Proposal of a Signature Scheme based on STS Trapdoor

Shigeo Tsujii[†] Masahito Gotaishi[†] Kohtaro Tadaki[†] Ryou Fujita[†]

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

Abstract. A New digital signature scheme based on Stepwise Triangular Scheme (STS) is proposed. The proposed trapdoor has resolved the vulnerability of STS and secure against both Gröbner Bases and Rank Attacks. In addition, as a basic trapdoor, it is more efficient than the existing systems. With the efficient implementation, the Multivariate Public Key Cryptosystems (MPKC) signature public key has the signature longer than the message by less than 25 %, for example.

Key words: public key cryptosystem, multivariate polynomial, multivariate public key cryptosystem, stepwise triangular scheme, digital signature

1 Introduction

Various kinds of Multivariate Public Key Cryptosystem (MPKC) are actively developed worldwide. Like traditional cryptosystems such as RSA or ElGamal, MPKCs are used both for encryption and signature. Historically most of them are based on either of the two 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 [24]. The new cryptosystem, which is widely known as "Matsumoto-Imai cryptosystem" (MI), was proposed in EUROCRYPT in 1988 [25]. MI was successfully cryptanalyzed by Patarin [27]. Patarin has extended the idea of MI further and proposed Hidden Field Equation (HFE) cryptosystem in 1996 [28]. Both MI and HFE are applied to signature schemes, resulting in SFLASH and QUARTZ [7, 31]. Although SFLASH was accepted as one of the final selections for the NESSIE, it was cryptanalyzed by Shamir et al. [14] in 2007. QUARTZ was one of the candidates for short digital signatures of NESSIE, but it consumes so much memory that it is difficult to implement in a practical system.

(ii) STS Trapdoor (Tsujii, et al. Shamir, Kasahara, et al.)
STS trapdoor was proposed by the group in Tokyo Institute of Technology led by Tsujii in 1985 [33]. Its initial scheme, which was named "Sequential Solution Method" [34], was cryptanalyzed by Kaneko, et al. in 1987 [18]. Tsujii et al. proposed the improved version in 1989 [35]. While the above cryptosystems have been proposed in Japan for encryption, Shamir proposed the signature scheme based on the same trapdoor, with its linear polynomials hidden, in CRYPTO 1993 [32]. His signature was also cryptanalyzed by Coppersmith et al. [5], with the attack similar to the Rank Attack, which is described later in this paper. 1989 version of Tsujii's cryptosystem, which was translated to English by Tadaki, et al. and

Table 1: Taxonomy of MPKC

Basic Scheme	Encryption	Signature
MI- HFE	MI Scheme A or C^* [25]	SFLASH [7]
	Hidden Field Equation [28]	QUARTZ [31]
	ℓ-IC [11]	ℓ-IC$^-$ [11]
	Square [4]	Square-Vinegar [1]
STS [17, 42]	Sequential Solution Method [34]	Birational Permutation [32, 19]
	TTM [26]	TTS [3, 43]
	RSE [20], RSSE [21]	Our Proposal
	Tractable Rational Map [39], MFE [41]	TRMS [40]
UOV	None	Unbalanced Oil and Vinegar [23], Rainbow [10]

published on the Cryptology ePrint Archive [36] in 2004, was cryptanalyzed by Ding et al. in PQCrypto 2008 [12].
Afterwards Kasahara et al. actively published various schemes including RSE, generalizing the concept of Sequential Solution Method [20, 21]. Moh et al. proposed their scheme utilizing the Sequential Solution Method [26, 39, 41]. 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) [42]. Here the family of MPKCs based on the trapdoor of Sequential Solution Method is called "STS scheme" in this paper.

Although both MI-HFE and STS have been studied for long time, it would safely be said that the application of STS to signatures is not so thoroughly discussed yet [3, 43, 40, 19] compared with the MI-HFE. On the other hand, one of the MPKCs exclusively for signature is UOV (Unbalanced Oil and Vinegar) scheme, which was proposed in 1999 and also well-known worldwide [29, 23]. The current situation is illustrated in the Table 1. We propose a new signature scheme based on STS. Random variables are included in each step according to the number of variables. All of the resulting polynomials have the same number of variables and therefore every public key polynomial has the same rank, regardless of the step (refer to Figure 4 and formula (1)). The resulting system would become secure against both Gröbner bases and Rank attack. We have presented the idea of applying the concept to encryption system [38][37]. Here we propose a signature scheme. As explained in the subsequent sections, the signature scheme which we propose here has the structure entirely different from STS, although it is based on STS scheme. Our scheme would be specified as another basic trapdoor for signatures.

2 Preliminaries

2.1 General Design of MPKC

In general, MPKCs are structured as shown in Figure 1 and Figure 2.

