Total Break of the SRP Encryption Scheme

Ray Perlner[1], Albrecht Petzoldt[1], and Daniel Smith-Tone[1,2]

[1]National Institute of Standards and Technology,
Gaithersburg, Maryland, USA
[2]Department of Mathematics, University of Louisville,
Louisville, Kentucky, USA

ray.perlner@nist.gov, albrecht.petzoldt@nist.gov, daniel.smith@nist.gov

Abstract. Multivariate Public Key Cryptography (MPKC) is one of the main candidates for secure communication in a post-quantum era. Recently, Yasuda and Sakurai proposed in [7] a new multivariate encryption scheme called SRP, which combines the Square encryption scheme with the Rainbow signature scheme and the Plus modifier.
In this paper we propose a practical key recovery attack against the SRP scheme, which is based on the min-Q-rank property of the system. Our attack is very efficient and allows us to break the parameter sets recommended in [7] within minutes. Our attack shows that combining a weak scheme with a secure one does not automatically increase the security of the weak scheme.

Keywords: Multivariate Cryptography, SRP Encryption Scheme, Cryptanalysis, min-Q-Rank

1 Introduction

Multivariate cryptography is one of the main candidates to guarantee the security of communication in the post-quantum era [1]. Multivariate schemes are in general very fast and require only modest computational resources, which makes them attractive for the use on low cost devices such as RFIDs or smart cards [2, 3]. While there exist many practical multivariate signature schemes such as UOV [4], Rainbow [5] and Gui [6], the number of secure and efficient multivariate public key encryption schemes is quite limited.

At ICISC 2015, Yasuda and Sakurai proposed in [7] a new multivariate encryption scheme called SRP, which combines the Square encryption scheme [8], the Rainbow signature scheme [5] and the Plus method [9]; hence the name SRP. The scheme is very efficient and has a comparably small blow up factor between plain and ciphertext size. In [7] it is claimed that, by the combination of Square and Rainbow into one scheme, several attacks against the single schemes are no longer applicable.

In this paper we present a new practical key recovery attack against the SRP encryption scheme, which uses the min-Q-rank property of the system to separate the Square from the Rainbow and Plus polynomials. By doing so, we can easily find (parts of) the linear transformations $\mathcal{T}$ and $\mathcal{U}$ used to hide the structure of the central map $\mathcal{F}$ in the public key. The attack is completed by using the known structure of the Rainbow part of the central map.

Our attack is very efficient and allows us (even with our limited resources) to break the SRP instances proposed in [7] for 80 and 112 bit security in 8 minutes and less than three hours respectively. Our attack therefore shows that this attempt to combine several multivariate schemes into one brings no extra security into the system.

Our paper is organized as follows. In Section 2, we give an overview of the basic concepts of multivariate public key cryptography and introduce the SRP encryption scheme of [7]. In Section 3 we recall the concept of the Q-Rank of a quadratic map, while Section 4 describes the main ideas and results of the Kipnis-Shamir attack on HFE needed for the description of our attack. Section 5 describes our key recovery attack against the SRP scheme in detail, whereas Section 6 deals with the complexity of our attack. In Section 7 we present the results of our computer experiments, and Section 8 concludes the paper.

2 The SRP Encryption Scheme

In this section, we recall the SRP scheme of [7]. Before we come to the description of the scheme itself, we start with a short overview of the basic concepts of multivariate cryptography.

2.1 Multivariate cryptography

The basic objects of multivariate cryptography are systems of multivariate quadratic polynomials over a finite field $\mathbb{F}$. The security of multivariate schemes is based on the *MQ Problem* of solving such a system. The MQ Problem is proven to be NP-Hard even for quadratic polynomials over the field GF(2) [10] and believed to be hard on average (both for classical and quantum computers).

To build a multivariate public key cryptosystem (MPKC), one starts with an easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ (*central map*). To hide the structure of $\mathcal{F}$ in the public key, we compose it with two invertible affine (or linear) maps $\mathcal{T} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{U} : \mathbb{F}^n \to \mathbb{F}^n$. The *public key* of the scheme is given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{U} : \mathbb{F}^n \to \mathbb{F}^m$. The relation between the easily invertible central map $\mathcal{F}$ and the public key $\mathcal{P}$ is referred to as a morphism of polynomials.

Definition 1 *Two systems of multivariate polynomials $\mathcal{F}$ and $\mathcal{G}$ are said to be related by a* morphism *iff there exist two affine maps $\mathcal{T}, \mathcal{U}$ such that $\mathcal{G} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{U}$.*

The *private key* consists of the three maps $\mathcal{T}, \mathcal{F}$ and $\mathcal{U}$ and therefore allows to invert the public key.

