Enhanced STS using Check Equation –Extended Version of the Signature scheme proposed in the PQCrypt2010–

Shigeo Tsujii† Masahito Gotaishi†

† Research and Development Initiative, Chuo University
1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan

Abstract. We propose solutions to the problems which has been left in the Enhanced STS, which was proposed in the PQCrypto 2010.
Enhanced STS signature scheme is defined as the public key with the Complementary STS structure, in which two STS public keys are symmetrically joined together. Or, the complementary STS is the public key where simply two STS public keys are joined together, without the protection with Check Equation.
We discuss the following issues left in the Enhanced STS, which was prosented in the PQCrypt2010:

(i) We implied that there may exist a way to cryptanalyze the Complementary STS structure. Although it has been proposed that the system be protected by Check Equations [35][37], in order to cope with an unknown attack, we did not show the concrete procedure. We show the actual procedure to cryptanalyze it and forge a signature.

(ii) We assumed that the Check Equation should be changed every time a document is signed. This practice is not always allowed. We improved this matter. The Check Equation which was proposed in the PQCrypto 2010 defined the valid life as a function of the number of times the documents are signed, because the secret key of Check Equation is analyzed by collecting valid signatures.

Now we propose a new method of integrating the Check Equation into the secret key and eliminate the risk of the hidden information drawn from the existing signature.

Key words: Multivariate Public Key Cryptosystem, Digital Signature, Stepwise Triangular Scheme, Check Equation

1 Introduction

1.1 MPKC Trapdoors

Multivariate Public Key Cryptosystem (MPKC) has long history of study and they are still actively studied worldwide. Although there are numerous kinds of trapdoors, most of the encryption scheme are based on either of the 2 basic trapdoors:

(i) MI-HFE Trapdoor (Matsumoto, Imai, Patarin)
The development of the first MPKC in the world had been launched around 1983 by Matsumoto and Imai [1]. The new cryptosystem, which is widely known as "Matsumoto-Imai cryptosystem" (MI), was proposed in EUROCRYPT in 1988 [2]. After Patarin [3] successfully cryptanalyzed MI, he extended the idea of MI further and proposed Hidden Field Equation (HFE) cryptosystem in 1996 [4].

(ii) STS Trapdoor (Tsujii, et al. Shamir, Kasahara, et al.)
STS trapdoor was proposed by Tsujii in 1985 [5]. Its initial scheme, which was named "Sequential Solution Method" [6], was cryptanalyzed by Hasegawa and Kaneko in 1987 [7]. Tsujii et al. proposed the improved version in 1989 [8]. 1989 version of Tsujii's cryptosystem, which was translated to English by Tadaki, et al. and published on the Cryptology ePrint Archive [9] in 2004, was cryptanalyzed by Ding et al. in PQCrypto 2008 [10].
Afterwards Kasahara et al. actively published various schemes including RSE, generalizing the concept of Sequential Solution Method [11][12]. Moh et al. proposed their scheme utilizing the Sequential Solution Method [13][14][15]. When Wolf, et al. attacked Kasahara's scheme with Rank Attack, they specified the family of the cryptosystems which Kasahara's group proposed as "Stepwise Triangular System" (STS) [16]. Here the family of MPKCs based on the trapdoor of Sequential Solution Method is called "STS scheme" in this paper.

1.2 MPKC signatures

Besides the 2 trapdoors for encryption, Unbalanced Oil and Vinegar (UOV) is another basic trapdoor proposed by Kipnis et al. [42][17]. Unlike other two, UOV is not used for encryption. Although no effective way of attacking UOV is found yet, it has 3 times more variables than polynomials. Therefore UOV scheme has not ever been implemented as it is. Ding et al. proposed its efficient implementation by the name of "Rainbow" [18]

The trapdoors for encryption have been applied to signature schemes, either by hiding polynomials ("minus" modification) or appending extra variables ("vinegar" modification)[19]. MI was modified into SFLASH [20] and HFE into QUARTZ [21]. SFLASH was cryptanalyzed [22] and QUARTZ consumes so much memory that currently it is difficult to implement.

Shamir proposed the signature scheme based on the Sequential Solution Method, with its linear polynomials hidden, in CRYPTO 1993 [23]. His signature was also cryptanalyzed by Coppersmith et al. [24], with the attack similar to the Rank Attack [16].

The current situation of MPKC encryption and signature schemes is illustrated in the Table 1.

1.3 Extra Variables of Signature trapdoor

Tsujii et al. [34][35][37] proposed a new signature scheme, which is named "Complementary STS structure." It was designed to fail the Rank Attack, which exploits the difference of rank among steps. However, it has turned out that the Complementary STS is possible to cryptanalyze by a variant of High Rank Attack. We discussed the vulnerability of the signature public keys and proposed to strengthen the signature key by eliminating the "ambiguity" of the signature.

All signature keys are "underdetermined," partly because most of MPKCs are not bijection. Some 'buffer' is necessary for signature to exist for every document. We proposed to strengthen

Table 1: Taxonomy of MPKC

Basic Scheme	Encryption	Signature
MI- HFE	MI Scheme A or C^* [2]	SFLASH [20]
	Hidden Field Equation [4]	QUARTZ [21]
	ℓ-IC [25]	ℓ-IC$^-$ [25]
	Square [26]	Square-Vinegar [27]
STS [28][16]	Sequential Solution Method [6]	Birational Permutation [23][29]
	TTM [13]	TTS [30][31]
	RSE [11], RSSE [12] PPS [32][33]	Enhanced STS [34][35][37]
	Tractable Rational Map [14], MFE [15]	TRMS [36]
UOV	None	Unbalanced Oil and Vinegar [17] Rainbow [18]

the public key by appending "Check equations" [37]. Now we discussed the improvement of Check Equation further to make the actual implementation possible.