Figure 1 shows the case of encryption, Figure 2 the signature. The plaintext variable vector is

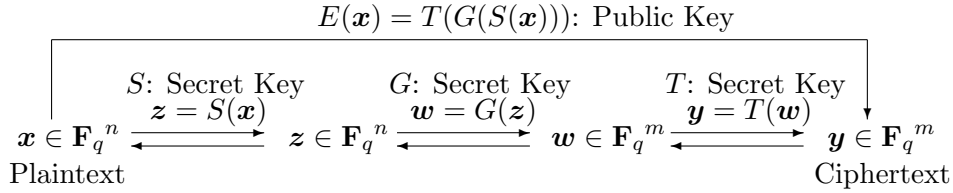


Figure 1: Multivariate Public Key Cryptosystem (Encryption Scheme)

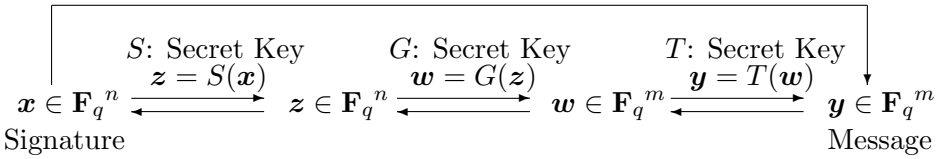


Figure 2: Multivariate Public Key Cryptosystem (Signature Scheme)

transformed to intermediate variable vector by the initial affine transformation S in the encryption scheme. On the other hand, in signature schemes, it is the message variable vector that is transformed. Subsequently, the central map part transforms the intermediate vector with the system of polynomials (usually quadratic) which has some trapdoor structure. Finally, intermediate polynomial vector is transformed by the affine transformation T to form the polynomial vector. The resulting polynomial vector is the public key.

2.2 Summary of STS Scheme and its Security

Sequential Solution Method [34] is a cryptosystem for encryption. The equation system obtained by inverting the affine transformation is shown in Figure 3, where the last polynomial is univariate. And the number of variables increases as the sequential number of the polynomial decreases. When the i variables up to v_i are obtained by solving the n-th to $(n-i+1)$-th equation, the $(n-i)$-th equation becomes univariate by substituting the variables up to v_i with solution. The system is thus solved by solving the sequence of univariate equations one by one, as shown in Figure 3. Random Singular Simultaneous Equation (R(S)SE) cryptosystem [20][21] 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 equation in the L-th step. $(L-1)$-th step has 4 polynomials with 8 variables. Among them, 4 variables are obtained by solving the 4-variate *determined* system of equation in the L-th step. In this way, the overall system is solved by solving the subsystems of equation 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:

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

Figure 3: Non-linear Transformations in the Sequential Solution Method

(i) Vulnerability to the Gröbner Bases Attack [6, 15]
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 HFE [15]. 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 [17, 42]
Since public key and central map polynomials of MPKCs are quadratic, Since elements of the 1st layer have n variables, In the STS scheme where r is 4, the linear space spanned by the central map polynomials has 4 linearly independent polynomials with the rank less than 4. Likewise, it has 8 polynomials with the rank up to 8. If the public key is 100-variate *determined* polynomial system, the linear space spanned by the polynomials has 25 subspaces with the dimension 4. The central map polynomial vector is hidden by the affine transformation T. However, it is possible to compute a transformation equivalent for the inverse transformation T^{-1}. If it is found, low-rank central equations, which are easy to solve, are computed from the public key [17, 42]. Therefore it should be possible to compute the bases of the linear space equivalent for the central map vectors. Although the effectiveness of the Rank Attack should be discussed more in detail, we have to consider the countermeasure against Rank Attack in designing MPKCs. It has been pointed out that STS scheme is also vulnerable to Rank Attack.

3 Enhanced STS Scheme

3.1 The Key Idea

The vulnerability of the STS Scheme to Rank Attack is caused by the difference of rank among each step. On the other hand, all polynomials in the top steps of STS are random and with high rank. Therefore if two independent STS schemes are symmetrically combined together, this vulnerability would be corrected. One of the systems increases the number of variables by r from the initial r variables and the other decreases by r from the initial m. If a new central map is created by linearly combining the elements of each system in the same step, the rank of all elements in the central map becomes the same. Consequent cryptosystem should be secure both against Gröbner Bases and Rank Attack. The concept of the structure is illustrated in Figure 5. The purpose of