To encrypt a message $M \in \mathbb{F}^n$, one simply computes $C = \mathcal{P}(M) \in \mathbb{F}^m$.
To decrypt a ciphertext $C \in \mathbb{F}^m$, one computes recursively $\mathbf{x} = \mathcal{T}^{-1}(C) \in \mathbb{F}^m$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x}) \in \mathbb{F}^n$ and $M = \mathcal{U}^{-1}(\mathbf{y})$. $M \in \mathbb{F}^n$ is the plaintext corresponding to the ciphertext C. This process is illustrated in Figure 1.

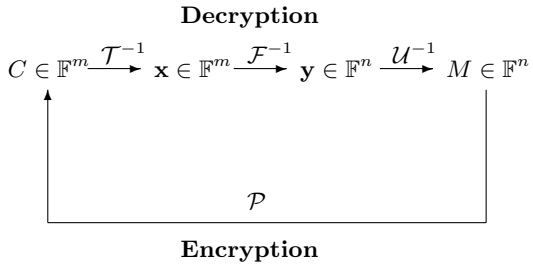


Fig. 1. Encryption and decryption process for multivariate public key encryption schemes

Since, for multivariate encryption schemes, we have $m \geq n$, the pre-image of the vector $\mathbf{x}$ under the central map $\mathcal{F}$ and therefore the decrypted plaintext will (with overwhelming probability) be unique.

2.2 SRP

The SRP encryption scheme was recently proposed by Yasuda and Sakurai in [7] by combining the Square encryption scheme [8], the Rainbow signature scheme [5] and the Plus method [9]. Since both Square and Rainbow are very efficient, the same holds for the SRP scheme. Furthermore, the combination with Rainbow provides an efficient way to distinguish between correct and false solutions of Square. In [7] it is claimed that, by the combination of Square and Rainbow into one scheme, several attacks against the single schemes are no longer applicable.

In this paper, we restrict to variants of SRP in which the Rainbow part is replaced by UOV [4]. Note that the parameter sets proposed in [7] are of this type. However we note that our attack can easily be generalized to variants of SRP which use a Rainbow (and not UOV) map $\mathcal{F}_R$ and that these modifications have no significant effect on the running time of the attack.
We choose a finite field $\mathbb{F} = \mathbb{F}_q$ of odd characteristic with $q \equiv 3 \bmod 4$ and, for an odd integer d, a degree d extension field $\mathbb{E} = \mathbb{F}_{q^d}$. Let $\phi : \mathbb{F}^d \to \mathbb{E}$ be an isomorphism between the vector space $\mathbb{F}^d$ and the field $\mathbb{E}$. Moreover, let o, r, s and l be non-negative integers.

Key Generation Let $n = d + o - l$, $n' = d + o$ and $m = d + o + r + s$. The *central map* $\mathcal{F} : \mathbb{F}^{n'} \to \mathbb{F}^m$ of the scheme is the concatenation of three maps $\mathcal{F}_S$, $\mathcal{F}_R$, and $\mathcal{F}_P$. These maps are defined as follows.

(i) The Square part $\mathcal{F}_S : \mathbb{F}^{n'} \to \mathbb{F}^d$ is the composition of the maps

$$\mathbb{F}^{n'} \xrightarrow{\pi_d} \mathbb{F}^d \xrightarrow{\phi} \mathbb{E} \xrightarrow{X \mapsto X^2} \mathbb{E} \xrightarrow{\phi^{-1}} \mathbb{F}^d.$$

Here $\pi_d : \mathbb{F}^{d+o} \to \mathbb{F}^d$ is the projection to the first d coordinates.

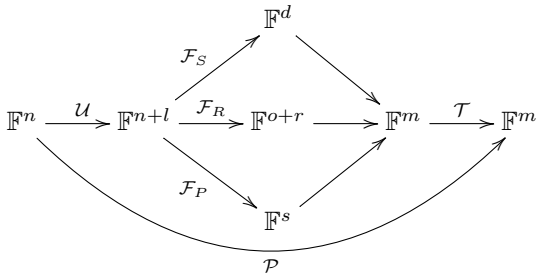
(ii) The UOV (Rainbow) part $\mathcal{F}_R = (f^{(1)}, \ldots, f^{(o+r)}) : \mathbb{F}^{n'} \to \mathbb{F}^{o+r}$ is constructed as the usual UOV signature scheme: let $V = \{1, \ldots, d\}$ and $O = \{d + 1, \ldots, d + o\}$. For every $k \in \{1, \ldots, o + r\}$, the quadratic polynomial $f^{(k)}$ is of the form

$$f^{(k)}(x_1, \ldots, x_{n'}) = \sum_{i \in O, j \in V} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i,j \in V, i \leq j} \beta_{i,j}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \eta^{(k)},$$

with $\alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)}, \gamma_i^{(k)}, \eta^{(k)}$ randomly chosen in $\mathbb{F}$. [1]