1.4 New Idea described in this paper

The result of our study presented in the PQCrypt2010 following points untouched. Now we discuss them in this paper :

(i) We implied that there may exist a way to cryptanalyze the Complementary STS structure. Although it has been proposed that the system be protected by Check Equations [35][37], in order to cope with an unknown attack, we did not show the concrete procedure. We show the actual procedure to cryptanalyze it and forge a signature.

(ii) We assumed that the Check Equation should be changed every time a document is signed. This practice is not always allowed. The Check Equation which was proposed in the PQCrypto 2010 defined its valid life as a function of the number of times the documents are signed, because the secret key of Check Equation could be analyzed by collecting valid signatures.

This paper is organized as follows. In Section 2, we describe relevant background on STS and Complementary STS. In Section 3, we explain that cryptanalysis of Complementary STS structure is still possible by a variant of High Rank Attack. In Section 4, we describe the concept of Check equation proposed in [37] and propose the further improvement.

2 Preliminaries

2.1 General Design of MPKC

General structure of MPKCs is shown in Figure 1.
The internal operation such as the central map and the affine transformation is hidden and users

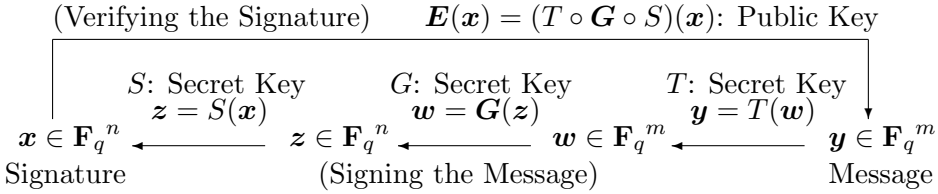

Figure 1: Multivariate Public Key Cryptosystem

encrypt the message just by assigning plaintext values to the variables of the polynomials. The message is signed by obtaining the preimage of the document by the mapping $\boldsymbol{E}(\boldsymbol{x})$ in signature schemes.

2.2 Summary of STS Scheme and its Security

Central map of the Sequential Solution Method [6] is shown in the formula (1). The first polynomial is univariate. The number of variables increases in the later sequence number. The equation system is solved by solving the sequence of univariate equations one by one from the top.

$$\begin{aligned} w_1 &= g_1(v_1) \\ w_2 &= g_2(v_1, v_2) \\ &\vdots \\ w_{k-1} &= g_{k-1}(v_1, v_2, \ldots, v_{k-1}) \\ w_k &= g_k(v_1, v_2, \ldots, v_{k-1}, v_k) \end{aligned} \tag{1}$$

Random Singular Simultaneous Equation (R(S)SE) cryptosystem [11][12] proposed by Kasahara et al. is a system where the equation is solved by solving each r-variate *determined* equation system, instead of the univariate equation. Kasahara et al. published various encryption system for the case of $r = 4$ and $r = 5$. In the case of $r = 4$, the legitimate receiver solves the 4-variate *determined* random equations in the first step. the second step has 4 polynomials with 8 variables. Among them, 4 variables are obtained by solving the 4-variate *determined* system of equations in the first step. In this way, the overall system is solved by solving the subsystems of equations step by step. It should be noted that both RSSE, one of the variants of STS scheme, and MI are bijections, while the majority of MPKCs are not.
The STS Scheme has 2 vulnerabilities:

(i) Vulnerability to the Gröbner Bases Attack [38][40]
It is possible to solve multivariate algebraic equation systems by computing the Gröbner bases of the ideal generated by the public key. This is the Gröbner bases attack, which successfully cryptanalyzed various MPKCs including Patarin's HFE Challenge [40]. According to the

ideal theory, the affine transformation, which seems to effectively disguise the structure of the central map, does not influence the complexity of computing Gröbner bases. The structure of the STS polynomials in the central map is vulnerable to Gröbner bases algorithm and easily computed. According to our experiments, the time complexity of computing Gröbner bases of the STS scheme is roughly the same as MI scheme.

(ii) Vulnerability to the Rank Attack [28][16][41]
Since the central map have several polynomials with small number of variables, The linear space spanned by the public key has a basis with low rank such as r or $2r$. Although structure of the central map is hidden by the affine transformation T, its equivalent inverse transformation $\tilde{T}^{-1}$ is found by probing for low-rank elements by generating random linear combinations of public key elements [28][16]. Once each step is sorted out, the equivalent copy of the central map is restored and the plain text is restored.

2.3 Complementary STS Structure

Complementary STS structure was proposed by Tsujii et al[34][35][37]. It was inteded to avoid the Rank Attack by eliminating the gap of rank among steps. Besides, it has been confirmed by experiment that the Complementary STS structure is secure against the Gröbner bases attack [37]. The concept of the structure is illustrated in Figure 2.