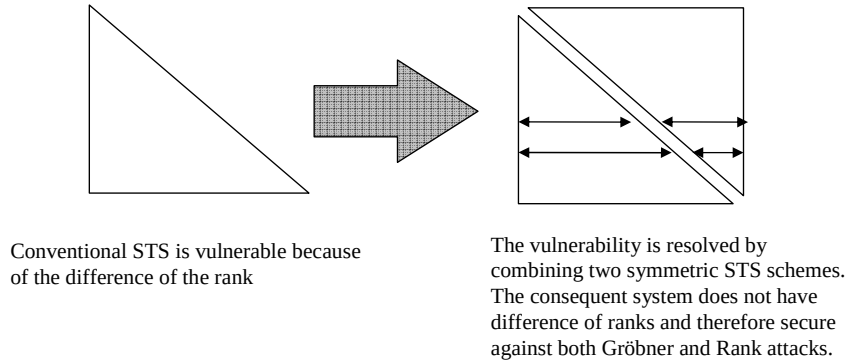


Figure 4: Basic Idea of Enhanced STS

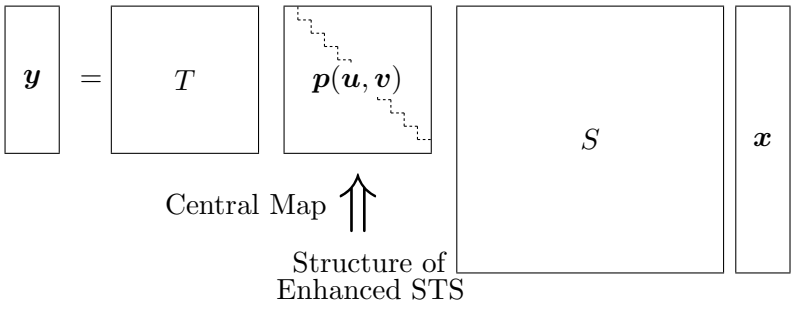


Figure 5: Structure of Enhanced STS

Figure 5 is to describe the essentials of our idea and therefore we prioritized the understandability over the preciseness, i.e. the definition and description of $\boldsymbol{u}, \boldsymbol{v}$ is not accurate. Precise definition of polynomials and variables are provided in the next subsection.

3.2 Enhanced STS Trapdoor

Enhanced STS Signature Scheme is described as follows:
$\boldsymbol{u} := (u_1, \ldots, u_m)$ and $\boldsymbol{v} := (v_1, \ldots, v_{m-r})$ are sets of variables. The number of the steps L is equal to m/r, hence m must be divisible by r. Let the polynomial vectors $\boldsymbol{p} \in \boldsymbol{F}_q[\boldsymbol{u}, \boldsymbol{v}]^m$ be a polynomial vector described in the formula (1). The length of the variable $\boldsymbol{x}$ (signature length) is $n(= 2m - r)$. Polynomials in the step 1 of $\boldsymbol{p}$ 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 $\boldsymbol{v}$.

$$
\begin{array}{ll}
\text{Step } 1 & \left\{ \begin{array}{l} p_1(u_1, \ldots, u_r,\ v_1, \ldots, v_{m-r}) \\ \qquad\qquad\qquad\qquad \vdots \\ p_r(u_1, \ldots, u_r,\ v_1, \ldots, v_{m-r}) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } i & \left\{ \begin{array}{l} p_{(i-1)r+1}(u_1, \ldots, u_{ir},\ v_{(i-1)r+1}, \ldots, v_{m-r}) \\ \qquad\qquad\qquad\qquad \vdots \\ p_{(i-1)r+r}(u_1, \ldots, u_{ir},\ v_{(i-1)r+1}, \ldots, v_{m-r}) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } L-1 & \left\{ \begin{array}{l} p_{(L-2)r+1}(u_1, \ldots, u_{m-r}, v_{m-2r+1}, \ldots, v_{m-r}) \\ \qquad\qquad\qquad\qquad \vdots \\ p_{(L-2)r+r}(u_1, \ldots, u_{m-r}, v_{m-2r+1}, \ldots, v_{m-r}) \end{array} \right. \\
\text{Step } L & \left\{ \begin{array}{l} p_{(L-1)r+1}(u_1, \ldots, u_m) \\ \qquad\qquad\qquad\qquad \vdots \\ p_{(L-1)r+r}(u_1, \ldots, u_m) \end{array} \right.
\end{array}
\tag{1}
$$

All polynomials of $\boldsymbol{p}$ have the rank m, but when constant value $\boldsymbol{c} := (c_1, \ldots, c_{m-r})$ are assigned to $\boldsymbol{v}$, the consequent polynomial vector $\boldsymbol{p}' = \boldsymbol{p}(\boldsymbol{u}, \boldsymbol{c})$ has STS structure (formula (2)).

$$
\begin{array}{ll}
\text{Step } 1 & \left\{ \begin{array}{l} p'_1(u_1, \ldots, u_r) \\ \qquad\qquad \vdots \\ p'_r(u_1, \ldots, u_r) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } i & \left\{ \begin{array}{l} p'_{(i-1)r+1}(u_1, \ldots, u_{ir}) \\ \qquad\qquad \vdots \\ p'_{(i-1)r+r}(u_1, \ldots, u_{ir}) \end{array} \right. \\
\qquad\qquad \vdots & \\
\text{Step } L-1 & \left\{ \begin{array}{l} p'_{(L-2)r+1}(u_1, \ldots, u_{m-r}) \\ \qquad\qquad \vdots \\ p'_{(L-2)r+r}(u_1, \ldots, u_{m-r}) \end{array} \right. \\
\text{Step } L & \left\{ \begin{array}{l} p'_{(L-1)r+1}(u_1, \ldots, u_{m-r}, \ldots, u_m) \\ \qquad\qquad \vdots \\ p'_{(L-1)r+r}(u_1, \ldots, u_{m-r}, \ldots, u_m) \end{array} \right.
\end{array}
\tag{2}
$$

The central map of the Enhanced STS $\boldsymbol{w}$ is created by substituting $\boldsymbol{u}$ with $\boldsymbol{z}_1 := (z_1, \ldots, z_m)$ and $\boldsymbol{v}$ with $\boldsymbol{z}_2 := (z_{m+1}, \ldots, z_n)$ in the polynomial vector $\boldsymbol{p}$. The linear polynomial vector $\boldsymbol{z} := \boldsymbol{z}_1 || \boldsymbol{z}_2 =$