(iii) The Plus part $\mathcal{F}_P = (g^{(1)}, \ldots, g^{(s)}) : \mathbb{F}^{n'} \to \mathbb{F}^s$ consists of s randomly chosen quadratic polynomials $g^{(1)}, \ldots, g^{(s)}$.

We additionally choose an affine embedding $\mathcal{U} : \mathbb{F}^n \hookrightarrow \mathbb{F}^{n'}$ of full rank and an affine isomorphism $\mathcal{T} : \mathbb{F}^m \to \mathbb{F}^m$. The *public key* is given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{U} : \mathbb{F}^n \to \mathbb{F}^m$ and the *private key* consists of $\mathcal{T}, \mathcal{F}$ and $\mathcal{U}$.



Encryption: Given a message $M \in \mathbb{F}^n$, the ciphertext C is computed as $C = \mathcal{P}(M) \in \mathbb{F}^m$.

Decryption: Given a ciphertext $C = (c_1, \ldots, c_m) \in \mathbb{F}^m$, the decryption is executed as follows.

(1) Compute $\mathbf{x} = (x_1, \ldots, x_m) = \mathcal{T}^{-1}(C)$.
(2) Compute $X = \phi(x_1, \ldots, x_d) \in \mathbb{E}$.

[1] Note that, while, in the standard UOV signature scheme, we only have o polynomials, the map $\mathcal{F}_R$ consists of $o + r$ polynomials of the Oil and Vinegar type. This fact is needed to reduce the probability of decryption failures (see footnote 3).

(3) Compute $R_{1,2} = \pm X^{(q^d+1)/4} \in \mathbb{E}$ and set $\mathbf{y}^{(i)} = (y_1^{(i)}, \ldots, y_d^{(i)}) = \phi^{-1}(R_i) \in \mathbb{F}^d$ $(i = 1, 2)$. [2]

(4) Given the vinegar values $y_1^{(i)}, \ldots, y_d^{(i)}$ $(i = 1, 2)$, solve the two systems of $o + r$ linear equations in the $n' - d = o$ variables $u_{d+1}, \ldots, u_{n'}$ given by

$$f^{(k)}(y_1^{(i)}, \ldots, y_d^{(i)}, u_{d+1}, \ldots, u_{n'}) = x_{d+k} \quad (i = 1, 2)$$

for $k = 1, \ldots, o + r$. The solution is denoted by $(y_{d+1}, \ldots, y_{n'})$. [3]

(5) Compute the plaintext $M \in \mathbb{F}^n$ by finding the pre-image of $(y_1, \ldots, y_{n'})$ under the affine embedding $\mathcal{U}$.

3 Q-Rank

A critical quantity tied to the security of multivariate BigField schemes is the Q-rank (or more correctly, the min-Q-rank) of the public key.

Definition 2 *Let $\mathbb{E}$ be a degree n extension field of $\mathbb{F}_q$. The Q-rank of a quadratic map $f(\overline{x})$ on $\mathbb{F}_q^n$ is the rank of the quadratic form $\phi \circ f \circ \phi^{-1}$ in $\mathbb{E}[X_0, \ldots, X_{n-1}]$ via the identification $X_i = \phi(\overline{x})^{q^i}$.*

Quadratic form equivalence corresponds to matrix congruence, and thus the definition of the rank of a quadratic form is typically given as the minimum number of variables required to express an equivalent quadratic form. Since congruent matrices have the same rank, this quantity is equal to the rank of the matrix representation of this quadratic form, even in characteristic 2, in which the quadratics x^{2q^i} are additive, but not linear for $q > 2$.

Q-rank is invariant under one-sided isomorphisms $f \mapsto f \circ U$, but is not invariant under isomorphisms of polynomials in general. The quantity that is often meant by the term Q-rank, but more properly called min-Q-rank, is the minimum Q-rank among all nonzero linear images of f. This min-Q-rank is invariant under isomorphisms of polynomials and is the quantity relevant for cryptanalysis.

