Cryptanalysis of Enhanced TTS, STS and all its Variants, or: Why Cross-Terms are Important

Abstract. We show that the two multivariate signature schemes *Enhanced STS* and *Enhanced TTS* are vulnerable due to systematically missing cross-terms. To this aim, we generalize equivalent keys for an improved algebraic key recovery attack. In particular, we demonstrate that it is impossible to choose both secure and efficient parameters for Enhanced STS and break all current parameters of both schemes. Since 2010, many variants of Enhanced STS, such as check equations or hidden pair of bijections were proposed. We break all these variants and show that making STS secure will either lead to a variant known as the Oil, Vinegar and Salt signature scheme or, if we also require the signing algorithm to be efficient, to the well-known Rainbow signature scheme. The latter is a variant of Unbalanced Oil and Vinegar. Enhanced STS was proposed at PQCrypto 2010. We show that our attack is far more efficient than any previously known attack. Enhanced TTS was proposed at ACISP 2005. Besides of rank attacks on early versions of TTS, there are no successful attacks known so far.

Key words: Multivariate Cryptography, Algebraic Cryptanalysis, STS, TTS, Rank Attack, Key Recovery Attack

1 Introduction

All signature schemes discussed in this article use a public multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with

$$\mathcal{P} := \begin{pmatrix} p^{(1)}(x_1, \ldots, x_n) \\ \vdots \\ p^{(m)}(x_1, \ldots, x_n) \end{pmatrix}$$

and

$$p^{(k)}(x_1, \ldots, x_n) := \sum_{1 \leq i \leq j \leq n} \gamma_{ij}^{(k)} x_i x_j = x^{\intercal} \mathfrak{P}^{(k)} x, \text{ for } 1 \leq k \leq m, \gamma_{ij} \in \mathbb{F}_q$$

where $\mathfrak{P}^{(k)}$ is the $(n \times n)$ matrix describing the quadratic form of $p^{(k)}$ and $x = (x_1, \ldots, x_n)^{\intercal}$. Note that we can neglect linear and constant terms for cryptanalytical purposes as they never mix with quadratic terms and thus have no effect for us. The corresponding $\mathcal{MQ}$-problem is $\mathcal{NP}$-complete [6] and thus we

cannot hope to efficiently invert the *general* public map $\mathcal{P}$. However, the trapdoor is given by a structured central map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with

$$\mathcal{F} := \begin{pmatrix} f^{(1)}(u_1, \ldots, u_n) \\ \vdots \\ f^{(m)}(u_1, \ldots, u_n) \end{pmatrix}$$

and

$$f^{(k)}(u_1, \ldots, u_n) := \sum_{1 \le i \le j \le n} \gamma_{ij}^{(k)} u_i u_j = u^\intercal \mathfrak{F}^{(k)} u.$$

To hide the trapdoor we choose two secret linear transformations S, T and define $\mathcal{P} := T \circ \mathcal{F} \circ S$. See figure 1 for illustration.

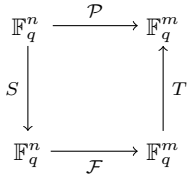


Fig. 1. $\mathcal{MQ}$-Scheme.

One way to achieve a secret map $\mathcal{F} = (f_1, \ldots, f_m)^\intercal$ was given by the *Sequential Solution Method* of Tsujii [14, 17]. The idea was somehow similar to the independently proposed schemes of Shamir [13] and Moh [11]. In 2004 Kasahara and Sakai extended this idea to the so-called RSE system [8], which later was generalized to the *Stepwise Triangular System* (STS) by Wolf *et al.* [18]. Here the central polynomials $f^{(k)}$ are some random quadratic polynomial in a restricted number of variables. See figure 2 for the stepped structure of the resulting $\mathcal{MQ}$-system. Inverting this map is possible as long as solving r quadratic equations in r variables is practical. Consequently, we need to restricts r to rather small values, *e.g.* $r = 4 \ldots 9$.

In the same year Wolf *et al.* [18] showed how to efficiently break the proposed parameters of the STS schemes RSSE(2)PKC and RSE(2)PKC using a HighRank attack. At PQCrypto 2010 Tsujii *et al.* [16] tried to fix the scheme by proposing a new variant called *Enhanced STS*, which uses a complementary STS structure (cf. section 2). Only a few months later they noticed themselves that the scheme is obviously not immune to HighRank attacks, although this was originally a design goal. To fix this problem, they proposed several new variants [7, 15]. In section 2 we will shortly repeat the HighRank Attack. We then give a more efficient algebraic key recovery attack which makes use of a generalization of equivalent keys, which we call *good keys*, and missing cross-terms. The latter are quadratic monomials of two variables from different sets, which do not exist in the central map $\mathcal{F}$ by construction. We conclude that it is impossible