$(z_1(\boldsymbol{x}), \ldots, z_n(\boldsymbol{x}))$ is the image of the affine transformation $S(\boldsymbol{x})$.

$$\boldsymbol{w} \;:=\; \boldsymbol{p}(\boldsymbol{z}_1, \boldsymbol{z}_2) = \begin{pmatrix} p_1(z_1, \ldots, z_r,\ z_{m+1}, \ldots, z_n) \\ \vdots \\ p_r(z_1, \ldots, z_r,\ z_{m+1}, \ldots, z_n) \\ \vdots \\ \vdots \\ p_{m-2r+1}(z_1, \ldots, z_{m-r},\ z_{n-r+1}, \ldots, z_n) \\ \vdots \\ p_{m-r}(z_1, \ldots, z_{m-r},\ z_{n-r+1}, \ldots, z_n) \\ p_{m-r+1}(z_1, \ldots, z_m) \\ \vdots \\ p_m(z_1, \ldots, z_m) \end{pmatrix} \tag{3}$$

Finally, the public key $\boldsymbol{y}$ is created by applying affine transformation T to the central map $\boldsymbol{w}$

$$\boldsymbol{y} := T(\boldsymbol{w}) \tag{4}$$

Public Key:

- Polynomial Vector $\boldsymbol{y}$

Secret Key:

- Central Map $\boldsymbol{w}$
- Affine Transformations S and T

3.3 Signature and Verification

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

Signature

(i) Apply the inverse affine transformation T^{-1} to the message $\boldsymbol{m}$.

(ii) Substitute each element of $\boldsymbol{v}$ with random number.

(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) Value of $\boldsymbol{x}$ is computed by inverting the affine transformation S to the vector $\boldsymbol{u}||\boldsymbol{v}$. Thus obtained vector $(s_1, \ldots, s_n)$ is the signature of $\boldsymbol{m}$.

Verification

Signature verification is done by assigning the signature $(s_1, \ldots, s_n)$ to $\boldsymbol{x}$ of the public key and checking whether the value is equal to $\boldsymbol{m}$.

4 Discussion of the Security

Following attacks for MPKCs should be possible both to encryption and signature schemes:

(i) Gröbner Bases Attack [6, 15]

(ii) Rank Attack [17, 42]

(iii) Differential Attack [16, 13, 14]

(iv) Other attacks exploiting other Vulnerability of the Trapdoor

Security against these attacks is discussed.

4.1 Security against Gröbner Bases Attack

Besides the constraint on the rank of the two STS systems, quadratic polynomials in the central map are all random. Since coefficients are randomly determined, there is not a structural vulnerability for Gröbner Bases algorithm to exploit. Consequently, it is expected that the system is secure against Gröbner Bases Attack. The above assumption is validated by experiment by a computer.

4.1.1 Experiment

The above Enhanced STS Signature System is implemented in the script language of Magma, the computational algebra system. The public keys generated by the above program were tested the time complexity of Gröbner Bases Attack and compared with the random system of n-variate system with m polynomials.
Since the signature polynomials are underdetermined, usually Gröbner Bases Attacks are done after excess variables are eliminated. In this experiment random values were assigned to the variables $x_{m+1}, \ldots, x_n$. Thus obtained m-variate *determined* polynomial sets are the generators of the ideals.
Computing Environment
We perform the experiments using the computational algebra system Magma. Gröbner bases are computed by $F4$ algorithm implemented in Magma as the function `GroebnerBasis()`. The attack is repeated 10 times for each condition. All computer experiments are performed with the following environment:

(i) Computer: Japan Computing System (JCS) VC98220WSA-4U/T workstation, with CPU AMD Opteron 8220 (2.80 GHz) quadcore and 128 Gbyte Memory

(ii) Magma ver. 2.15-15 running on Red Hat Enterprise Linux Advanced Platform Standard. The computation time is counted by the function `Cputime()` of Magma.

Condition
The parameter r is fixed at 4 and the message length m is varied from 18 to 25. The signature length n is set $2m - r$. The public key is generated under the above condition.

Result is shown in Table 2 and Figure 6.

Table 2: F4 computation time vs. the size of the signed messages

Message Length	F4 Computation Time in Second	
	Enhanced STS	Random System
18	4.06	4.32
19	8.05	8.24
20	17.04	16.47
21	34.44	33.25
22	103.41	99.99
23	166.10	159.57
24	1038.48	1020.04
25	2159.80	2125.24

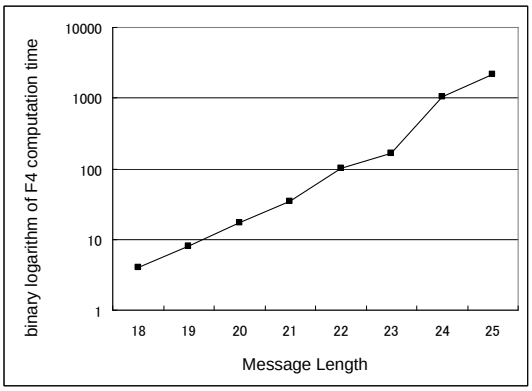


Figure 6: Relationship between the size of the message and binary logarithm of F4 computation time

Not only the time complexity of computation increases exponentially as the message length increases, the F4 computing time is almost equal to the random system. Hence the signature system is expected to be sufficiently secure against Gröbner bases attack.