In particular, min-Q-rank can be defined in circumstances for which Q-rank may make little sense. Specifically, consider the case in which there are more equations than variables, or the case in which we consider an extension field of smaller degree than the number of variables. We may then define min-Q-rank in the following manner.

[2] The fact of $q \equiv 3 \bmod 4$ and d odd allows us to compute the square roots of X by this simple operation. Therefore, the decryption process of both Square and SRP is very efficient.

[3] In [7, Proposition 1] it was shown that the probability of both $(y_1^{(1)}, \ldots, y_d^{(1)})$ and $(y_1^{(2)}, \ldots, y_d^{(2)})$ leading to a solution of the linear system is about $1/q^{-r-1}$. Therefore, with overwhelming probability, one of the two possible solutions is eliminated during this step.

Definition 3 *Let $\mathbb{E}$ be a degree $d < n$ extension field of $\mathbb{F}_q$. The min-Q-rank of a quadratic map $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ over $\mathbb{E}$ is*

$$\textit{min-Q-rank}(f) = \min_{L_1} \max_{L_2} \{ \textit{Q-rank}(L_1 \circ f \circ L_2) \},$$

where $L_1 : \mathbb{F}_q^d \to \mathbb{F}_q^m$ and $L_2 : \mathbb{F}_q^n \to \mathbb{F}_q^d$ are nonzero linear transformations. As above, "Q-rank" computes the rank of its input as a quadratic form over $\mathbb{E}[X_0, \ldots, X_{d-1}]$ via the identification $X_i = \phi(\overline{x})^{q^i}$.

4 The KS Attack and Minors Modeling

The property of low min-Q-rank is a weakness of many BigField schemes and has been exploited in many attacks, see [11–15]. While the attack in [12] exploits the low min-Q-rank property to speed up a direct algebraic attack, the other cryptanalyses use the Kipnis-Shamir (KS) attack of [11] with either the original KS modeling or with the minors modeling approach pioneered in [13].

The KS-attack recovers a related private key for a low min-Q-rank system with codomain isomorphic to a degree n extension field $\mathbb{E}$ by exploiting the fact that a quadratic form embedded in the homogeneous quadratic component of the private key is of low rank, say r. Using polynomial interpolation, the public key can be expressed as a collection of quadratic polynomials G over $\mathbb{E}$, and it is known that there is a linear map N such that $N \circ G$ has rank r as a quadratic form over $\mathbb{E}$; thus, there exists a rank r matrix that is an $\mathbb{E}$-linear combination of the Frobenius powers of G. This turns the task of recovering the transformation N into solving a MinRank problem over $\mathbb{E}$.

Definition 4 (**MinRank Problem(n,r,k)**)*: Given k $n \times n$ matrices $\mathbf{M}_1, \ldots, \mathbf{M}_k \in \mathcal{M}_{n \times n}(\mathbb{E})$, find an $\mathbb{E}$-linear combination $\mathbf{M} = \sum_{i=1}^{k} \alpha_i \cdot \mathbf{M}_i$ satisfying*

$$\textit{Rank}(\mathbf{M}) \leq r.$$

The key recovery attack of [13] revises the KS approach by modeling the low min-Q-rank property differently. The authors show that an $\mathbb{E}$-linear combination of the *public* polynomials has low rank as a quadratic form over $\mathbb{E}$. Setting the unknown coefficients in $\mathbb{E}$ of each of the public polynomials as variables, the polynomials representing $(r+1) \times (r+1)$ minors of such a linear combination, which must be zero due to the rank property, reside in $\mathbb{F}_q[t_{0,0}, \ldots, t_{0,m-1}]$. Thus a Gröbner basis needs to be computed over $\mathbb{F}_q$ and the variety computed over $\mathbb{E}$. This technique is called minors modeling and dramatically improves the efficiency of the KS-attack. The complexity of the KS-attack with minors modeling is asymptotically $\mathcal{O}(n^{(\lceil log_q(D) \rceil + 1)\omega})$, where $2 < \omega \leq 3$ is the linear algebra constant.

One should note that the situation is more complicated when multiple variable

types are utilized in a scheme. In the case that there are more variables than the degree of $\mathbb{E}$ over $\mathbb{F}_q$, the dimensions of the matrices do not match the degree of the extension. Still, if there is a central map with low min-Q-rank with a small subspace of the plaintext space as its domain, as it is the case of SRP, it may remain possible to recover a low rank map. Specifically, using fewer variables does not increase the rank of a quadratic form.