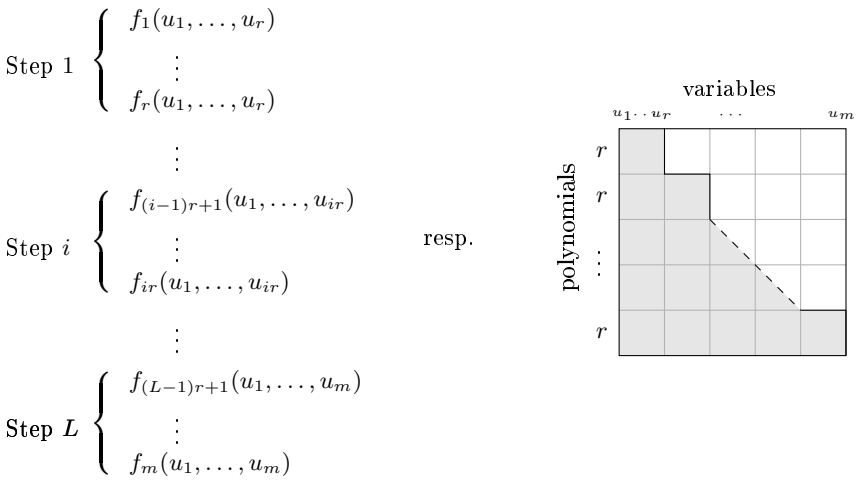


Fig. 2. Central map of STS based signature schemes like RSSE(2)PKC or RSE(2)PKC. The gray parts of the matrix indicate that those variables occur in the corresponding polynomial and white parts indicate that they do not.

to find a secure and efficient parameter set for Enhanced STS. In section 3 we will also break the new variants of STS. In section 4 we apply our attack to Enhanced TTS and break current sets of parameters. In section 5 we discuss possible improvements and conclude our work.

2 Cryptanalysis of Enhanced STS

To exploit different ranks in plain STS, we use the quadratic form of the polynomials $f^{(k)}$, *i.e.* $f^{(k)} = u^\intercal \mathfrak{F}_i u$ for $u = (u_1, \ldots, u_m)^\intercal$ and some $(m \times m)$ matrix $\mathfrak{F}_i$. Note that we have $n = m = Lr$ here. Obviously the rank of these matrices in the i-th step is ir. Now we use that the rank is invariant under the bijective transformation $S^{-1}u = x$ of variables, *i.e.* $\operatorname{rank}(S^\intercal \mathfrak{F}_i S) = \operatorname{rank}(\mathfrak{F}_i)$ for all i. In addition, the public polynomials $p_i = x^\intercal \mathfrak{P}_i x$ are given by some linear combination $\mathfrak{P}_i = \sum_{j=1}^{m} t_{ij} S^\intercal \mathfrak{F}_j S = S^\intercal \left(\sum_{j=1}^{m} t_{ij} \mathfrak{F}_j \right) S$. As the rank is changed by the transformation of equations T, we can use the rank property of the underlying central equations $f^{(k)}$ as a distinguisher to obtain the full transformation T.

Enhanced STS was thought to resist rank attacks. Tsujii *et al.* introduce two sets $U = \{u_1, \ldots, u_m\}$ and $V = \{v_1, \ldots, v_{m-r}\}$ of variables and construct central polynomials $f^{(k)}$ which all have the *same* rank m. The construction is very similar to figure 2, but every polynomial $f^{(k)}$ depends on m variables. See figure 3 for details.

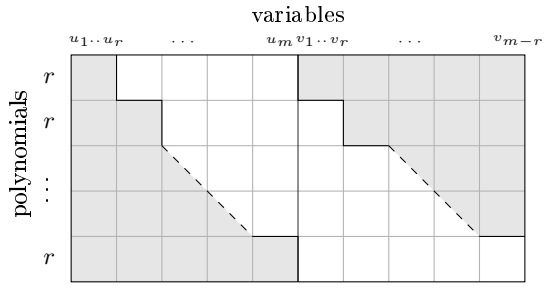


Fig. 3. Central map of Enhanced STS. The gray parts of the matrix indicate that those variables occur in the corresponding polynomial and white parts indicate that they do not.

As the corresponding $\mathcal{MQ}$-system $\mathcal{F}$ has m quadratic equations but $n = 2m - r$ variables, we could fix all variables of V to random values and obtain an $\mathcal{MQ}$-system of r equations and r variables in the first step. Solving this $\mathcal{MQ}$-system, substituting the solution in the next step and so on, allows for a reasonable efficient inversion of $\mathcal{F}$.

Tsujii *et al.* themselves noticed [15] that having the same rank m for the central polynomials $f^{(k)}$ does not prevent rank attacks in any way, as the rank of the public polynomials is $2m - r$. The following simple HighRank attack is still applicable.

HighRank Attack. In order to reconstruct T we have to search for linear combinations of the public polynomials $\mathfrak{P}_i$, such that the rank decrease from $2m-r$ to m. Let $\sigma \in S_m$ be a random permutation, which we need for randomization. Then there exist $\lambda_i \in \mathbb{F}_q$ such that the following linear combination has rank $2m - 2r$ and thus the rank drops by r.

$$\mathfrak{P}_{\sigma(r+1)} + \sum_{i=1}^{r} \lambda_i \mathfrak{P}_{\sigma(i)} =: \widetilde{\mathfrak{P}}$$