4.2 Security against Rank Attack

As discussed above, all polynomials in all steps of the central map have the same rank. Since there is not a difference of rank between each polynomial, the public key is entirely inoculate to Rank Attacks.

4.3 Security against Differential Attack

Differential Attack was designed to attack internally perturbed system such as PMI [8] and IPHFE [9], both of which are created by modifying existing trapdoors such as MI and HFE. Since our scheme does not depend on any trapdoors of MI or HFE, it is not applicable.

4.4 Attacks Exploiting Other Vulnerabilities of the Trapdoor

We are going to further investigate its security and discuss whether there is not any such vulnerability.

5 Efficiency of the Basic Trapdoor Scheme

Now the efficiency of the proposed system is discussed by comparing the size of the polynomial with existing schemes. The Oil and Vinegar system, which is classified as the only basic trapdoor for signature, requires the variables to be "Unbalanced." Hence the Vinegar variables must be longer than the Oil variables. Consequently the signature becomes far longer than the message. Although, as shown in the discussion of the security, the proposed system is sufficiently secure with

the signature as short as a twice of the message. Therefore the implementation of the proposed scheme is expected to be more compact than the Unbalanced Oil and Vinegar. Besides, Oil and Vinegar scheme has the constraint that a product of two Oil variables does not exist. Nevertheless, the proposed scheme is not restricted in such a way.
Consequently, our scheme is closer to random polynomials than existing MPKCs and therefore it should be highly secure. Since the time complexity of attacks increases more steeply than existing systems, use of computing resources such as CPU and memory would be more efficient than the existing MPKC signature schemes.

6 Improvement in the Practical Implementation

The new idea of applying the STS cryptosystem to signature scheme is proposed. The structure of the central map was described above. Here we propose further improvement to employ in implementation. One is to shorten the signature (number of variables) and thereby making the public key more compact. Another one is an idea to further improve the security.

6.1 Further Improving the Efficiency of the Public Key

The advantage of the Enhanced STS over existing trapdoors has been described above. Although, the signature is still at least twice (precisely, $(2 - r/m)$ times) as long as the message. Now we propose to divide the overall polynomial system into several blocks. The central map $\boldsymbol{w}$ is divided into k blocks $B_1, \ldots, B_k$, each of which has $b := m/k$ polynomials. So $\boldsymbol{w} := B_1||B_2, \ldots, ||B_k$ $:= [\boldsymbol{p}_1(\boldsymbol{u}_1, \boldsymbol{v}_1), \ldots, \boldsymbol{p}_k(\boldsymbol{u}_k, \boldsymbol{v}_k)]^T$. Each block B_i has the structure of Enhanced STS, where the polynomial system $\boldsymbol{p}_i(\boldsymbol{u}_i, \boldsymbol{v}_i)$ becomes STS when random values are assigned to $\boldsymbol{v}_i$. The elements of each block are algebraic function of $(\boldsymbol{u}_i, \boldsymbol{v}_i)$, where $\boldsymbol{u} := \boldsymbol{u}_1||\boldsymbol{u}_2|| \ldots ||\boldsymbol{u}_k$. The variable set $\boldsymbol{u}_1$ and $\boldsymbol{v}_1$ are given initially and $\boldsymbol{v}_i$ $(2 \leq i \leq k)$ is defined such that the $(b - r)$ dimensional linear space spanned by $\boldsymbol{v}_i$ is contained in the one spanned by $\boldsymbol{u}_1 \cup \boldsymbol{v}_1 \cup \boldsymbol{u}_2 \ldots \boldsymbol{u}_{i-1} \cup \boldsymbol{v}_{i-1}$. As illustrated in Figure 7, the value of $\boldsymbol{v}_i$ is given by solving all systems $B_1, \ldots, B_{i-1}$. In this case the set of variables $\boldsymbol{u}_1 \cup \boldsymbol{u}_2 \ldots \cup \boldsymbol{u}_k \cup \boldsymbol{v}_1 \ldots \cup \boldsymbol{v}_k$ has the dimension $m + b - r$, i.e. the signature length exceeds the message length by $b - r$. Therefore the ratio of signature to message length is $1 + (b - r)/m$. Generally the system takes the above structure. A message is signed as follows.

6.1.1 Signing a Message

(i) Give random values to the variables $\boldsymbol{v}_1$.

(ii) Equation system B_1, which becomes STS, is solved to find the values of $\boldsymbol{u}_1$.

(iii) Since the value of $\boldsymbol{v}_1$ and $\boldsymbol{u}_1$ is found, $\boldsymbol{v}_2$ is known.

(iv) Step 2 to 3 are repeated until the last block.

The security of the combined signature system is assured as long as the basic trapdoor of Enhanced STS is structurally secure.