$\boldsymbol{u} := (u_1, \ldots, u_m)$ and $\boldsymbol{v} := (v_1, \ldots, v_{m-r})$ are sets of variables. The number of the steps L is

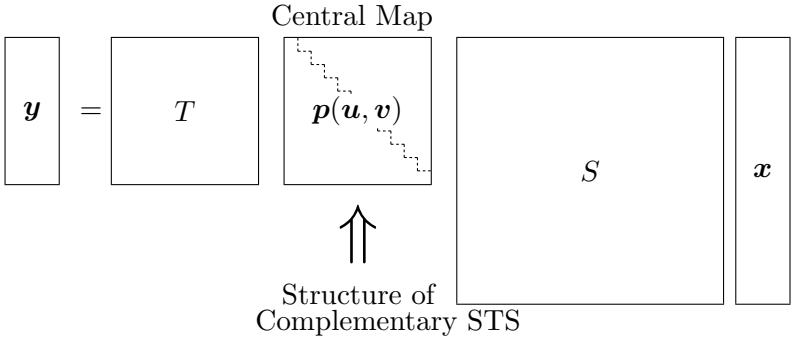

Figure 2: Structure of Complementary STS

equal to m/r, hence m must be divisible by r. The number of variables is $n := 2m - r$. Let the polynomial vector $\boldsymbol{G} = (g_1(\boldsymbol{u}, \boldsymbol{v}), \ldots, g_m(\boldsymbol{u}, \boldsymbol{v}))$ be a polynomial vector described in the formula

(2).

$$
\begin{array}{ll}
\text{Step 1} & \left\{ \begin{array}{l} g_1(u_1,\ldots,u_r,\ v_1,\ldots,v_{m-r}) \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ g_r(u_1,\ldots,u_r,\ v_1,\ldots,v_{m-r}) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } i & \left\{ \begin{array}{l} g_{(i-1)r+1}(u_1,\ldots,u_{ir},\ v_{(i-1)r+1},\ldots,v_{m-r}) \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ g_{(i-1)r+r}(u_1,\ldots,u_{ir},\ v_{(i-1)r+1},\ldots,v_{m-r}) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } L & \left\{ \begin{array}{l} g_{(L-1)r+1}(u_1,\ldots,u_m) \\ \qquad\qquad\qquad\quad \vdots \\ g_{(L-1)r+r}(u_1,\ldots,u_m) \end{array} \right.
\end{array}
\tag{2}
$$

Polynomials in the step 1 of $\boldsymbol{G}$ include r variables $u_1,\ldots,u_r \in \boldsymbol{u}$ and all variables of $\boldsymbol{v}$, with the total number of variables m. The variables of $\boldsymbol{u}$ increase by r as the step proceeds, and so many variables of $\boldsymbol{v}$ decrease, thereby keeping the total number of variables included in each polynomial at m. Hence the polynomials in the last step $L := m/r$ have all variables of $\boldsymbol{u}$ and no variable of $\boldsymbol{v}$. All polynomials of $\boldsymbol{G}$ have the rank m, but when constant value $\boldsymbol{c} := (c_1,\ldots,c_{m-r})$ are assigned to $\boldsymbol{v}$, the resulting polynomial vector $\boldsymbol{G'} = g_1(\boldsymbol{u},\boldsymbol{c}),\ldots,g_m(\boldsymbol{u},\boldsymbol{c})$ has STS structure (formula (3)).

$$
\begin{array}{ll}
\text{Step 1} & \left\{ \begin{array}{l} g'_1(u_1,\ldots,u_r) \\ \qquad\quad \vdots \\ g'_r(u_1,\ldots,u_r) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } i & \left\{ \begin{array}{l} g'_{(i-1)r+1}(u_1,\ldots,u_{ir}) \\ \qquad\quad \vdots \\ g'_{(i-1)r+r}(u_1,\ldots,u_{ir}) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } L & \left\{ \begin{array}{l} g'_{(L-1)r+1}(u_1,\ldots,\ldots,u_m) \\ \qquad\quad \vdots \\ g'_{(L-1)r+r}(u_1,\ldots,\ldots,u_m) \end{array} \right.
\end{array}
\tag{3}
$$

The public key $\boldsymbol{E}$ is created by applying affine transformation T and S to the central map $\boldsymbol{G}$.

$$\boldsymbol{E} := T \circ \boldsymbol{G} \circ S$$

The message $\boldsymbol{m} := (m_1,\ldots,m_m)$ is signed as follows:

Signing a Message

(i) Inverse affine transformation T^{-1} is applied to the message $\boldsymbol{m}$.

(ii) Random numbers are assigned to all variables of $\boldsymbol{v}$.

(iii) Since thus computed set of polynomials $p_1(u_1, \ldots, u_r), \ldots, p_m(u_1, \ldots, u_m)$ has the structure of m-variate STS, $\boldsymbol{u}$ is computed by decrypting the STS cryptosystem.

(iv) Signature $(s_1, \ldots, s_n)$ is computed by inverting the affine transformation S to the vector $\boldsymbol{u}||\boldsymbol{v}$.

Verification
Signature is verified by assigning the signature value $(s_1, \ldots, s_n)$ to the variable and checking whether the value is equal to $\boldsymbol{m}$.