There are 2 different solutions, as we can eliminate the r matrices $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ or $\mathfrak{F}_{m-r+1}, \ldots, \mathfrak{F}_m$ such that $\widetilde{\mathfrak{P}}$ has rank $2m - 2r$. In the first case $\widetilde{\mathfrak{P}}$ is a linear combination of secret polynomials, who do not contain variables $v_1, \ldots, v_r$ respectively $u_{m-r+1}, \ldots, u_m$ in the latter case. Thus brute forcing all λ_i has complexity $q^r/2$. Once we have eliminated all the $\mathfrak{F}_i$ of one step in one polynomial $\widetilde{\mathfrak{P}}$ we easily eliminate those $\mathfrak{F}_i$ in all the other $m-r$ polynomials by just determining $\ker(\widetilde{\mathfrak{P}})$. The linear system $\sum_{i=1}^{m} \lambda_i \mathfrak{P}_i \omega = 0$ provides all $m - r$ polynomials of rank $2m - 2r$. The complexity of this first step is $2(2m - r)^3$. Repeating this L times yields r matrices $\mathfrak{F}_i$ of rank m. At this point we know the kernel of one of the central blocks of $\mathcal{F}$ and could use this to separate the matrices in the steps before, which are still linear combinations of some $\mathfrak{F}_i$. Choosing a vector

that lies in the kernel of the matrices obtained in the i-th step, but not in the kernel of matrices recovered in step $i+1, \ldots, L$ easily provides T. The overall complexity of this HighRank attack is given by

$$\frac{L}{2}q^r + 2L(2m-r)^3 + \sum_{i=1}^{L-1}(ir)^3 = \mathcal{O}(q^r).$$

Algebraic Key Recovery Attack. We saw that the complexity of the HighRank attack strongly depends on the field size q and the parameter r. Even if r is restricted to small values due to efficiency constraints, it is possible to choose q large enough to obtain a scheme secure against the previously mentioned attack. For example, let $r = 9$ and $q = 2^9$. Now we describe a new key recovery attack that is almost independent of the field size q and thus makes it impossible to find a parameter set that is both efficient and secure. To ease explanation we fix a parameter set of enhanced STS to illustrate the attack. As there are no parameters given in [15], which is by the way not very courteous to cryptanalyst, we choose $m = 27$, $r = 9$ and $q = 2^9$ as this prevents message recovery attacks via Gröbner Bases on the public key as well as HighRank attacks. The number of steps is given by $L = m/r = 3$. The number of variables is $n = 2m - r = |U| + |V| = 27 + 18 = 45$. Note that a legitimate user would need to solve three generic $\mathcal{MQ}$-system with 9 equations and variables over $\mathbb{F}_{2^9}$ to compute a signature. While possible in theory, it is far too inefficient for practical use. For comparison, solving a generic $\mathcal{MQ}$-system with 3 equations and variables over $\mathbb{F}_{2^9}$ using the fastest known method, *i.e.* the hybrid approach [3] by guessing one variable, as well as the very fast F_4 implementation of Magma V2.16-1 [4] on a Intel Xeon X33502.66GHz (Quadcore) with 4 GB of RAM using only one core, took us 2201 seconds on average. We were not even able to solve a $\mathcal{MQ}$-system with 4 equations and variables over $\mathbb{F}_{2^9}$ due to a lack of memory. But despite of choosing such a large r, we now show that the resulting scheme is still not secure.

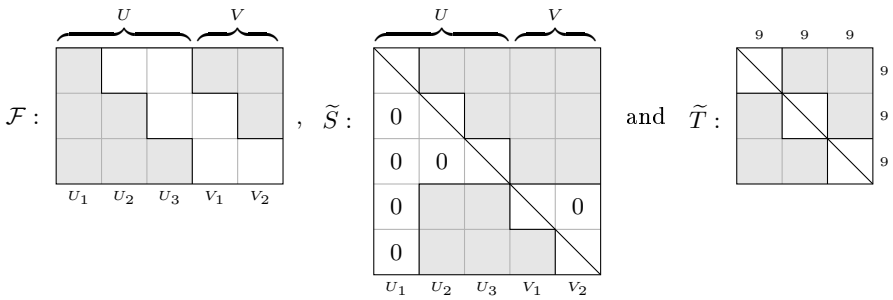


Fig. 4. Central map $\mathcal{F}$ of Enhanced STS and the minimal representative S and T of the class of equivalent keys.

Figure 4 shows the structure of the central map $\mathcal{F}$. The picture describing $\mathcal{F}$ has to be read as figure 3. Every little square denotes a (9×9) array. Moreover, we give the structure of the secret key $\widetilde{S} := S^{-1}$, which is a (45×45) matrix with ones at the diagonal, zeros at the white parts and unknown values at the gray parts. Note that there are many different secret keys S respectively S^{-1} that preserve the structure of $\mathcal{F}$, *i.e.* preserve systematical zero coefficients in the polynomials $f^{(i)}$. We call all them *equivalent keys* and can assume that there is one representative with the structure given in figure 4 with overwhelming probability. The same holds for $\widetilde{T} := T^{-1}$. The notion of equivalent keys was introduced by Wolf *et al.* [19, 20]. We skip the derivation of $\widetilde{S}$ and $\widetilde{T}$ given in figure 4 as it was already known and is very similar to the proof of lemma 1.