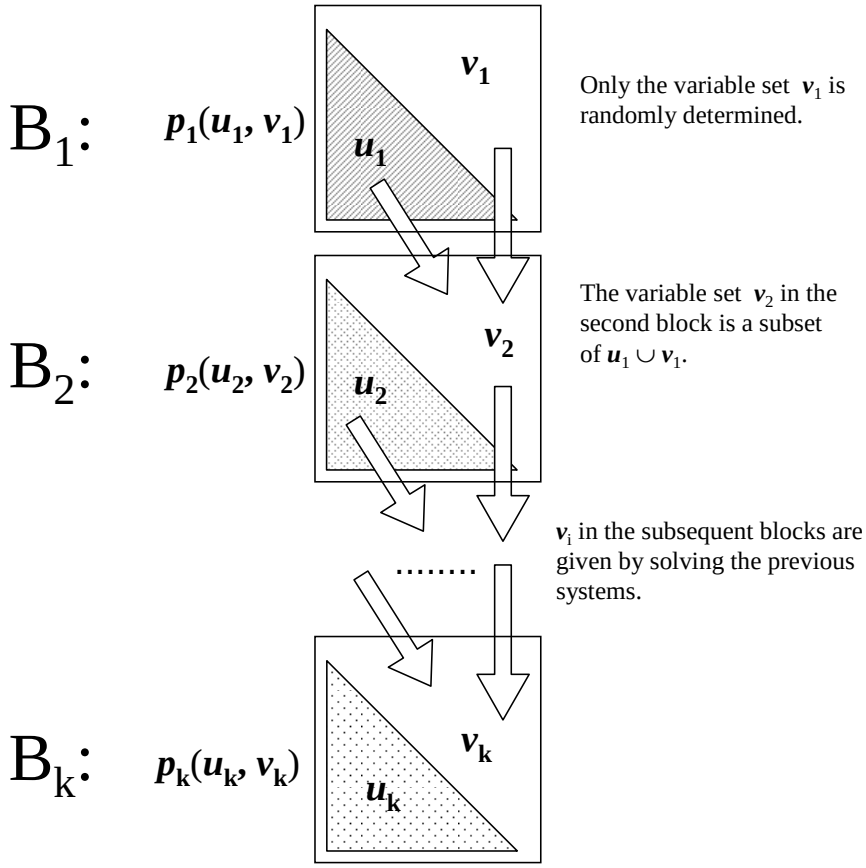


Figure 7: Implementation of Enhanced STS and operation of signing

6.1.2 Example

If a system has the message length $m = 256$ and the STS step size $r = 4$, and divided into 4 blocks ($k = 4$), each block has $m/k = 64$ polynomials. Each variable set $\boldsymbol{u}_i$ has 64 elements and $\boldsymbol{v}_i$ has 56. In this case the signature length is $256 + 64 - 4 = 316$, which is approximately 1.23 times as long as the message. Although characteristic of the finite field is 2 in the above discussion, we think that the base ring should be $GF(2^8)$. Other environmental factor should have to be considered in the actual implementation.

6.2 Security Improvement by Check Polynomial System

6.2.1 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 [29]. 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.

6.2.2 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. Although, it is possible to further improve its security by limiting the acceptable value of the variables in $\boldsymbol{v}$. Together with the public key $\boldsymbol{p}(\boldsymbol{x})$, the system of check equations $\boldsymbol{g}(\boldsymbol{x})$ 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 $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{o}$. The difference of the signing and verifying procedure between the conventional MPKC signature and the one using the check polynomials is illustrated in Figure 8

6.2.3 Generation of the System of Check Equation

It is possible to create a polynomial set $\boldsymbol{g}(\boldsymbol{x})$, all elements of which become 0 when $\boldsymbol{v}$ is equal to the pre-defined vector $\boldsymbol{\alpha} \in \boldsymbol{F}_2^{m-r}$. Let $\boldsymbol{f}(\boldsymbol{u}, \boldsymbol{v}) \in \boldsymbol{F}_2[\boldsymbol{u}, \boldsymbol{v}]^{m-r}$ be a set of random polynomials of $\boldsymbol{x}$. Then the polynomial set $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{u}, \boldsymbol{v}) - \boldsymbol{f}(\boldsymbol{\alpha}, \boldsymbol{v})$ 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 value $\boldsymbol{\alpha}$ to the variables $\boldsymbol{u}$

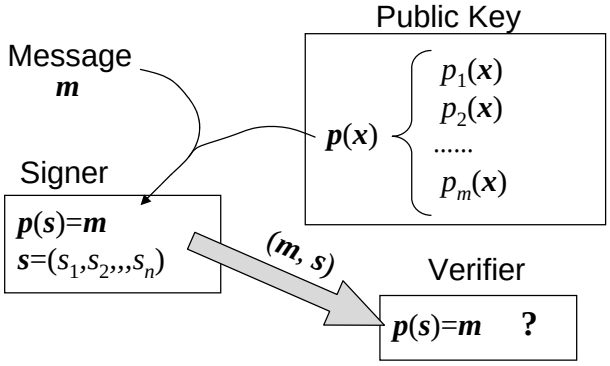
(iii) The consequent STS polynomials are solved. The solution is $\boldsymbol{s'} \in \boldsymbol{F}_2^n$