3 Rank Attack to the Complementary STS structure

3.1 Rank Attack of Wolf et al.

Original idea of the Rank Attack was proposed by Goubin and Courtois [28], in order to cryptanalyze TPM, the signature scheme based on TTM. Based on that idea, Wolf et al. [16] proposed the Rank Attack designed for STS scheme. They successfully cryptanalyzed Kasahara's challenge and published the solution in the paper. They proposed two kinds of Attacks, High Rank and Low Rank.
High Rank Attack The procedure of High Rank Attack is described here. Low Rank Attack, which is described in the next paragraph, exploits the similar property of STS. Following vector spaces are considered:

$$J_l := \{\boldsymbol{b}'T^{-1} \mid \boldsymbol{b}' \in \boldsymbol{F}_q^m \ \wedge b'_{lr+l} = \ldots = b'_m = 0\} \text{ for } \ 1 \leq l \leq L$$

Obviously they form a ascending chain, i.e. $J_1 \subset J_2 \ldots \subset J_L$. Because the dimension of J_l is lr, when a random element $\boldsymbol{a}$ of the space J_{l+1} is picked up, $\boldsymbol{a} = (a_1, \ldots, a_m)$ is also an element of J_{l+1} with the probability of q^{-r}. If $\boldsymbol{a} \in J_l$, a polynomial $\sum_{i=1}^m a_i p_i$ is transformed by S^{-1} to an element of the union of the steps $l+1, \ldots, L$ of the central equations. Since the polynomial $f := \sum_{i=1}^m a_i p_i$ has only $n-(l-1)r$ independent variables, its quadratic form has the rank $n-(l-1)r$ or less. It should be the criteria to determine that the matrix included in J_{i+1} is also included in J_i. The algorithm of High Rank Attack is shown below. `matrixCheck` in the line 006 is a function that returns true when the rank of $\sum_{i=1}^m a_i P_i$ is equal to or less than lr. Wolf et al. [16] also proposed to use more efficient function `polynomialCheck` which can be used instead of `matrixCheck`. Wolf et al. estimated the time complexity of this algorithm as $\mathcal{O}(L \times mq^r \times n^3)$. mq^r is the number of random generation of the vector and n^3 is the evaluation of the quadratic form. The process is repeated L times.

HighRankAttack($\mathcal{P}$)

Input: $\mathcal{P}$: system of public equations
Output: $\widetilde{T}$ an equivalent copy of the transformation T^{-1}

001 $Q_i \leftarrow$computeMatrix(p_i); $J_L \leftarrow \boldsymbol{F}_q^m$
002 **for** $l \leftarrow L-1$ **downto** 1 **do**
003 $\quad J_l \leftarrow \{0\}$
004 $\quad$ **repeat**

005 $\boldsymbol{a} \in_R J_{l-1}$
006 **if** matrixCheck$(Q_1, \ldots, Q_m, \boldsymbol{a}, l)$ **then**
007 $J_l \cup \leftarrow \{\boldsymbol{a}\}$
008 **until** Dimension$(J_l) =^? lr$
009 $\widetilde{J} \leftarrow J_{l+1} \cup J_l$
010 **for** $i \leftarrow 1$ **to** r **do**
011 $RowVector(\widehat{T}, lr + i) \leftarrow BasisVector(\widetilde{J}, i)$
012 **end for**
013 **end for**
014 **return** $\widetilde{T} \leftarrow \widehat{T}^{-1}$
015 **endproc**

It should be noted that the descending chain of vector subspaces also exists in the Complementary STS systems. The following sequence of linear space

$$I_l := \{\boldsymbol{b}' T^{-1} \mid \boldsymbol{b}' \in \boldsymbol{F}_q^m \wedge b'_{lr+l} = \ldots = b'_m = 0\} \text{ for } 1 \leq l \leq L$$

has the ascending chain $I_1 \subset I_2 \ldots \subset I_L$. Therefore fundamentally Rank Attack is not impossible against Complementary STS. However, it is not possible to identify members of two linear spaces just by comparing the rank of the quadratic form.

$$H_1 = \{\boldsymbol{b}' T^{-1} \mid \boldsymbol{b}' \in \boldsymbol{F}_q^m \wedge b'_{m-r+1} = \ldots = b'_m = 0\}$$
$$H_2 = \{\boldsymbol{c}' T^{-1} \mid \boldsymbol{c}' \in \boldsymbol{F}_q^m \wedge c'_1 = \ldots = c'_r = 0\}$$

Both the polynomial $f = \sum_{i=1}^m a_i p_i$ $((a_1, \ldots, a_m) \in H_1)$ and $g = \sum_{i=1}^m b_i p_i$ $((b_1, \ldots, b_m) \in H_2)$ have the rank $m - r$. It is possible to distinguish members of H_1 and H_2 by comparing the variables of f and g. But when an element of H_1 is happened to be found, it is possible to directly obtain other $m - r$ bases of the $\overline{H_1} \cap \boldsymbol{F}_q^m$.

3.2 Improved High Rank Attack

As described above, Wolf's rank attack probes for $(m - r)$ elements of $\overline{J}_1 \cap \boldsymbol{F}_q^m$. The following function `EliminateHigh` probes for a polynomial with the rank less than $(m - r)$ and find other $(m - r - 1)$ elements with the rank $(m - r)$, which share the kernel (of the quadratic form).

Function: `EliminateHigh`
Input: M: A tuple of $n \times n$ matrices $\{Q_1, \ldots, Q_m\}$
r: Step size
Output: M': Set of matrices within the linear space spanned by M, with the rank within $(n - r)$

001 **loop**
002 **loop**
003 $(a_1, \ldots, a_m) \in_R \boldsymbol{F}_q^m$
004 $R := \sum_{i=1}^m a_i Q_i$
005 **if** $Rank(R) = n - r$ **then**
006 exit the **loop**

007 **end** of the **loop**
008 $K := Kernel(R)$
009 $\boldsymbol{a} \in_R K$
010 $C := \begin{pmatrix} \boldsymbol{a}Q_1 \\ \vdots \\ \boldsymbol{a}Q_m \end{pmatrix}$
011 if $Rank(C) \leq r$ **then**
012 $\tilde{B} := Matrix(Kernel(C))$
013 **exit** the **loop**
014 **end** of the **loop**
015 $M' := \{\sum_{i=1}^{m} b_{ij}Q_i\}$ $(\tilde{B} = (b_{ij}), 1 \leq j \leq m - r)$
016 return M'
017 **endproc**

In the above function `EliminateHigh`, the set of matrices M' also have the structure of Complementary STS. Therefore it is possible to generate sets of matrices with lower rank from M'. The program `BetterHighRankAttack` calls the `EliminateHigh` repeatedly and generate L tuples of square matrices $H_1, \ldots, H_L$.