An algebraic key recovery attack uses the special structure of $\mathcal{F}$ to obtain equations in $\widetilde{S}$ and $\widetilde{T}$ through the following equality derived from $\mathcal{F} = T^{-1} \circ \mathcal{P} \circ S^{-1}$ with $\widetilde{T} := T^{-1} =: (\widetilde{t}_{ij})$ and $\widetilde{S} := S^{-1}$.

$$\mathfrak{F}_i = \widetilde{S}^{\intercal} \left(\sum_{j=1}^{m} \widetilde{t}_{ij} \mathfrak{P}_j \right) \widetilde{S} \tag{1}$$

As $\mathfrak{P}$ is publicly known and we further know that some of the entries of $\mathfrak{F}$ are systematically zero, we obtain cubic equations in the elements of $\widetilde{S}$ and $\widetilde{T}$. To ease notation in (2) we use $u_{j+m} := v_j$ for $j = 1, \ldots, m-r$. It is interesting to observe that the equations obtained from the coefficients $u_i u_j$ in f_k are of the form

$$0 = \sum_{x=1}^{n} \sum_{y=1}^{n} \sum_{z=1}^{n} \alpha_{xyz} \widetilde{t}_{kx} \widetilde{s}_{yi} \widetilde{s}_{zj} \tag{2}$$

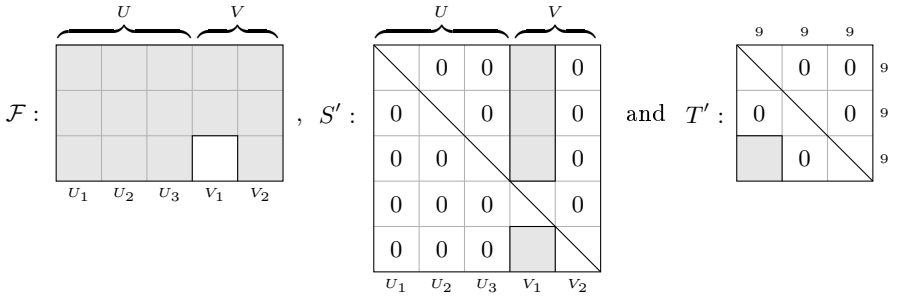
for some coefficients $\alpha_{xyz} \in \mathbb{F}_q$ that depend on the public key matrices $\mathfrak{P}_j$ (cf. [12, Sec. 3] for an explicit formula). In particular every monomial contains one variable of the i-th column and one variable of the j-th column of S. Due to the special form of $\widetilde{S}$ this immediately implies that all equations obtained by zero monomials $u_i u_j$ with $u_i \in U_1 := \{u_1, \ldots, u_9\}$ and $u_j \in U_2 \cup U_3 := \{u_{10}, \ldots, u_{18}\} \cup \{u_{19}, \ldots, u_{27}\}$, as well as $u_i v_j$ with $u_i \in U_1$ and $v_j \in V_1 \cup V_2 := \{v_1, \ldots, v_9\} \cup \{v_{10}, \ldots, v_{18}\}$ become quadratic instead of cubic. This change hence greatly improves the overall attack complexity. Defining $U \times V := \{\{u, v\} \,|\, u \in U, v \in V\}$ the total amount of equations obtained by systematical zeros in $\mathcal{F}$ is

$$\begin{aligned}
&9 \cdot (|(U_2 \cup U_3) \times (U_2 \cup U_3)| + |(U_2 \cup U_3) \times (V_1 \cup V_2)|) \\
&+ 9 \cdot (|(U_3 \cup V_1) \times (U_3 \cup V_1)| + |(U_3 \cup V_1) \times (U_2 \cup V_2)|) \\
&+ 9 \cdot (|(V_1 \cup V_2) \times (V_1 \cup V_2)| + |(V_1 \cup V_2) \times (U_2 \cup U_3)|) \\
&= 27 \cdot (171 + 324) = 13,365 \text{ cubic equations and}
\end{aligned}$$

$$\begin{aligned}
&9 \cdot |(U_2 \cup U_3) \times U_1| + 9 \cdot |(U_3 \cup V_1) \times U_1| + 9 \cdot |(V_1 \cup V_2) \times U_1| \\
&= 27 \cdot 162 = 4374 \text{ quadratic equations.}
\end{aligned}$$

Solving this system of equations in 486 variables $\widetilde{t}_{ij}$ and 1134 variables $\widetilde{s}_{ij}$ with a common Gröbner basis algorithm like F_4 has a total complexity of 2^{877} (cf. [1, 2]). This huge complexity is due to the large number of variables and the fact that the complexity estimation assumes *generic equations* and thus does not take the structure of the equations into account. In order to decrease the complexity, we have to break down the problem into smaller pieces. This can be done if we further decrease the number of variables in $\widetilde{S}$ and $\widetilde{T}$. Therefore we generalize the notion of equivalent keys to keys that do not preserve the *whole* structure of $\mathcal{F}$ but just parts of it. We call these keys *good keys* if they also reveal some parts of the keys $\widetilde{S}$ respectively $\widetilde{T}$. At a first glance it is not clear that such good keys actually exists. The following lemma proves the existence of good keys and constructively give a special class of them.