5 Key Recovery for SRP

In this section we explain our key recovery attack on SRP in detail. For the purpose of simplicity of exposition, we restrict to the homogeneous quadratic case. The method extends to the general case trivially.

We note that a public key of SRP is isomorphic to an analogous scheme without the embedding as long as $\pi_d \circ \mathcal{U}$ is full rank, which occurs with high probability. In this case, let $\pi'_d : \mathbb{F}_q^n \to \mathbb{F}_q^d$ be the projection onto the first d coordinates and find a projection $\rho : \mathbb{F}_q^{n+l} \to \mathbb{F}_q^n$ such that $\mathcal{U}' = \rho \circ \mathcal{U}$ has full rank and $\pi'_d \circ \mathcal{U}' = \pi_d \circ \mathcal{U}$. Let $\mathcal{F}^* : \mathbb{E} \to \mathbb{E}$ represent the squaring map so that $\mathcal{F}_S = \phi^{-1} \circ \mathcal{F}^* \circ \phi \circ \pi_d$. Then given the central maps $\mathcal{F}'_R = \mathcal{F}_R \circ \mathcal{U} \circ \mathcal{U}'^{-1}$ and $\mathcal{F}'_P = \mathcal{F}_P \circ \mathcal{U} \circ \mathcal{U}'^{-1}$, which are of Rainbow shape and of random shape respectively, one easily checks that

$$\mathcal{T} \circ \begin{bmatrix} \mathcal{F}^* \circ \pi_d \\ \mathcal{F}_R \\ \mathcal{F}_P \end{bmatrix} \circ \mathcal{U} = \mathcal{T} \circ \begin{bmatrix} \mathcal{F}^* \circ \pi'_d \\ \mathcal{F}'_R \\ \mathcal{F}'_P \end{bmatrix} \circ \mathcal{U}'.$$

It therefore suffices to consider the scheme with $l = 0$; however, for specificity, we analyze the embedding explicitly in the following discussion.

The attack is broken down into two main steps. The first is finding a related Square component private key. Then we discuss how to systematically solve for the Rainbow and Plus polynomials to complete key recovery.

5.1 The min-Q-Rank of SRP

While it is true that the min-Q-rank of the public key of an instance of SRP over a degree n extension is expected to be high, the public key retains the property that there exists a linear combination of the public forms which is of low Q-rank over the degree d extension used by the Square component. We verify this claim.

Let α be a primitive element of the degree d extension $\mathbb{E}$ of $\mathbb{F}_q$. Fix a vector space isomorphism $\phi : \mathbb{F}_q^d \to \mathbb{E}$ defined by $\phi(\overline{x}) = \sum_{i=0}^{d-1} x_i \alpha^i$. Furthermore, fix a one dimensional representation $\Phi : \mathbb{E} \to \mathbb{A}$ defined by $a \overset{\Phi}{\mapsto} (a, a^q, \ldots, a^{q^{d-1}})$.

Define $\mathcal{M}_d : \mathbb{F}_q^d \to \mathbb{A}$ by $\mathcal{M}_d = \Phi \circ \phi$. We can explicitly represent this map

with the matrix

$$\mathbf{M}_d = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \alpha^q & \cdots & \alpha^{q^{d-1}} \\ \alpha^2 & \alpha^{2q} & \cdots & \alpha^{2q^{d-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{d-1} & \alpha^{(d-1)q} & \cdots & \alpha^{(d-1)q^{d-1}} \end{bmatrix} \in \mathcal{M}_{d\times d}(\mathbb{E}),$$

acting via right multiplication (so that we may use algebraists' left-to-right composition). Thus we can pass between the two interesting representations of elements in $\mathbb{E}$ of the form $(x_0, \ldots, x_{d-1}) \in \mathbb{F}_q^d$ and $(X, X^q, \ldots, X^{q^{d-1}}) \in \mathbb{A}$ simply by right multiplication by $\mathbf{M}_d$ or $\mathbf{M}_d^{-1}$.

The above map $\mathbf{M}_d$ provides another way of expressing an SRP public key. Note first that any homogeneous $\mathbb{F}_q$-quadratic map from $\mathbb{E}$ to $\mathbb{E}$ induces a quadratic form on $\mathbb{A}$ that can be represented as a $d \times d$ matrix with coefficients in $\mathbb{E}$. Since the maps $\mathcal{F}_R$ and $\mathcal{F}_P$ can be written as vectors of quadratic forms over $\mathbb{F}_q[x_1, \ldots, x_n]$ in matrix form, the entire public key can be expressed as a matrix equation.