Program: `BetterHighRankAttack`
Input: $\boldsymbol{P} = (p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}))$: Public Key of Complementary STS structure
r: Size of each Step
Output: Tuple of square matrices $\boldsymbol{H} = \boldsymbol{H}_1||, \ldots, ||\boldsymbol{H}_L$
such that $Kernel(\boldsymbol{H}_1) \subset Kernel(\boldsymbol{H}_2) \ldots \subset Kernel(\boldsymbol{H}_L)$, and corresponding polynomials span the same linear space as $\boldsymbol{P}$.

001 $\boldsymbol{H}_i := \phi$ $(1 \leq i \leq L - 1)$
002 $M := (Q_1, \ldots, Q_m)$ (Q_i is the quadratic form of p_i)
003 **for** i from 1 to L **loop**
004 $M' :=$ `EliminateHigh`(M, r)
005 $W := LinearSpace(M \cap \overline{M'})$
006 $\boldsymbol{H}_i := Basis(W)$
007 $M := M'$
008 **end** of the **for loop**
009 return $\boldsymbol{H}_1||\boldsymbol{H}_2|| \ldots ||\boldsymbol{H}_L$
010 **endproc**

Let I_i be the linear space spanned by rows of the member of the tuple of matrices $\boldsymbol{H}_i$, there is a descending chain $I_1 \supset I_2 \ldots \supset I_{L-1}$. Therefore a tuple of polynomials correspoinding to the tuple of matrices $\boldsymbol{H}$ are easily tranformed into STS structure.

4 Security Improvement by Check Function

4.1 Vulnerability of Underdetermined MPKC signature scheme

Almost all MPKC signature schemes are underdetermined, in order to enable preimage of every message to exist. As well as it increases the public key size compared with the message length (number of equations), it might generate vulnerability for the attackers to exploit. If the signature public key has m polynomials with n variables defined on $GF(q)$, the equation system derived from the public key has q^{n-m} solutions as a rule of thumb. In the case of our Complementary STS signature, there can be more than q^{m-r} valid signatures. We propose here a further security improvement by appending extra polynomials.
It should be noted that most of the MPKC signature public keys have subsets of the variable set. Messages are signed by assigning value to the elements of one subset and solving the consequent equation. Therefore typically the structure of the subsets constitutes an important part of the secret key. In the case of Enhanced STS, variables are specified into subsets $\boldsymbol{u}$ and $\boldsymbol{v}$. Most of the attacks to MPKC signatures are done by finding the elements of the subsets, like done to the Balanced Oil and Vinegar [42]. In case an attack should be developed to distinguish the variables of $\boldsymbol{u}$ from the ones of $\boldsymbol{v}$, the signature scheme is in serious jeopardy.

4.2 System of Check Equations

In case even either one of the two linear spaces spanned by the set of vectors $\boldsymbol{u}$ and the one spanned by $\boldsymbol{v}$ should be found by any remote chance, the signatures would be forged by solving the equation. Tsujii et al.[37] proposed the countermeasure against such cases and named the reinforced Complementary STS public key as "Enhanced STS." Their idea is to limit the acceptable value of the variables in $\boldsymbol{v}$. Together with the public key $\boldsymbol{P}(\boldsymbol{x})$, the system of check equations $\boldsymbol{W}(\boldsymbol{x})$ is published. It is specified as a rule that the valid signature must satisfy both the system of equation $\boldsymbol{P}(\boldsymbol{x}) = \boldsymbol{m}$ and $\boldsymbol{W}(\boldsymbol{x}) = \boldsymbol{0}$, as shown in the Figure 3.

4.3 Generation of the System of Check Equation

It is possible to create a polynomial set $\boldsymbol{W}(\boldsymbol{x})$, all elements of which become 0 when $\boldsymbol{v}$ is equal to the pre-defined vector $\boldsymbol{\alpha} \in \boldsymbol{F}_q^{m-r}$. Let $\boldsymbol{f}(\boldsymbol{u}, \boldsymbol{v}) \in \boldsymbol{F}_q[\boldsymbol{u}, \boldsymbol{v}]^{m-r}$ be a set of random polynomials of $\boldsymbol{x}$. Then the polynomial set $\boldsymbol{W}(\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{u}, \boldsymbol{v}) - \boldsymbol{f}(\boldsymbol{u}, \boldsymbol{\alpha})$ satisfies the condition. The system of check equations is one-time use. The system is renewed every time a message is signed.
Then messages are signed in the following way:

Signing a Message

(i) Invert the Affine transformation T^{-1} to the message $\boldsymbol{m}$

(ii) Assign the pre-defined value $\boldsymbol{\alpha}$, instead of random numbers, to the variables $\boldsymbol{v}$

(iii) The consequent STS polynomials are solved. The solution is $\boldsymbol{s}' \in \boldsymbol{F}_q^n$

(iv) The affine transformation is inverted to the solution. $\boldsymbol{s} := S^{-1}\boldsymbol{s}'$

Verification

(i) It is checked whether $\boldsymbol{P}(\boldsymbol{s})$ is equal to $\boldsymbol{m}$

(ii) It is checked whether $\boldsymbol{W}(\boldsymbol{s})$ is zero vector

This Check Equation is applicable to other public key signature, as long as the algebraic map defined by $\boldsymbol{P}(\boldsymbol{u}, \boldsymbol{\alpha})$ is bijection. Otherwise existence of signature is not assured.