Lemma 1. *Let $\widetilde{S}$ and $\widetilde{T}$ be equivalent keys for enhanced STS of the form given in figure 4. Then there exist good keys S' and T', of the following form.*



S' is all zero except the gray parts, which are equal to the corresponding values in $\widetilde{S}$ and the diagonal, which contains only ones. Similarly, the gray parts of T' equal the corresponding values in $\widetilde{T}$.

Proof. To preserve the structure of $\mathcal{F}$ given in lemma 1 we are allowed to map variables $U_1 \cup U_2 \cup U_3 \cup V_2 \mapsto U_1 \cup U_2 \cup U_3 \cup V_2$ as well as $V_1 \mapsto V_1$. As soon as we were to map variables from V_1 to any other set of variables, all polynomials would contain variables from V_1 and thus the whole structure of $\mathcal{F}$ would be destroyed. Now we show that using such a transformation Ω of variables, we can uniquely map $\widetilde{S}$ to S' by $\widetilde{S}\Omega = S'$.

$$\widetilde{S}\Omega := \begin{pmatrix} I & \widetilde{S}^{(1)} & \widetilde{S}^{(2)} & \widetilde{S}^{(3)} & \widetilde{S}^{(4)} \\ 0 & I & \widetilde{S}^{(5)} & \widetilde{S}^{(6)} & \widetilde{S}^{(7)} \\ 0 & 0 & I & \widetilde{S}^{(8)} & \widetilde{S}^{(9)} \\ 0 & \widetilde{S}^{(10)} & \widetilde{S}^{(11)} & I & 0 \\ 0 & \widetilde{S}^{(12)} & \widetilde{S}^{(13)} & \widetilde{S}^{(14)} & I \end{pmatrix} \begin{pmatrix} \Omega^{(1)} & \Omega^{(2)} & \Omega^{(3)} & 0 & \Omega^{(4)} \\ \Omega^{(5)} & \Omega^{(6)} & \Omega^{(7)} & 0 & \Omega^{(8)} \\ \Omega^{(9)} & \Omega^{(10)} & \Omega^{(11)} & 0 & \Omega^{(12)} \\ \Omega^{(13)} & \Omega^{(14)} & \Omega^{(15)} & \Omega^{(16)} & \Omega^{(17)} \\ \Omega^{(18)} & \Omega^{(19)} & \Omega^{(20)} & 0 & \Omega^{(21)} \end{pmatrix} \stackrel{!}{=} S'$$

Obviously $\Omega^{(16)} = I$ and thus $\widetilde{S}^{(3)}, \widetilde{S}^{(6)}$, $\widetilde{S}^{(8)}$ and $\widetilde{S}^{(14)}$ remain unchanged. As $\widetilde{S}$ is regular, all other $\Omega^{(i)}$ are uniquely determined by $\widetilde{S}^{-1}S'$. Showing that T' is a

good key is trivial: If we only want to $f_{2r+1}, \ldots, f_{3r}$ to contain no V_1 variables, we are allowed to map all polynomials except $f_1, \ldots, f_r$ to one another. □

Using the good keys of lemma 1 we end up with 405 cubic equations, 2916 quadratic equations and 405 variables. The complexity of solving such a system using F_4 is still 2^{151}. To bring this game to an end, we only need to assure that f_{30} do not contain the variable v_1. Analogous to lemma 1 we obtain $|(U \cup V_2 \cup V_1 \backslash \{v_1\}) \times \{v_1\}| = 44$ quadratic equations and one cubic equation. Using good keys analogous to lemma 1 we obtain 9 variables t_{27j} for $1 \leq j \leq 9$ as well as 36 variables s_{i28} for $1 \leq i \leq 36$. Applying the generic complexity analysis as before still provides the same, and hence infeasible complexity of 2^{151}. Reason: now the number of equations equals the number of variables, so the overall complexity does not change. To obtain a better attack complexity we somehow have to use the fact that all quadratic equations are bihomogeneous, *i.e.* of the form $\sum_{i=1}^{36} \sum_{j=1}^{9} \alpha_{ij} t_{27j} s_{i28}$ for some $\alpha_{ij} \in \mathbb{F}_q$. In [5] Faugère *et al.* analyzed systems of such a special structure and gave an upper bound on the degree of regularity for F_4. To use their results we first have to guess one variable t_{ij} such that we obtain a system of 44 bihomogeneous equations in 44 variables. According to their results we now obtain a degree of regularity of 9 and a complexity of $2^9 \binom{44+9}{9}^2 \approx 2^{73}$. In general the degree of regularity is r, as we have $r-1$ variables t_{ij} after guessing and thus the complexity of our attack for arbitrary parameters is given by

$$q \binom{2m-1}{r}^2.$$

Once we obtained a single row/column of $\widetilde{S}$ and $\widetilde{T}$, the whole system breaks down as all other elements are now determined through linear equations. To show that this is actually true for *all* elements of $\widetilde{S}, \widetilde{T}$, let us label every equation obtained by a zero coefficient of $u_i u_j$ in f_k by (u_i, u_j, k) (cf. (2)). Now, (u_i, v_1, k) and (v_j, v_1, k) with $i = 1, \ldots, 27$, $j = 1, \ldots, 18$ and $k = 19, \ldots, 26$ provide linear equations in t_{ij} with $i = 19, \ldots, 26$ and $j = 1, \ldots, 9$. Next we can apply the same approach using good keys as above for v_1 to v_i, $i = 2, \ldots, 9$. As we already know the coefficients t_{ij} of the appropriate good key, all bihomogeneous equations become linear in s_{ij}. We can now determine the next blocks in T through linear equations only. We repeat the process until all secret coefficients are recovered.

