as an encryption system, to signature. It was expected that the vulnerability of the 'Triangular' structure could be corrected by combining it with another symmetric triangular structure into 'rectangular.'

2.1 Complementary STS Structure

Wolf et al. [23] pointed out that it is possible to cryptanalyze the STS cryptosystems such as RSE(2) and RSSE(2), by exploiting the descending 'Chain of Kernels.'

Tsujii et al. proposed to combine two independent STS central maps [21].

While one STS system increases the variables by r from the initial r as the step proceeds, the other decreases the variables by r from the initial (m-r). If a new central map is created by linearly combining the elements with the elements of the corresponding step, the rank (=number of variables) of all elements in the central map becomes the same. Resulting cryptosystem should be secure both against Gröbner Bases and Rank Attack. The concept of the structure is illustrated in Figure 2.



Fig. 2. Complementary STS Structure

The central map of Complementary STS is shown in the formula (3). The whole system has m polynomials with (2m - r) variables. Every polynomial in

the system has the rank m.

Step 1
$$\begin{cases} p_{1}(u_{1},...,u_{r}, v_{1},...,v_{m-r}) \\ \vdots \\ p_{r}(u_{1},...,u_{r}, v_{1},...,v_{m-r}) \\ \vdots \\ p_{(i-1)r+1}(u_{1},...,u_{ir}, v_{(i-1)r+1},...,v_{m-r}) \\ \vdots \\ p_{(i-1)r+r}(u_{1},...,u_{ir}, v_{(i-1)r+1},...,v_{m-r}) \\ \vdots \\ p_{(L-2)r+1}(u_{1},...,u_{m-r},v_{m-2r+1},...,v_{m-r}) \\ \vdots \\ p_{(L-2)r+r}(u_{1},...,u_{m}) \\ Step L \begin{cases} p_{(L-1)r+1}(u_{1},...,u_{m}) \\ \vdots \\ p_{(L-1)r+r}(u_{1},...,u_{m}) \\ \vdots \\ p_{(L-1)r+r}(u_{1},...,u_{m}) \end{cases} \end{cases}$$
(3)

All elements of $\boldsymbol{u} := (u_1, \ldots, u_m) \in \boldsymbol{F}_q[x_1, \ldots, x_{2m-r}]^m$ and $\boldsymbol{v} := (v_1, \ldots, v_{m-r}) \in \boldsymbol{F}_q[x_1, \ldots, x_{2m-r}]^{m-r}$ are intermediate variables generated by the affine transformation $\boldsymbol{S} : (\boldsymbol{u}, \boldsymbol{v})^T = \boldsymbol{S}(\boldsymbol{x})$. When arbitrary values are assigned to v_1, \ldots, v_{m-r} , the structure of the formula (3) becomes STS central map.

2.2 Check Equation -Enhanced STS

After proposing the Complementary STS, Tsujii et al. found that the 'Chain of Kernels' was not completely eliminated in the Complementary STS either, and that High Rank Attack on the structure is still possible [20]. Therefore they have improved the signature system and proposed the new system as "Enhanced STS [20][22]." This system uses the "Verifier" equation system in parallel with the public key. The procedure of signing and validating is illustrated in the Figure 3.

P'(u, v) is the Complementary STS public key, system of polynomials with n(=2m-r)-variate m polynomials. Let $H' \in F_q[u, v]$ be the polynomial system designed to satisfy $\forall u \in F_q^m$, $H'(u, \alpha) = 0$. The polynomial system $H(x) := H' \circ S$ is the "Check Equation," which satisfies H(x) = 0 $\forall x$ such that $S(x) = (u, \alpha)$.

The procedure of signing a message m is as follows:

1. Affine transformation T is inverted to the m.

$$m' = T^{-1}(m)$$

2. The value $(\alpha_1, \ldots, \alpha_{m-r})$ are assigned to (v_1, \ldots, v_{m-r})



Fig. 3. Improving the Security by Check Equation

- 3. The resulting $P'(u_1, \ldots, u_m, \alpha_1, \ldots, \alpha_{m-r})$ is *m*-variate STS public key, which is bijection.
- 4. The equation system $P'(u_1, \ldots, u_m, \alpha_1, \ldots, \alpha_{m-r}) = m$ is solved.
- 5. The signature is obtained by inverting the affine transformation S to the root $(s'_1, \ldots, s'_m, \alpha_1, \ldots, \alpha_{m-r})$.

$$\boldsymbol{s} := (s_1, \ldots, s_n) = \boldsymbol{S}^{-1}(s'_1, \ldots, s'_m, \alpha_1, \ldots, \alpha_{m-r})$$

The procedure of validation is done this way:

- 1. It is checked whether $P(s_1, \ldots, s_n)$ is m.
- 2. It is checked whether $H(s_1, \ldots, s_n)$ is **0**.