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

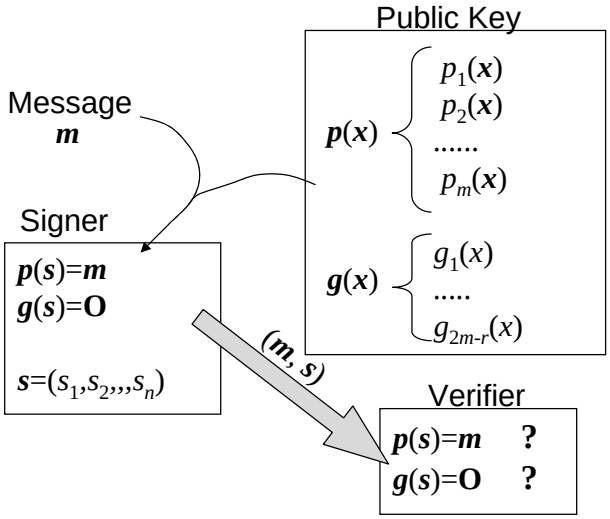
Verification

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

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



(1) Conventional MPKC signature scheme:
There are a number of valid signatures to a given message.



(2) MPKC signature with check equations:
Most of the solution of the equation are excluded from the set of valid signatures. Only the solution which satisfy the n equations are accepted.

Figure 8: Comparison between conventional Signature and the Signature with Check Equation System

7 Conclusion

We proposed a new basic trapdoor for signature scheme based on STS, with two different STS polynomial systems combined together —a system to be called "Enhanced STS." This signature scheme is secure against various existing attacks and more efficient than existing schemes such as UOV, in itself.

Based on the above concept, we proposed a signature system where the signature is still shorter. Consequently this system has a compact public key.
We are going to study further to evaluate and improve the proposed system.

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] J. Baena, C. Clough, and J. Ding. Square-Vinegar signature scheme. *Proc. PQCrypto 2008*, Lecture Notes in Computer Science, Vol.5299, pp.17–30, Springer, 2008.

[2] A. Braeken, C. Wolf, and B. Preneel. A study of the security of unbalanced oil and vinegar signature schemes. *Proc. CT-RSA 2005*, Lecture Notes in Computer Science, Vol.3376, pp.29–43, Springer, 2005.

[3] J. M. Chen and B. Y. Yang. A more secure and efficacious TTS signature scheme. *Proc. ICISC 2003*, Lecture Notes in Computer Science, Vol.2971, pp.320–338, Springer, 2003.

[4] C. Clough, J. Baena, J. Ding, B. Y. Yang, and M. S. Chen. Square, a new multivariate encryption scheme. *Proc. CT-RSA 2009*, Lecture Notes in Computer Science, Vol.5473, pp.252–264, Springer, 2009.

[5] D. Coppersmith, J. Stern, and S. Vaudenay. Attacks on the birational permutation signature schemes. *Proc. CRYPTO '93*, Lecture Notes in Computer Science, Vol.773, pp.435–443, Springer, 1994.

[6] N. Courtois, M. Daum, and P. Felke. On the security of HFE, HFEv- and Quartz. *Proc. PKC 2003*, Lecture Notes in Computer Science, Vol.2567, pp.337–350, Springer, 2003.

[7] N. Courtois, L. Goubin, and J. Patarin. SFLASHv3, a fast asymmetric signature scheme. Cryptology ePrint Archive, Report 2003/211, October 2003. Available at URL: `http://eprint.iacr.org/2003/211` .

[8] J. Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. *Proc. PKC 2004*, Lecture Notes in Computer Science, Vol.2947, pp.305–318, Springer, 2004.

[9] J. Ding and D. Schmidt. Cryptanalysis of HFEv and internal perturbation of HFE. *Proc. PKC 2005*, Lecture Notes in Computer Science, Vol.3386, pp.288–301, Springer, 2005.

[10] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. *Proc. ACNS 2005*, Lecture Notes in Computer Science, Vol.3531, pp.164–175, Springer, 2005.

[11] J. Ding, C. Wolf, and B. Y. Yang. ℓ-Invertible Cycles for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic ($\mathcal{MQ}$) public key cryptography. *Proc. PKC 2007*, Lecture Notes in Computer Science, Vol.4450, pp.266–281, Springer, 2007.

[12] J. Ding and J. Wagner. Cryptanalysis of rational multivariate public key cryptosystems. *Proc. PQCrypto 2008*, Lecture Notes in Computer Science, Vol.5299, pp.124–136, Springer, 2008.

[13] V. Dubois, L. Granboulan, and J. Stern. Cryptanalysis of HFE with internal perturbation. *Proc. PKC 2007*, Lecture Notes in Computer Science, Vol.4450, pp.249–265, Springer, 2007.

[14] V. Dubois, P. A. Fouque, A. Shamir, and J. Stern. Practical cryptanalysis of SFLASH. *Proc. CRYPTO 2007*, Lecture Notes in Computer Science, Vol.4622, pp.1–12, Springer, 2007.

[15] J. C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. *Proc. CRYPTO 2003*, Lecture Notes in Computer Science, Vol.2729, pp.44–60, Springer, 2003.

[16] P. A. Fouque, L. Granboulan, and J. Stern. Differential cryptanalysis for multivariate schemes. *Proc. EUROCRYPT 2005*, Lecture Notes in Computer Science, Vol.3494, pp.341–353, Springer, 2005.