To summarize our new attack, we first used the fact that cross-terms from $(U \cup V_2) \times V_1$ do not exist to obtain quadratic instead of cubic equations in the key recovery attack. Second, we reduced the number of variables through good keys. And third, we used the special bihomogeneous structure of the equations to lower the attack's complexity. In order to protect the scheme against this attack we either have to increase m or r. But as this would increase the signature length as well as the complexity of the signing algorithm such that Enhanced STS cannot be efficient and secure at the same time. In general it do not seem to be a good idea to use an exponential time signing algorithm (cf. section 5).

3 Cryptanalysis of Enhanced STS Variants

Check Equation Enhanced STS. The original Enhanced STS contain m quadratic equations in $2m-r$ variables in the public key and thus have q^{m-r} possible valid signatures to one message. Even if current algorithms cannot take advantage of underdetermined $\mathcal{MQ}$-systems, Tsujii *et al.* [15] suggested to strength their signature by adding $m-r$ check equations and thus fix one unique signature. Performing message recovery point of view, the attacker now would have to solve a $\mathcal{MQ}$-system of $2m-r$ (public key) equations and variables. Before he had to solve a system of m equations and variables after just guessing the additional $m-r$ variables.

However, the check equations do not affect the algebraic key recover attack in section 2. Moreover, if the check equations are not chosen purely random and thus introducing new structure, the attack may even benefit.

Hidden Pair of Bijection. The overall idea is very general. Take a pair $F_1, F_2 : \mathbb{F}_q^m \to \mathbb{F}_q^m$ of bijections with a disjoint set of variables, *i.e.* $u = (u_1, \ldots, u_m)$ and $v = (v_1, \ldots, v_m)$ and connect them with a function H containing all the cross-terms of u and v. The central polynomial $f^{(k)}$ is given by

$$f^{(k)}(u,v) := F_1(u) + F_2(v) + H(u,v) \text{ for some } H(u,v) := \sum_{j=1}^{m}\sum_{i=1}^{m} \alpha_{ij} u_i v_j.$$

If F_1 and F_2 contain some trapdoor and we assign u or v zero, we can invert the central map. An instantiation of this scheme using the STS trapdoor is depicted in figure 5.

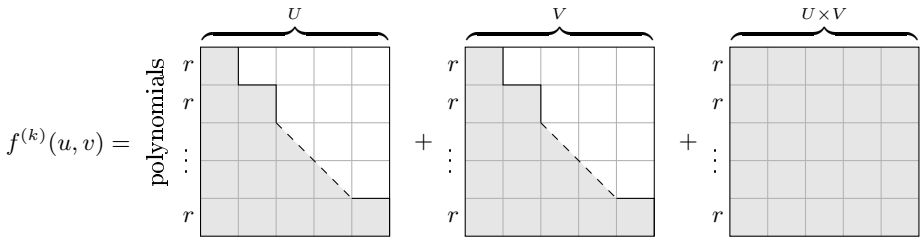


Fig. 5. Secret map $\mathcal{F}$ of Hidden Pair of Bijection using STS trapdoor.

The first observation is that due to the cross-terms in H all the secret matrices $\mathfrak{F}_i$ have full rank $2m$ and thus rank attacks are not trivially applicable. But there is a smart way in applying rank attacks to the scheme. The weak point is the signing algorithm proposed by Tsujii *et al.*, which first chooses u or v to be

zero. They claimed that this would not help an attacker, as his chance to guess the right choice is $\frac{1}{2}$. Well, if we collect $4m-1$ valid signatures $x_1, \ldots, x_{4m-1}$ to arbitrary massages, which are all signed using the same secret S, we can built an efficient distinguisher. We know $X := (x_1^\intercal, \ldots, x_{2m-1}^\intercal)$ is (up to column permutations) of the following form

$$X = S \cdot \begin{array}{|c|c|} \hline & 0 \\ \hline 0 & \\ \hline \end{array}$$

The probability of matrix X to have rank $2m-1$ is $(1/2)^{2m-1} 2\binom{2m-1}{m}$ which is sufficiently large—for example choosing $m = 30$ this equals 0.21. Once we found a collection of signatures $x_1, \ldots, x_{2m-1}$, such that $\mathrm{rank}(X) = 2m-1$ we obtained an efficient distinguisher. If $X || x_j$ for $j \geq 2m$ still has rank $2m-1$ we add x_j to the set A. If the rank increase by one we add x_j to the set B. As soon as both sets A and B are of cardinality m we easily obtain a transformation $\widetilde{S}$ which separates the U and V space through linear algebra. After fixing one of the both sets of variables we obtain a plain STS scheme and can apply the HighRank or the Key Recovery attack from above.

In order to prevent this attack we would have to assign arbitrary values to u respectively v instead of all zeros. This immediately invalidate the trapdoor and renders the scheme unusable. In every step we would have to solve a quadratic underdetermined system of equation without destroying possible solution through guessing variables. We will discuss this question further in section 5.