Even if the Complementary STS public key P(x) is successfully cryptanalyzed by any chance, it is impossible to find the signature which also satisfies the equation $H(s_1, \ldots, s_n) = 0$.

It should be noted that the $P(v_1, \ldots, v_m, \alpha_1, \ldots, \alpha_{m-r})$ is a bijection and therefore it is possible to sign any message even if a pre-determined value (condition to satisfy H(x) = 0) $(\alpha_1, \ldots, \alpha_{m-r})$ is assigned to v_2 . Otherwise it frequently occurs that signature of m does not exist.

2.3 Vulnerability of Check Equation methodology

Although it might be difficult to solve the equation H(x), it should be noted that all valid signatures corresponding to the check equation H(x) satisfy H(x) =**0**, regardless of the message, i.e. every valid signature lies in a certain *m*dimensional space, although the signature is *n*-dimensional. Therefore, if *m* valid signatures are collected, the linear space where every signature lies is found. The attack is done as follows:

- 8 Gotaishi, and Tsujii
- 1. Signatures $\sigma_1, \ldots, \sigma_{m+1}$ are collected.
- 2. Differentials $\Delta \sigma_1 = \sigma_1 \sigma_{m+1}$, $\Delta \sigma_2 = \sigma_2 \sigma_{m+1}$, ..., $\Delta \sigma_m = \sigma_m \sigma_{m+1}$ are computed.
- 3. An *m*-variate linear polynomial vector $\boldsymbol{L}(\boldsymbol{u}) = u_1 \Delta \boldsymbol{\sigma}_1 + \ldots + u_{m-1} \Delta \boldsymbol{\sigma}_{m-1} + u_m \Delta \boldsymbol{\sigma}_m + \boldsymbol{\sigma}_{m+1} \in \boldsymbol{F}_q[u_1, \ldots, u_m]^n$ is created.
- 4. The *n* elements of L(u) are assigned to each element of P(x).
- 5. The resulting system of *m*-variate polynomials P'(u) := P(L(u)) has the STS structure.

Then it is possible to sign any message y by solving the equation P'(u) = y. Afterwards the solution is assigned to the *n*-dimensional linear polynomial vector L(u). This signature also satisfies the check equation H(x) = 0.

Because of this vulnerability, Tsujii et al. proposed [22] to change the check equation every time a message is signed.

3 "Hidden Pair of Bijection" Signature

Based on the idea of "Complementary Bijections" and "Check Equations," a new idea of MPKC signature is created.

3.1 Basic Trapdoor

Let F_1 , F_2 : $F_q^m \to F_q^m$ be a pair of bijections. Now it is assumed that $F_1(\mathbf{0}) = F_2(\mathbf{0}) = \mathbf{0}$. A polynomial vector $H(v) := (h_1(v), \ldots, h_m(v)) \in F_q[v]^m$ is defined as follows:

$$h_i(\boldsymbol{v}) = \sum_{j=1}^{m} \sum_{k=1}^{m} a_{ijk} v_j v_{m+k} \qquad (1 \le i \le m)$$
(4)

Coefficients $a_{ij} \in \mathbf{F}_q$ are random values. When either the vector $\mathbf{v}_1 := (v_1, \ldots, v_m)$ or $\mathbf{v}_2 := (v_{m+1}, \ldots, v_n)$ is $\mathbf{0}, \mathbf{H}(\mathbf{v})$ is $\mathbf{0}$, regardless of the rest of the elements of vector \mathbf{v} . Now the following mapping $\mathbf{P'}(\mathbf{v}) : \mathbf{F}_q^{2m} \to \mathbf{F}_q^m$ is created:

$$P'(v) := F_1(v_1) + F_2(v_2) + H(v)$$

$$(v_1 := (v_1, \dots, v_m), v_2 := (v_{m+1}, \dots, v_{2m}))$$
(5)

If **0** is assigned to v_2 , both $F_2(v_2)$ and H(v) are zero vector, leaving only $F_1(v_1)$, the bijection over F_q^m . Therefore for any message $y \in F_q^m$, one of its pre-images is easily obtained as $(F_1^{-1}(y), \mathbf{0})$. Another pre-image is also obtained by computing $(\mathbf{0}, F_2^{-1}(y))$.