[17] L. Goubin and N. Courtois. Cryptanalysis of the TTM cryptosystem. *Proc. ASIACRYPT 2000*, Lecture Notes in Computer Science, Vol.1976, pp.44–57, Springer, 2000.

[18] 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. *Proc. 10th SITA*, JA5-3, November 1987. In Japanese.

[19] 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.

[20] M. Kasahara and R. Sakai. A construction of public key cryptosystem for realizing ciphertext of size 100 bit and digital signature scheme. *IEICE Transactions on Fundamentals*, E87-A, No.1 (2004), 102–109.

[21] M. Kasahara and R. Sakai. A construction of public-key cryptosystem based on singular simultaneous equations. *IEICE Transactions on Fundamentals*, E88-A, No.1 (2005), 74–80.

[22] A. Kipnis and A. Shamir. Cryptanalysis of the oil and vinegar signature scheme. *Proc. CRYPTO '98*, Lecture Notes in Computer Science, Vol.1462, pp.257–266, Springer, 1998.

[23] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar signature schemes. *Proc. EUROCRYPT '99*, Lecture Notes in Computer Science, Vol.1592, pp.206–222, Springer, 1999.

[24] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa. A class of asymmetric cryptosystems using obscure representations of enciphering functions. *1983 National Convention Record on Information Systems, IECE Japan*, S8-5, 1983. In Japanese.

[25] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. *Proc. EUROCRYPT '88*, Lecture Notes in Computer Science, Vol.330, pp.419–453, Springer, 1988.

[26] T. T. Moh. A public key system with signature and master key functions. Communications in Algebra, 27(5), pp.2207–2222, 1999.

[27] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. *Proc. CRYPTO '95*, Lecture Notes in Computer Science, Vol.963, pp.248–261, Springer, 1995.

[28] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. *Proc. EUROCRYPT '96*, Lecture Notes in Computer Science, Vol.1070, pp.33–48, Springer, 1996.

[29] J. Patarin. The oil and vinegar signature scheme. Presented at the Dagstuhl Workshop on Cryptography, September 1997. transparencies.

[30] J. Patarin, L. Goubin, and N. Courtois. C^*_{-+} and HM: Variations around two schemes of T. Matsumoto and H. Imai. *Proc. ASIACRYPT '98*, Lecture Notes in Computer Science, Vol.1514, pp.35–49, Springer, 1998.

[31] J. Patarin, N. Courtois, and L. Goubin. QUARTZ, 128-bit long digital signatures. *Proc. CT-RSA 2001*, Lecture Notes in Computer Science, Vol.2020, pp.282–297, Springer, 2001.

[32] A. Shamir. Efficient signature schemes based on birational permutations. *Proc. CRYPTO '93*, Lecture Notes in Computer Science, Vol.773, pp.1–12, Springer, 1994.

[33] S. Tsujii. Public key cryptosystem using nonlinear equations. *Proc. 8th SITA*, pp.156–157, December 1985. In Japanese.

[34] 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. *IEICE Transactions* (D), J69-D, No.12 (1986), 1963–1970. In Japanese.

[35] 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. *IEICE Transactions* (A), J72-A, No.2 (1989), 390–397. In Japanese. An English translation of [35] is included in [36] as an appendix.

[36] 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, December 2004. Available at URL: `http://eprint.iacr.org/2004/366` .

[37] S. Tsujii, K. Tadaki, M. Gotaishi, R. Fujita, and M. Kasahara. Proposal of PPS multivariate public key cryptosystems. Cryptology ePrint Archive, Report 2009/264, June 2009. Available at URL: `http://eprint.iacr.org/2009/264` .

[38] S. Tsujii, K. Tadaki, M. Gotaishi, R. Fujita, and M. Kasahara. Proposal of integrated MPKC: PPS — STS enhanced by perturbed piece in hand method —. Technical Report of IEICE, ISEC2009-27, SITE2009-19, ICSS2009-41 (2009-07), July 2009. In Japanese.

[39] L. C. Wang and F. H. Chang. Revision of tractable rational map cryptosystem. Cryptology ePrint Archive, Report 2004/046, 2006. Available at URL: `http://eprint.iacr.org/2004/046` .

[40] L. C. Wang, Y. H. Hu, F. Lai, C. Y. Chou, and B. Y. Yang. Tractable rational map signature. *Proc. PKC 2005*, Lecture Notes in Computer Science, Vol.3386, pp.244–257, Springer, 2005.

[41] L. C. Wang, B. Y. Yang, Y. H. Hu, and F. Lai. A "medium-field" multivariate public-key encryption scheme. *Proc. CT-RSA 2006*, Lecture Notes in Computer Science, Vol.3860, pp.132–149, Springer, 2006.

[42] C. Wolf, A. Braeken, and B. Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. *Proc. SCN 2004*, Lecture Notes in Computer Science, Vol.3352, pp.294–309, Springer, 2004.

[43] B. Y. Yang and J. M. Chen. Building secure tame-like multivariate public-key cryptosystems: the new TTS. *Proc. ACISP 2005*, Lecture Notes in Computer Science, Vol.3574, pp.518–531, Springer, 2005.