To achieve this matrix representation of the public key, we need some additional notation. We blockwise define

$$\widetilde{\mathbf{M}}_d = \begin{bmatrix} \mathbf{M}_d & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{o+r+s} \end{bmatrix} \in \mathcal{M}_{m\times m}(\mathbb{E})$$

and

$$\widehat{\mathbf{M}}_d = \begin{bmatrix} \mathbf{M}_d \\ \mathbf{0}_{o\times d} \end{bmatrix} \in \mathcal{M}_{n'\times d}(\mathbb{E}).$$

Note that $\widetilde{\mathbf{M}}_d = \Phi \oplus id_{o+r+s}$ and $\widehat{\mathbf{M}}_d = \Phi \circ \pi_d$. Furthermore, let $\mathbf{F}^{*i}$ be the matrix representation of the quadratic form over $\mathbb{A}$ corresponding to the map $x \mapsto x^{2q^i}$.

Let $(\mathbf{F}_{S,0}, \ldots, \mathbf{F}_{S,d-1}, \mathbf{F}_{R,0}, \ldots, \mathbf{F}_{R,o+r-1}, \mathbf{F}_{P,0}, \ldots, \mathbf{F}_{P,s-1})$ denote the m-dimensional vector of $(d+o)\times(d+o)$ symmetric matrices associated to the private key. The function corresponding to the application of each coordinate of a vector of such quadratic forms followed by the application of a linear map represented by a matrix will be denoted by the right product of the vector by the matrix. Next, note that

$$(\mathbf{F}_{S,0}, \mathbf{F}_{S,1}, \ldots, \mathbf{F}_{S,d-1})\mathbf{M}_d = (\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top, \widehat{\mathbf{M}}_d\mathbf{F}^{*1}\widehat{\mathbf{M}}_d^\top, \ldots, \widehat{\mathbf{M}}_d\mathbf{F}^{*d-1}\widehat{\mathbf{M}}_d^\top),$$

which yields

$$\begin{aligned}(\overline{x}\mathbf{F}_{S,0}\overline{x}^\top, &\overline{x}\mathbf{F}_{S,1}\overline{x}^\top, \ldots, \overline{x}\mathbf{F}_{S,d-1}\overline{x}^\top)\mathbf{M}_d \\ &= (\overline{x}\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top\overline{x}^\top, \overline{x}\widehat{\mathbf{M}}_d\mathbf{F}^{*1}\widehat{\mathbf{M}}_d^\top\overline{x}^\top, \ldots, \overline{x}\widehat{\mathbf{M}}_d\mathbf{F}^{*d-1}\widehat{\mathbf{M}}_d^\top\overline{x}^\top),\end{aligned}$$

as functions of $\overline{x}$. Then we obtain the equation

$$\begin{aligned}&(\mathbf{F}_{S,0},\ldots,\mathbf{F}_{S,d-1},\mathbf{F}_{R,0},\ldots,\mathbf{F}_{P,m-1})\widetilde{\mathbf{M}}_d\\&=(\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top,\ldots,\widehat{\mathbf{M}}_d\mathbf{F}^{*d-1}\widehat{\mathbf{M}}_d^\top,\mathbf{F}_{R,0},\ldots,\mathbf{F}_{P,s-1}).\end{aligned}\tag{1}$$

Next, consider the relation between the public key and the central maps of the private key.

$$(\mathbf{P}_0,\ldots,\mathbf{P}_{m-1})\mathbf{T}^{-1}=(\mathbf{U}\mathbf{F}_{S,0}\mathbf{U}^\top,\ldots,\mathbf{U}\mathbf{F}_{P,s-1}\mathbf{U}^\top).$$

By Equation (1), we have

$$\begin{aligned}&(\mathbf{P}_0,\ldots,\mathbf{P}_{m-1})\mathbf{T}^{-1}\widetilde{\mathbf{M}}_d\\&=(\mathbf{U}\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top\mathbf{U}^\top,\ldots,\mathbf{U}\widehat{\mathbf{M}}_d\mathbf{F}^{*d-1}\widehat{\mathbf{M}}_d^\top\mathbf{U}^\top,\mathbf{U}\mathbf{F}_{R,0}\mathbf{U}^\top,\ldots,\mathbf{U}\mathbf{F}_{P,s-1}\mathbf{U}^\top).\end{aligned}$$