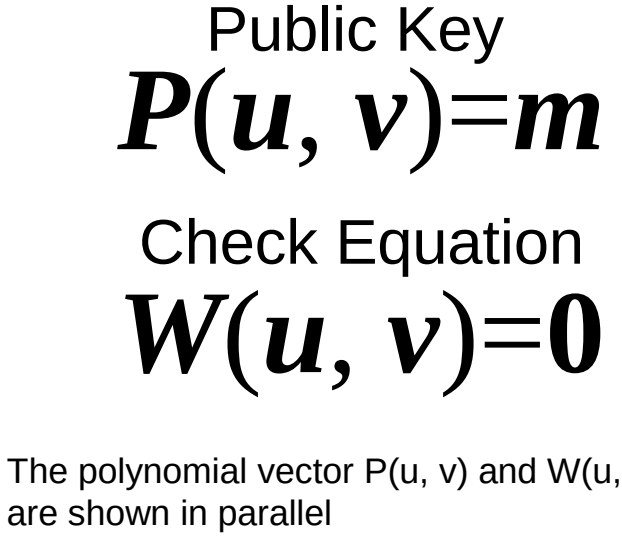

Figure 3: Reinforcement of the Signature Public Key by Check Equation

4.4 Problem of Check Equation

The Check Equation contains a vulnerability that the Check Equation itself gives information on the specification between $\boldsymbol{u}$ and $\boldsymbol{v}$. It should be noted that the polynomial vector $\boldsymbol{W}$ has the form of "balanced Oil and Vinegar," with $\boldsymbol{v}$ as the vinegar variable and $\boldsymbol{u}$ the oil. Therefore it is possible to distinguish $\boldsymbol{u}$ from $\boldsymbol{v}$ by the Kipnis-Shamir attack [43]. There is another way of creating new public key by generating linear combination of the public key and check equation [44]. However, this system gives some information to attckers, that all valid signatures satisfy some linear equations, regardless of the documents.

Now we face a serious dilemma between hiding information and eliminating degree of freedom. We tried to eliminate the degree of freedom and give constraint. But it turned out that the constraint gives information to attackers. We found an effective way to solve the dilemma with "Hidden Pair of Bijection."

4.5 Hidden Pair of Bijection Signature

Now it is assumed that the variable $\boldsymbol{u}$ and $\boldsymbol{v}$ have the same length of m. Let $\boldsymbol{F}(\boldsymbol{u}) \in \boldsymbol{F}_q[u_1, \ldots, u_m]^m$ be the STS central map of $\boldsymbol{u}$. $\boldsymbol{G}(\boldsymbol{v}) \in \boldsymbol{F}_q[v_1, \ldots, v_m]^m$ be another STS central map of $\boldsymbol{u}$. Let

$\boldsymbol{H}(\boldsymbol{u}, \boldsymbol{v})$ be the random linear combination of cross-term between $\boldsymbol{u}$ and $\boldsymbol{v}$. $H_k = \sum_{i=1,j=1}^{i\leq m, j\leq m} h_{kij} u_i v_j$ $(1 \leq k \leq m)$

Let A_1 and A_2 be regular $m \times m$ matrices. Then the polynomial vector $\boldsymbol{P'}(\boldsymbol{u}, \boldsymbol{v}) := A_1\boldsymbol{F}(\boldsymbol{u}) + A_2\boldsymbol{G}(\boldsymbol{v}) + \boldsymbol{H}(\boldsymbol{u}, \boldsymbol{v})$ is a $2m$-variate polynomial vector. Now this polynomial vector has an interesting property. It becomes bijection of $\boldsymbol{u}$ when $\boldsymbol{v}$ is zero vector. On the other hand, it becomes bijection of $\boldsymbol{v}$ when $\boldsymbol{u}$ is zero vector. In this central map $\boldsymbol{P'}$, the equation system $\boldsymbol{F} + \boldsymbol{H}$ is acting as the check equation of $\boldsymbol{G}$ and inversely, $\boldsymbol{G} + \boldsymbol{H}$ is acting as the check equation of $\boldsymbol{F}$.

Subsequently an affine transformation $S : \boldsymbol{x} \rightarrow \boldsymbol{u}, \boldsymbol{v}$ are applied to create the public key $\boldsymbol{P}(\boldsymbol{x})$:

$$\boldsymbol{P}(\boldsymbol{x}) = \boldsymbol{P'} \circ S(\boldsymbol{x})$$

It should be noted that the matrices A_1 and A_2 are playing the role of left-hand affine transformation T.