There are two ways to sign a given message, but it is impossible to know whether **0** was assigned to v_1 or v_2 , without the knowledge of the hidden structure. This pair of bijections, F_1 and F_2 , is the central map.

Public Key 3.2

The HPB public key G(x) is created as follows:

$$P(x) = T_1(F_1(S_1(x))) + T_2(F_2(S_2(x))) + H(S(x))$$
(6)

In the formula (6), $T_1, T_2: F_q^m \to F_q^m$ are affine transformations. S_1 and S_2 are the higher and lower half of an affine transformation $\boldsymbol{S}: \boldsymbol{F}_q^{2m} \to \boldsymbol{F}_q^{2m}$ i.e. $\boldsymbol{S}_1(\boldsymbol{x}) = (v_1, \dots, v_m)^T, \ \boldsymbol{S}_2(\boldsymbol{x}) := (v_{m+1}, \dots, v_{2m})^T.$

- 1. Public Key:
- *m*-dimensional polynomial vector $\boldsymbol{P}(\boldsymbol{x})$
- 2. Private Key

Affine transformations T_1, T_2, S , and the pair of bijections $F_1(x_1), F_2(x_2)$

A message $\boldsymbol{y} \in \boldsymbol{F}_q^m$ is signed along the following procedure. This is the case in which F_2 is set zero:

- 1. T_1 is inverted to the message y: $y' = T_1^{-1}(y)$ 2. Bijection F_1 is inverted: $s' := F_1^{-1}(y')$
- 3. Signature s is computed by inverting the affine transformation S.

$$s = S^{-1}(s', 0)$$

It is also possible to sign by setting F_1 to **0**, instead of F_2 .

 \boldsymbol{F}_1 and \boldsymbol{F}_2 are not limited to STS. Any central map of bijection can be used. Moreover, the trapdoors of the both need not be identical. Combinations such as 'STS and MI' are possible.

3.3 **Rainbow-like Implementation**

The public key of HPB has twice as long signatures as the message. Although it is shorter than that of Unbalanced Oil & Vinegar, it is not short enough for practical use. In order to shorten the signature length compared with the message, it is possible to appned extra variables and polynomials by the implementation similar to Rainbow [8].

Let $P(v_1, \ldots, v_{2m})$ be the 2*m*-variate HPB public key. New variables v_{2m+1},\ldots,v_{2m+k} $(k \ge m)$ are appended and linear polynomial vector $\boldsymbol{\lambda}(\boldsymbol{v}) :=$ $(\ell_1,\ldots,\ell_k)^T \in \boldsymbol{F}_q[v_1,\ldots,v_{2m+k}]^k$ is created as follows:

$$\boldsymbol{\lambda} := A \times (v_{2m+1}, \dots, v_{2m+k})^T + B \times (v_1, \dots, v_{2m})^T$$
(7)

In the formula (7), A is a $k \times k$ invertible matrix and B is a $k \times 2m$ full-rank matrix. Then a polynomial vector Q(v) is created, using a k-variate quadratic bijection $\boldsymbol{\Gamma}(\boldsymbol{v}) \in \boldsymbol{F}_q[v_1, \dots, v_k]$ and random 2*m*-variate quadratic polynomial vector $R(v_1, ..., v_{2m})$.

$$\boldsymbol{Q}(\boldsymbol{v}) := \boldsymbol{\Gamma}(\boldsymbol{\lambda}) + \boldsymbol{R}(v_1, \dots, v_{2m}) \tag{8}$$

When constants are assigned to the variables v_1, \ldots, v_{2m} , polynomial vector Q(v) becomes a bijection from F_q^k to F_q^k . So a new (2m + k)-variate central map is created:

$$\begin{pmatrix} \boldsymbol{Q}(v_1,\ldots,v_{2m+k})\\ \boldsymbol{P}(v_1,\ldots,v_{2m}) \end{pmatrix}$$
(9)

When either v_1, \ldots, v_m or v_{m+1}, \ldots, v_{2m} are set all zero, the (m+k) dimensional polynomial vector (9) is a bijection of the remaining variables. Now the number of variables is (2m+k) and the number of polynomials (m+k).

4 Discussion of Security

4.1 Security against Gröbner Bases Attack

 F_1 and H are working as the perturbation polynomials of the central map F_2 and vice versa. Therefore the HPB public key is expected to be difficult to attack by computing the Gröbner bases. The assumption was confirmed by experiments.