Let $\widehat{\mathbf{T}}=\mathbf{T}^{-1}\widetilde{\mathbf{M}}_d=[t_{i,j}]\in\mathcal{M}_{m\times m}(\mathbb{E})$ and let $\mathbf{W}=\mathbf{U}\widehat{\mathbf{M}}_d$. Then we have that

$$\sum_{i=0}^{m-1}t_{i,0}\mathbf{P}_i=\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^\top.\tag{2}$$

Since the rank of $\mathbf{F}^{*i}$ is one for all i, the rank of this $\mathbb{E}$-linear combination of the public matrices is bounded by one. Indeed, if the rank were zero, then $\mathbf{W}=\mathbf{0}$, and the scheme reduces to a weak version of Rainbow+ whose kernel is the vinegar subspace. In particular, for all practical parameters one sets $d>l$, implying $d+o-l>o$, which verifies that $\mathbf{W}\neq\mathbf{0}$ (due to the fact that $\mathbf{U}$ is required to be full rank). Thus we obtain the following:

Theorem 1 *The min-Q-rank of the public key P of SRP(q,d,o,r,s,l) is, with high probability, given by:*

$$\textit{min-Q-rank}(P)=\begin{cases}0\ \textit{if}\ d\leq l\ \textit{and}\ \mathbf{U}\widehat{\mathbf{M}}_d=\mathbf{0},\\1\ \textit{otherwise.}\end{cases}$$

Proof. If $\mathbf{U}\widehat{\mathbf{M}}_d=\mathbf{0}$, then the span of P is of dimension at most $m-d$, and thus the min-Q-rank of P is zero. Otherwise, with high probability, the public polynomials are linearly independent. In this case, for any choice of L_1, there exists an L_2 such that the Q-rank of the composition $L_1\circ P\circ L_2$ is positive.

Consider, in particular, L_1 to be the $\mathbb{F}_q$-linear transformation defined by the matrix consisting of the first d columns of $\mathbf{T}^{-1}$. Let $L_2:\mathbb{F}_q^d\to\mathbb{F}_q^n$ be linear of full rank. Then

$$\phi\circ L_1\circ\mathcal{P}\circ L_2\circ\phi^{-1}=\mathcal{F}^*\circ\phi\circ\pi_d\circ\mathcal{U}\circ L_2\circ\phi^{-1}.$$

Let $\mathbf{L}_2$ be the $d\times n$ matrix representation of L_2. Then the matrix representation of the above quantity is

$$\mathbf{M}_d^{-1}\mathbf{L}_2\mathbf{U}\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top\mathbf{U}^\top\mathbf{L}_2^\top\mathbf{M}_d^\top.$$

Since $\mathbf{F}^{*0}$ is of rank one and the image of $\widehat{\mathbf{M}}_d$ is $\mathbb{A}$, the product is of rank one exactly when $\mathbf{L}_2\mathbf{U}\widehat{\mathbf{M}}_d$ is nonzero, otherwise, the rank of the above matrix is zero. Since L_2 is chosen to maximize rank, the Q-rank is zero exactly when $\mathbf{U}\widehat{\mathbf{M}}_d$ is zero, which necessitates that $d \leq l$.

One may note here that the matrix $\widehat{\mathbf{T}}$ unmixes the Square equations from the Rainbow and Plus polynomials. It further mixes the Rainbow and Plus polynomials, but this is no issue since this phase of the attack is aimed at ultimately recovering a representation of $\mathcal{F}^*$.

5.2 Recovering the Output Transformation with MinRank

As demonstrated in the previous subsection, the recovery of $\widehat{\mathbf{T}}$ begins by solving a MinRank instance over $\mathbb{E}$. This phenomenon is well studied and has been the basis of previous cryptanalyses, see [13–15]. We may use the minors modeling approach to take advantage of the fact that we can compute the Gröbner basis over the small field, $\mathbb{F}_q$.

Due to the extremely low min-Q-rank of the system, the system of minors is homogeneous quadratic. The ideal generated by these minors is one dimensional, so we may set a single variable to a fixed value, say 1. We then recover a system of many quadratic equations in $m-1$ variables. This system is massively overdefined, so a solution can be recovered via linearization.

To accomplish this, we have to compute only as many minors as there are monomials in $m-1$ variables of total degree ≤ 2. There are exactly $\binom{m+1}{2}$ monomials in $m-1$ variables of degree less than or equal to two, so we randomly select $\binom{m+1}{2}$ minors and arrange their coefficients in a $\binom{m+1}{2} \times \binom{m+1}{2}$ matrix. As we will show in Section 6, we expect such a matrix to have full rank with high probability, roughly $\frac{q-1}{q}$ for large n and m. We may then linearly solve, recovering the first column of $\widehat{\mathbf{T}}$.