Signing the Message
There are two ways to sign:

(i) $\boldsymbol{v}$ is assumed zero vector

(ii) Inverse of the matrix A_1 is multiplied to the message $\boldsymbol{m}$:

$$\boldsymbol{m'} := A_1^{-1}\boldsymbol{m}$$

(iii) The equation $\boldsymbol{F}(\boldsymbol{u}) = \boldsymbol{m'}$ is solved. Let the root be $\boldsymbol{s'} := (s'_1, \ldots, s'_m)$

(iv) Affine transformation S is inverted to $(\boldsymbol{s'}, \boldsymbol{0})$:

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

The message can be signed by setting $\boldsymbol{u}$ to zero vector alternatively.
Then the attacker has no way to know whether $\boldsymbol{u}$ or $\boldsymbol{v}$ is set to zero. Therefore attacker could not distinguish the variable between $\boldsymbol{u}$ and $\boldsymbol{v}$. The structure of $\boldsymbol{F}$ and $\boldsymbol{G}$ is not restricted to STS, as long as they are bijection, such as Sequential Solution or Matsumoto-Imai.

5 Conclusion

We have discussed that it is still possible to attack the Complementary STS structure. As a countermeasure we have proposed the Check Equation system before. This discussion posed a dilemma that the designer of the public key has to tradeoff between hiding information and giving restriction. We have proposed the countermeasure of making $\boldsymbol{u}$ and $\boldsymbol{v}$ symmetric. This system gives constraint that the pre-defined value should be given to the extra variables instead of arbitrary value. At the same time, the information on which variables are set constant is hidden.

We expect that our system becomes a new MPKC signature trapdoor.

Acknowledgment

This work is supported by the Strategic Information and Communications R & D Promotion Programme (SCOPE) from the Ministry of Internal Affairs and Communications of Japan.

References

[1] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa, "A class of asymmetric cryptosystems using obscure representations of enciphering functions, " in 1983 National Convention Record on Information Systems, IECE Japan, 1983.

[2] 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, pp.419–453, New York, NY, USA, 1988, Springer-Verlag New York, Inc.

[3] J. Patarin, "Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt '88," Advances in Cryptology CRYPT0 ' 95, ed. D. Coppersmith, vol.963 of Lecture Notes in Computer Science, pp.248-261, Springer Berlin / Heidelberg, 1995.

[4] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," Advances in Cryptology EUROCRYPT '96, ed. U. Maurer, vol.1070 of Lecture Notes in Computer Science, pp.33-48, Springer Berlin / Heidelberg, 1996.

[5] S. Tsujii, "Public key cryptosystem using nonlinear equations," Proceedings of 8th SITA, 1985.

[6] S. Tsujii, K. Kurosawa, T. Ito, 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, vol.69, no.12, pp.1963–1970, 1986-12.

[7] S. Hasegawa, and T. Kaneko, "An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations," Proceedings of the Symposium on Information Theory and its Applications, JA5-3, 1987.

[8] S. TSUJII, A. Fujioka, and Y. 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, vol.72, no.2, pp.390-397, 1989-02.

[9] S. Tsujii, K. Tadaki, and R. 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 2004/366, 2004.

[10] J. Ding, and J. Wagner, "Cryptanalysis of rational multivariate public key cryptosystems," in Post-Quantum Cryptography, eds. J. Buchmann, and J. Ding, vol.5299 of Lecture Notes in Computer Science, pp.124-136, Springer Berlin / Heidelberg, 2008.

[11] M. KASAHARA, and R. SAKAI, "A construction of public key cryptosystem for realizing ciphertext of size 100 bit and digital signature scheme (asymmetric cipher) (<special section> cryptography and information security)," IEICE transactions on fundamentals of electronics, communications and computer sciences, vol.87, no.1, pp.102-109, 2004-01-01.

[12] M. KASAHARA, and R. SAKAI, "A construction of public-key cryptosystem based on singular simultaneous equations," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.1, pp.74–80, 2005.

[13] T.T. Moh, "A public key system with signature and master key functions," Communications in Algebra, vol.27, no.5, pp.2027–2222, 1999.

[14] L.C. Wang, and F.H. Chang, "Revision of tractable rational map cryptosystem," Cryptology ePrint Archive, Report 2004/046, 2004.

[15] L.C. Wang, B.Y. Yang, Y.H. Hu, and F. Lai, "A " medium-field " multivariate public-key encryption scheme," in Topics in Cryptology CT-RSA 2006, ed. D. Pointcheval, vol.3860 of Lecture Notes in Computer Science, pp.132-149, Springer Berlin / Heidelberg, 2006.

[16] C. Wolf, A. Braeken, and B. Preneel, "Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC," SCN, pp.294-309, 2004.

[17] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," Advances in Cryptology EUROCRYPT '99, ed. J. Stern, vol.1592 of Lecture Notes in Computer Science, pp.206-222, Springer Berlin / Heidelberg, 1999.

[18] J. Ding, and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in Applied Cryptography and Network Security, eds. J. Ioannidis, A. Keromytis, and M. Yung, vol.3531 of Lecture Notes in Computer Science, pp.164-175, Springer Berlin / Heidelberg, 2005.

[19] C. Wolf, and B. 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/`.

[20] L.G. Nicolas T. Courtois, and J. Patarin, "Sflashv3, a fast asymmetric signature scheme," Cryptology ePrint Archive, Report 2003/211, 2003.

[21] J. Patarin, N. Courtois, and L. Goubin, "QUARTZ, 128-bit long digital signatures," in Topics in Cryptology CT-RSA 2001, ed. D. Naccache, vol.2020 of Lecture Notes in Computer Science, pp.282-297, Springer Berlin / Heidelberg, 2001.

[22] V. Dubois, P.A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of Sflash," in Advances in Cryptology - CRYPTO 2007, ed. A. Menezes, vol.4622 of Lecture Notes in Computer Science, pp.1-12, Springer Berlin / Heidelberg, 2007.

[23] A. Shamir, "Efficient signature schemes based on birational permutations," CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, pp.1–12, London, UK, 1994, Springer-Verlag.