When an *underdetermined* system of equations is solved by computing Gröbner Bases, the extra variables are fixed in order to make the system *determined*. When Braeken et al.[2] tested the security of Unbalanced Oil & Vinegar, they fixed v variables by appending random v linear polynomials to the system. We employed their procedure.

Experiments HPB signature keys using STS (r = 1: sequential solution method) and Matsumoto-Imai as the bijection are created with varying length and algebraic attack using Gröbner Bases is done.

- 1. HPB systems P(x) with varying document length (with the signature length double the document length) from about 18 to 24 are generated. Parameter r of the STS is 1 (sequential solution method).
- 2. Document y are generated by random numbers.
- 3. The signature s for each document is generated
- 4. *m* Linear polynomials $\ell_1(\boldsymbol{x}), \ldots, \ell_m(\boldsymbol{x})$ are randomly generated.
- 5. The system of linear equations $\ell_1(\mathbf{x}) \ell_1(\mathbf{s}), \ldots, \ell_m(\mathbf{x}) \ell_m(\mathbf{s})$ is appended to the system of polynomials $\mathbf{P}(\mathbf{x}) \mathbf{y}$
- 6. Time to compute Gröbner bases of the ideal generated by the *determined* polynomial system created in the step 5 is measured.
- 7. The computation time is compared with a randomly generated 2m-variate equation systems with m polynomials. It is also made *determined* by appending m linear polynomials as done in the step 5

The reason for creating the linear equations as done in step 5 is to assure the root of the equation to exist.

The computer system used in calculating the Gröbner bases is as follows: Computer: Proside edAEW416R2 workstation with AMD Opteron Model 854 processors at 2.80GHz and 64GB of RAM is used for the HPB using two STSs. Japan Computing System (JCS) VC98220WSA-4U/T workstation, with CPU AMD Opteron 8220 (2.80 GHz) quadcore and 128 Gbyte Memory for the HPB using two MIs

Software: Magma ver. 2.15-15 [1] running on Red Hat Enterprise Linux Advanced Platform Standard for both computers.

Built-in function GroebnerBases () of Magma is used to compute the Gröbner bases by F_4 algorithm.

Table 1. Comparison of Gröbner base computing time, HPB(using Sequential Solution method) and Random polynomial system

	F4 Computing time(s)			
	in Second			
Message	HPB Public Key	Random	Difference	
Length	using Seq. Sol.	Polynomials		
18	2.26	2.33	-0.07	
19	4.33	4.35	-0.02	
20	8.69	8.74	-0.05	
21	17.34	17.43	-0.09	
22	56.00	55.87	0.13	
23	88.60	88.45	0.15	
24	604.21	604.70	-0.49	

Table 2. Comparison of Gröbner base computing time, HPB(using Matsumoto-Imai)

 and Random polynomial system

	F4 Computing time(s)			
	in Second			
Message	HPB Public Key	Random	Difference	
Length	using MI	Polynomials		
18	2.56	2.54	0.02	
20	10.09	10.14	-0.05	
22	64.78	64.95	-0.17	
24	777.63	754.26	23.37	
25	1601.42	1614.29	-12.87	

Table 1 is the result of the Gröbner bases attack to the HPB using a pair of STSs. Table 2 is for the ones using MIs. As shown in the both tables, the security of HPB against Gröbner bases is as high as the random quadratic polynomials.

4.2 Attack by collecting valid Signatures

As discussed in the section 2.3, if fixed constants are always assigned to fixed m variables out of 2m, it is possible to find to which variables (linear polynomials) the constants are assigned, by collecting (m + 1) signatures. Afterwards the attackers would find the structure of the central map. HPB is designed to innoculate the system against this attack. Since there are two ways to choose variables between (x_1, \ldots, x_m) and $(x_{m+1}, \ldots, x_{2m})$, the probability that randomly collected m signatures are all signed by setting the same variables to zero declines exponentially as m grows. However, it might occur that 90 out of 100 signatures are signed by setting the first half to zero and remaining 10 are not. In that case, 90 variables lie in the linear space spanned by x_{m+1}, \ldots, x_n and 10 variables are linear combinations of x_1, \ldots, x_m . The structure is similar to the trapdoors modified by internal perturbation with the r = 10. Now the security discussion for this attack assumes two MIs as the bijection pair, since its Differential Attack, which eliminates the effect of perturbation is extensively studied.