4 Cryptanalysis of Enhanced TTS

Enhanced TTS was proposed by Yang and Chen in 2005 [21]. The overall idea of the scheme was to use several layers of UOV trapdoors and to make them as sparse as possible. In contrast to UOV this would prevent the Kipnis and Shamir attack [10] without increasing the number of vinegar variables. In fact, while we have a signature blow up of factor 3 for UOV, EnTTS improves this figure to 1.3. As TTS was designed for high speed implementation it uses as few monomials as possible. For the purpose of cryptanalysis we generalize the scheme by adding *more* monomials. In particular, we adapt the definition of EnTTS as follows: As soon as monomial $x_i x_j$ with $x_i \in U$ and $x_j \in V$ occurs in the original TTS polynomial $f^{(k)}$, we just assume that all monomials $x_i x_j$ with $x_i \in U$ and $x_j \in V$ occur as well. This way we easily see that TTS is a very special case of the Rainbow signature scheme. We chose the largest parameter set $(n, m) = (32, 24)$ given in [21] to illustrate the TTS trapdoor in figure 6.
The attack is similar to the one described in section 2. Suppose we just want do preserve zero coefficients of $x_{32} x_i$ in polynomial $u^\intercal \mathfrak{F}_{14} u$. This leads to the good keys given in figure 7 and thus to 31 bihomogeneous equations in 10 variables

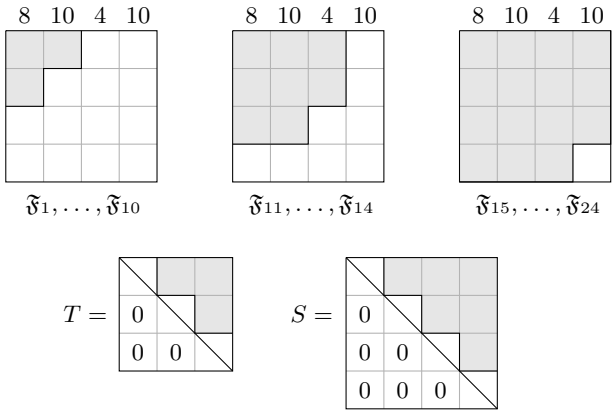


Fig. 6. Secret map $\mathcal{F}$ of TTS $(32, 24)$ and equivalent keys T and S.

t_{14i} with $i = 15, \ldots, 24$ and 24 variables s_{j32} with $j = 1, \ldots, 24$. Analogous to section 2 we first have to guess one variable t_{ij}. Solving the remaining system of 31 bihomogeneous equations in 31 has complexity $2^8 \binom{31+10}{10}^2 \approx 2^{68}$.

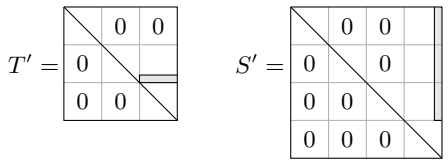


Fig. 7. Good Keys T' and S' for TTS $(32, 24)$.

But due to the special structure of EnTTS we can do even better. Applying the transformation of variables Ω analogous to lemma 1, we see that the monomial $u_{32}u_{32}$ do not occur in *any* of the secret polynomials. This way we additionally obtain 23 quadratic equations in s_{ij}. The complexity of solving a generic system of $23 + 31$ quadratic and 1 cubic equation in 32 variables is $2^{52.4}$. Note that this complexity is just an upper bound as we assumed generic equations and thus did not use the special structure of Enhanced TTS. In particular, we assume that we can effectively break any sensible increase of parameters using extra equations discarded so far.

5 Conclusions or: *Where do we take it from here?*

In summary, we have introduced a new attack that is applicable to both Enhanced STS and Enhanced TTS. It uses equations on cross-terms and the inherent bihomogenious structure of them. Due to the very strong structure of these

schemes, we rate it very unlikely that either of them can be repaired that still allows for an efficient scheme. So the question at hand is if non-linearity could help in any way to improve UOV or Rainbow. Or in other words, is it possible to repair STS at all?

Quick fix. One answer was already given by Kipnis *et al.* in the paper that proposed UOV [9]. One of their possible variants to repair the *balanced* Oil and Vinegar scheme and thus to avoid the attack of Kipnis and Shamir [10] was called *Oil, Vinegar and Salt* signature scheme. Here the variables are divided into three sets O, V and S. The central map $\mathcal{F}$ is constructed such that there are no monomials $u_i u_j$ with $u_i \in O$ and $u_j \in V \cup S$. After fixing the vinegar variables we obtain a system linear in the O variables and quadratic in the S variables. The best known way to solve such a system is to brute-force the S variables and then solve the remaining linear system. This way we loose a factor of $q^{|S|}$ in terms of efficiency. As it turned out later, a modified version of the Kipnis and Shamir attack actually *can* be applied to the Oil, Vinegar and Salt scheme. Ironically, the factor we gain compared to the original scheme is exactly the factor we loose in terms of efficiency. But as the (positive) effect of non-linearity to the public key size is negligible compared to the (negative) effect to the efficiency of the scheme, the best trade-off is to just to skip the salt variables and hence use the original UOV scheme.