[24] D. Coppersmith, J. Stern, S. Vaudenay, J. Stern, and S. Vaudenay, "Attacks on the birational permutation signature schemes," Proceedings of CRYPTO'93, number 773 in LNCS, pp.435–443, Springer-Verlag, 1994.

[25] J. Ding, C. Wolf, and B.Y. Yang, "ℓ-invertible cycles for multivariate quadratic (MQ) public key cryptography," PKC'07: Proceedings of the 10th international conference on Practice and theory in public-key cryptography, pp.266–281, Berlin, Heidelberg, 2007, Springer-Verlag.

[26] C. Clough, J. Baena, J. Ding, B.Y. Yang, and M.S. Chen, "Square, a new multivariate encryption scheme," CT-RSA, pp.252-264, 2009.

[27] J. Baena, C. Clough, and J. Ding, "Square-Vinegar signature scheme," in Post-Quantum Cryptography, eds. J. Buchmann, and J. Ding, vol.5299 of Lecture Notes in Computer Science, pp.17-30, Springer Berlin / Heidelberg, 2008.

[28] L. Goubin, and N. Courtois, "Cryptanalysis of the TTM cryptosystem," ASIACRYPT '00: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security, pp.44–57, London, UK, 2000, Springer-Verlag.

[29] Y. Hashimoto, and K. Sakurai, "On construction of signature schemes based on birational permutations over noncommutative rings," Proceedings of the First International Conference on Symbolic Computation and Cryptography (SCC 2008), pp.218–227, 2008.

[30] A. Braeken, C. Wolf, and B. Preneel, "A study of the security of Unbalanced Oil and Vinegar signature schemes," in Topics in Cryptology CT-RSA 2005, ed. A. Menezes, vol.3376 of Lecture Notes in Computer Science, pp.29-43, Springer Berlin / Heidelberg, 2005.

[31] B.Y. Yang, and J.M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new TTS," in Information Security and Privacy, eds. C. Boyd, and J.M. Gonzalez Nieto, vol.3574 of Lecture Notes in Computer Science, pp.518-531, Springer Berlin / Heidelberg, 2005.

[32] S. Tsujii, K. Tadaki, M. Gotaishi, R. Fujita, and M. Kasahara, "Proposal of integrated mpkc: PPS — STS enhanced by perturbed piece in hand method —", journal="technical report of ieice, isec2009-27, site2009-19, icss2009-41 (2009-07)," vol.109, no.115, pp.139-146, 2009-06-25.

[33] S. Tsujii, K. Tadaki, M. Gotaishi, R. Fujita, and M. Kasahara, "Proposal of pps multivariate public key cryptosystems," Cryptology ePrint Archive, Report 2009/264, 2009.

[34] S. TSUJII, M. GOTAISHI, and K. TADAKI, "Proposal of multivariate public key signature scheme applying the sts cryptosystem : Complementary sts signature," Technical report of IEICE. ISEC, vol.109, no.271, pp.55-60, 2009-11-05.

[35] S. Tsujii, M. Gotaishi, K. Tadaki, and R. Fujita, "Proposal of multivariate public key signature scheme applying the STS cryptosystem: Part II —enhanced STS signature—," Symposium on Cryptography and Information Security, 3A2-2, 2010.

[36] L.C. Wang, Y.H. Hu, F. Lai, C.Y. Chou, and B.Y. Yang, "Tractable rational map signature," in Public Key Cryptography - PKC 2005, ed. S. Vaudenay, vol.3386 of Lecture Notes in Computer Science, pp.244-257, Springer Berlin / Heidelberg, 2005.

[37] S. Tsujii, M. Gotaishi, K. Tadaki, and R. Fujita, "Proposal of a signature scheme based on STS trapdoor," in Post-Quantum Cryptography, ed. N. Sendrier, vol.6061 of Lecture Notes in Computer Science, pp.201-217, Springer Berlin / Heidelberg, 2010.

[38] N. Courtois, M. Daum, and P. Felke, "On the security of HFE, HFEv- and QUARTZ," in Public Key Cryptography PKC 2003, ed. Y. Desmedt, vol.2567 of Lecture Notes in Computer Science, pp.337-350, Springer Berlin / Heidelberg, 2002.

[39] Jaques Patarin, "HFE first challenge," 1996, http://www.minrank.org/challenge1.txt

[40] J.C. Faugere, and A. Joux, "Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Grobner Bases," in Advances in Cryptology - CRYPTO 2003, vol.2729 of Lecture Notes in Computer Science, pp.44-60, Springer Berlin / Heidelberg, 2003.

[41] C. Wolf, A. Braeken, and B. Preneel, "Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC," Cryptology ePrint Archive, Report 2004/237, 2004, (Extended version of [16]).

[42] J. Patarin, "The Oil and Vinegar signature scheme," Presented at the Dagstuhl Workshop on Cryptography, September 1997.

[43] A. Kipnis, and A. Shamir, "Cryptanalysis of the Oil & Vinegar signature scheme," in Advances in Cryptology CRYPTO '98, ed. H. Krawczyk, vol.1462 of Lecture Notes in Computer Science, pp.9-17, Springer Berlin / Heidelberg, 1998.

[44] M. Gotaishi, K. Tadaki, R. Fujita, and S. Tsujii, "Dually-perturbed matsumoto-imai signature (DPMS) scheme," IEICE transactions on fundamentals of electronics, communications and computer sciences, vol.E93-A, no.6, pp.1078-1085, 2010-06-01.