As Ding et al. discussed [8][6][3], the complexity of computing Gröbner bases is exponential function of the message length m as long as $r \ge 6$. Its probability is almost 100 % as long as m is sufficiently large. Consequently the resulting polynomial system is expected still secure against Gröbner bases attack. Another risk is the differential attack.

Fouque [9] pointed out that it is possible to look for the vector \boldsymbol{x} where the corresponding perturbation polynomials are all zero. If it is found, attackers can eliminate the effect of the perturbation.

The complexity of this attack is estimated to be $\mathcal{O}(m^3 q^r q^{\gcd(\theta,m)})$ [5], exponential function of r.

Here it is assumed that $2N(N \gg m)$ valid signatures are collected. Among them, N signatures, or half of all, are signed by assigning 0 to x_1, \ldots, x_m and the rest is otherwise. When m are selected out of 2N signatures, the probability that at least (m - k) of them are signed in the same way, is:

$$\frac{{}_{N}C_{m-k}}{{}_{2N}C_{m-k}} = \frac{N(N-1)\dots(N-m+k+1)}{2N(2N-1)\dots(2N-m+k+1)}$$
$$= \frac{1}{2^{m-k}} \times \frac{(N-1)(N-2)\dots(N-m+k+1)}{(N-\frac{1}{2})(N-1)\dots(N-\frac{m-k-1}{2})} < \frac{1}{2^{m-k}} \quad (10)$$

The following attack is considered:

- 1. Thereshold k is determined.
- 2. m signatures are randomly selected from N.
- 3. As described in the section 2.3, 2*m*-variate polynomials are transformed to *m*-variate.
- 4. Resulting *determined* polynomial system is attacked by differential attack.
- 5. If the attack takes more than $\mathcal{O}(m^3 q^k q^{\gcd(\theta,m)})$, the selection is regarded as "failure" and go back to the 2.

For the above attack to succeed, $\mathcal{O}(m^3 2^k 2^{\gcd(\theta,m)}) \times 2^{m-k} = \mathcal{O}(m^3 2^{gcd(\theta,m)} \times 2^m)$ operations are required.

Since the complexity of the attack increases exponetially as m grows, the HPB using the pair of MI is secure against this attack.

It is expected that almost the same security is established when STS is used.

5 Discussion

5.1 Advantage of HPB

HPB is a new scheme of MPKC signature. It has several advantages over existing signatures:

- HPB signature is twice as long as the document to be signed, shorter than the UOV.
- Unlike other signatures based on non-bijections such as QUARTZ [16] (using HFE), HPB always has pre-image and successfully signs the message in one attempt.

The first feature would not be so important, since it is possible to reduce the rate of signature to message using the rainbow-like structure. Important advantage would be the later. Since other major MPKC signatures such as QUARTZ or Rainbow are not assured to successfully sign the message in one attempt. This repetition would make significant difference of the efficiency.

5.2 Future Study

Since HPB uses a combination of existing trapdoors, further attacks should be investigated. Although, since each part of the pair perturbs another, it would be quite difficult to analyze it, such as by differential attack.

The pair of bijections need not have the same trapdoors. For example, MI and STS can form a pair. The configuration of the pairs and parameters would have to be discussed to determine the optimum condition.

Acknowledgment

Our work is supported by the Ministry of Economy, Technology, and Industry (METI) of the Japanese government.