The dilemma. STS can be seen as a layer-based version of Oil, Vinegar and Salt. So we can rephrase the question between UOV and UOV+S in this setting. In particular, we have to ask ourselves if the layered structure of STS allows for a better trade-off between efficiency and security than UOV. Unfortunately, we have to leave the final answer as an open question. However, we incline to the negative. To illustrate this, we want to elaborate some thoughts on this matter. One the one hand, it is not clear even for UOV if the ratio between efficiency and security increases for the layer-based scheme Rainbow. Especially the attack of section 4, which is not applicable to UOV, challenges this hope. On the other hand, the attack of Kipnis and Shamir [10] is exponential and not practical for layer-based schemes like Rainbow. So the question remains, if and how much security we can gain at all by introducing some non-linearity in each layer. Our intuition is that the loss of efficiency is always greater or equal than the gain of security in these cases and hence of no avail in practice. The reason is that on the one hand the signing algorithm becomes exponential instead of polynomial, as soon as we introduce non-linear parts. In comparison, the attack stays exponential in *both* cases, *i.e.* there is no security gap between the legitimate user and the attacker.

A way out? The only exception from this rule seem to be Gröbner bases that are used without any additional structure as a trapdoor. Clearly we have to use Vinegar variables in that case, as otherwise MinRank attacks are applicable. We found no way to fuse this into a working scheme—but got the impression that this is not possible at all. Hence, we leave it as an open problem, how to embed a Gröbner Basis into a scheme using Vinegar variables and to derive a both secure *and* efficient scheme.

Bibliography

[1] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[2] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In P. Gianni, editor, *MEGA 2005 Sardinia (Italy)*, 2005.

[3] L. Bettale, J.-C. Faugère, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *In Journal of Mathematical Cryptology*, 3:177–197, 2009.

[4] Computational Algebra Group, University of Sydney. *The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry.* http://magma.maths.usyd.edu.au/magma/.

[5] J.-C. Faugère, M. S. E. Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity. *J. Symb. Comput.*, 46(4):406–437, 2011.

[6] M. R. Garey and D. S. Johnson. *Computers and Intractability — A Guide to the Theory of NP-Completeness.* W.H. Freeman and Company, 1979. ISBN 0-7167-1044-7 or 0-7167-1045-5.

[7] M. Gotaishi and S. Tsujii. Hidden pair of bijection signature scheme. *IACR Cryptology ePrint Archive*, 2011.

[8] M. Kasahara and R. Sakai. A construction of public-key cryptosystem based on singular simultaneous equations. In *Symposium on Cryptography and Information Security — SCIS 2004*. The Institute of Electronics, Information and Communication Engineers, Jan. 27–30 2004. 6 pages.

[9] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar signature schemes — extended version, 2003. 17 pages.

[10] A. Kipnis and A. Shamir. Cryptanalysis of the Oil and Vinegar signature scheme. In *Advances in Cryptology — CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 257–266. Hugo Krawczyk, editor, Springer, 1998.

[11] T. Moh. A public key system with signature and master key function. *Communications in Algebra*, 27(5):2207–2222, 1999. Electronic version: http://citeseer/moh99public.html.

[12] A. Petzoldt, E. Thomae, S. Bulygin, and C. Wolf. Small public keys and fast verification for multivariate quadratic public key systems. In *CHES*, pages 475–490, 2011.

[13] A. Shamir. Efficient signature schemes based on birational permutations. In *Advances in Cryptology — CRYPTO 1993*, volume 773 of *Lecture Notes in Computer Science*, pages 1–12. Douglas R. Stinson, editor, Springer, 1993.

[14] S. Tsujii, A. Fujioka, and Y. Hirayama. Generalization of the public-key cryptosystem based on the difficulty of solving non-linear equations. *The*

Transactions of the Institute of electronics and communication Engineers of Japan, 1989.

[15] S. Tsujii and M. Gotaishi. Enhanced STS using check equation - extended version of the signature scheme proposed in the PQCrypt2010. *IACR Cryptology ePrint Archive*, 2010.

[16] S. Tsujii, M. Gotaishi, K. Tadaki, and R. Fujita. Proposal of a signature scheme based on STS trapdoor. In *PQCrypto*, pages 201–217, 2010.

[17] S. Tsujii, K. Kurosawa, T. Itho, 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*, 1986.

[18] C. Wolf, A. Braeken, and B. Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. In *Conference on Security in Communication Networks — SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 294–309. Springer, Sept. 8–10 2004. Extended version: http://eprint.iacr.org/2004/237.

[19] C. Wolf and B. Preneel. Equivalent keys in HFE, C*, and variations. In *Proceedings of Mycrypt 2005*, volume 3715 of *Lecture Notes in Computer Science*, pages 33–49. Serge Vaudenay, editor, Springer, 2005. Extended version http://eprint.iacr.org/2004/360/, 15 pages.

[20] C. Wolf and B. Preneel. Equivalent keys in multivariate quadratic public key systems. *Journal of Mathematical Cryptology*, 4(4):375–415, 2011.

[21] B.-Y. Yang and J.-M. Chen. Building secure tame-like multivariate public-key cryptosystems: The new TTS. In *ACISP 2005*, volume 3574 of *LNCS*, pages 518–531. Springer, July 2005.