References

- Wieb Bosma, John Cannon, and Catherine Playoust, The Magma Algebra System I: The User Language, Journal of Symbolic Computation 24 (1997), no. 3-4, 235– 265.
- An Braeken, Christopher Wolf, and Bart Preneel, A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes, Topics in Cryptology - CT-RSA 2005 (Alfred Menezes, ed.), Lecture Notes in Computer Science, vol. 3376, Springer Berlin / Heidelberg, pp. 29–43.
- J. Ding, J. Gower, D. Schmidt, C. Wolf, and Z. Yin, Complexity Estimates for the F4 Attack on the Perturbed Matsumoto-Imai Cryptosystem, Cryptography and Coding (Nigel Smart, ed.), Lecture Notes in Computer Science, vol. 3796, Springer Berlin / Heidelberg, 2005, pp. 262–277.
- Jintai Ding, A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation, Public Key Cryptography PKC 2004 (Feng Bao, Robert Deng, and Jianying Zhou, eds.), Lecture Notes in Computer Science, vol. 2947, Springer Berlin / Heidelberg, 2004, pp. 305–318.
- Jintai Ding and Jason E. Gower, *Inoculating Multivariate Schemes Against Differ*ential Attacks, Public Key Cryptography - PKC 2006 (Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, eds.), Lecture Notes in Computer Science, vol. 3958, Springer Berlin / Heidelberg, 2006, pp. 290–301.
- Jintai Ding, Jason E. Gower, and Dieter Schmidt, Multivariate Public Key Cryptosystems (Advances in Information Security), Springer-Verlag New York, Inc., 2006.
- Jintai Ding and Dieter Schmidt, Cryptanalysis of HFEv and Internal Perturbation of HFE, Public Key Cryptography, 2005, pp. 288–301.
- Jintai Ding and Dieter Schmidt, Rainbow, a New Multivariable Polynomial Signature Scheme, Applied Cryptography and Network Security (John Ioannidis, Angelos Keromytis, and Moti Yung, eds.), Lecture Notes in Computer Science, vol. 3531, Springer Berlin / Heidelberg, 2005, pp. 164–175.
- Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern, Differential Cryptanalysis for Multivariate Schemes, Advances in Cryptology - EUROCRYPT 2005 (Ronald Cramer, ed.), Lecture Notes in Computer Science, vol. 3494, Springer Berlin / Heidelberg, 2005, pp. 341–353.
- Michael R. Garey and David S. Johnson, Computers and Intractability; A Guide to the Theory of NP-Completeness, W. H. Freeman & Co., New York, NY, USA, 1990.
- Masao Kasahara and Ryuichi Sakai, A construction of public-key cryptosystem based on singular simultaneous equations, IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences E88-A (2005), no. 1, 74–80.
- T. Matsumoto and H. Imai, Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88 (New York, NY, USA), Springer-Verlag New York, Inc., 1988, pp. 419–453.
- 13. T. T. Moh, A public key system with signature and master key functions, Communications in Algebra 27 (1999), no. 5, 2027–2222.
- Jacques Patarin, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88, Advances in Cryptology - CRYPTO '95 (Don Coppersmith, ed.), Lecture Notes in Computer Science, vol. 963, Springer Berlin / Heidelberg, 1995, pp. 248–261.

- _____, Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, Advances in Cryptology - EURO-CRYPT '96 (Ueli Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer Berlin / Heidelberg, 1996, pp. 33–48.
- Jacques Patarin, Nicolas Courtois, and Louis Goubin, QUARTZ, 128-Bit Long Digital Signatures, Topics in Cryptology CT-RSA 2001 (David Naccache, ed.), Lecture Notes in Computer Science, vol. 2020, Springer Berlin / Heidelberg, 2001, pp. 282–297.
- Adi Shamir, Efficient Signature Schemes Based on Birational Permutations, CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology (London, UK), Springer-Verlag, 1994, pp. 1–12.
- S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, and T. Matsumoto, A public-key cryptosystem based on the difficulty of solving a system of non-linear equations, The Transactions of the Institute of Electronics and Communication Engineers of Japan 69 (1986-12), no. 12, 1963–1970.
- Shigeo Tsujii, Atsushi Fujioka, and Yuusuke Hirayama, Generalization of the public-key cryptosystem based on the difficulty of solving a system of non-linear equations, The Transactions of the Institute of Electronics, Information and Communication Engineers. A 72 (1989-02), no. 2, p390–397.
- Shigeo Tsujii and Masahito Gotaishi, Enhanced STS using Check Equation Extended Version of the Signature scheme proposed in the PQCrypt2010-, Cryptology ePrint Archive, Report 2010/480, 2010, http://eprint.iacr.org/.
- Shigeo Tsujii, Masahito Gotaishi, Kohtaro Tadaki, and Ryo Fujita, Proposal of Multivariate Public Key Signature Scheme Applying the STS Cryptosystem: Part II — Enhanced STS Signature—, The 2010 Symposium on Cryptography and Information Security 3A2-2, 2010.
- Proposal of a Signature Scheme Based on STS Trapdoor, Post-Quantum Cryptography (Nicolas Sendrier, ed.), Lecture Notes in Computer Science, vol. 6061, Springer Berlin / Heidelberg, 2010, pp. 201–217.
- Christopher Wolf, An Braeken, and Bart Preneel, Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC, Cryptology ePrint Archive, Report 2004/237, 2004, http://eprint.iacr.org/.
- 24. Christopher Wolf and Bart Preneel, *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*, Cryptology ePrint Archive, Report 2005/077, 2005, http://eprint.iacr.org/.