Once the first column of $\widehat{\mathbf{T}}$ is recovered, the first d columns can be generated by the relation

$$t_{i,j} = t_{i,j-1}^q \text{ for } j = 1, \ldots, d-1.$$

We will return to the issue of computing the remaining columns of $\widehat{\mathbf{T}}$ and separating the Rainbow and Plus polynomials in Subsection 5.5.

5.3 Recovering the Input Transformation

Once the first column of the transformation $\widehat{\mathbf{T}} = [t_{i,j}]$ is discovered, we have access to the rank one matrix

$$\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i.$$

This matrix encodes the representation of the squaring map.

Theorem 2 *Given the first column of* $\widehat{\mathbf{T}}$*, the recovery of* $\mathbf{W}$ *requires the solution of a linear system of* $d+o-l-1$ *independent equations in* $d+o-l$ *variables.*

Proof. First, note that $\mathbf{W} = [w_{i,j}]$ is of the form $w_{i,j} = w_{i,j-k}^{q^k}$ for all $i \in \{0, 1, \ldots, d+o-l\}$ and for all $0 \leq j, k < d$. Thus, it suffices to solve for the first column of $\mathbf{W}$. Let K be the left kernel of the low rank matrix

$$\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i.$$

Let $\mathbf{K}$ be the matrix whose rows form a basis of K. By Equation (2), we know that

$$\mathbf{0}_{d+o-l-1\times d+o-l} = \mathbf{K}\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^{\top},$$

and since $\mathbf{W}$ is of full rank, it must be the case that

$$\mathbf{K}\mathbf{W}\mathbf{F}^{*0} = \mathbf{0}_{d+o-l-1\times d}.$$

Thus $K\mathbf{W} = ker(\mathbf{F}^{*0})$. In a proper basis the representation of $\mathbf{F}^{*0}$ contains a single nonzero entry in the first row and first column. Thus, the relation that $K\mathbf{W} = ker(\mathbf{F}^{*0})$ is equivalent to the condition that the first column of $\mathbf{W}$ is in the right kernel of $\mathbf{K}$. Since this right kernel is one dimensional, this process recovers all equivalent matrices $\mathbf{W}$.

Recall that we have the relation

$$\mathbf{W} = \mathbf{U}\widehat{\mathbf{M}}_d = \mathbf{U}\begin{bmatrix}\mathbf{M}_d \\ \mathbf{0}_{o\times d}\end{bmatrix}.$$

Then multiplying on the right by $\mathbf{M}_d^{-1}$ yields

$$\mathbf{W}\mathbf{M}_d^{-1} = \mathbf{U}\begin{bmatrix}\mathbf{M}_d \\ \mathbf{0}_{o\times d}\end{bmatrix}\mathbf{M}_d^{-1} = \mathbf{U}\begin{bmatrix}\mathbf{I}_d \\ \mathbf{0}_{o\times d}\end{bmatrix}. \tag{3}$$

Thus, we obtain the first d columns of $\mathbf{U}$. We may extend this matrix in any manner to obtain a full rank $n\times(d+o)$ matrix. With high probability, a random concatenation of o columns produces a full rank matrix $\mathbf{U}$. For the sake of recovering $\mathcal{F}_S$, we insist that the first n columns of $\mathbf{U}$ form an invertible matrix.

5.4 Recovering the Square Map

We now assume that we have recovered the first column, $[t_{i,0}]$, of $\widehat{\mathbf{T}}$ and that we have recovered $\mathbf{U}$. Let $\widehat{\mathbf{U}}$ represent the matrix consisting of the first $d+o-l$ columns of $\mathbf{U}$. By construction, $\widehat{\mathbf{U}}$ is invertible. We set $\mathbf{U} = \begin{bmatrix}\widehat{\mathbf{U}} & \widehat{\mathbf{U}}'\end{bmatrix}$.

We can now explicitly compute

$$\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i = \mathbf{W}\mathbf{F}^{*0}\mathbf{W}^{\top}.$$

Note that

$$\mathbf{W} = \mathbf{U}\widehat{\mathbf{M}}_d = \begin{bmatrix}\widehat{\mathbf{U}} & \widehat{\mathbf{U}}'\end{bmatrix} \begin{bmatrix}\mathbf{M}_d \\ \mathbf{0}_{o\times d}\end{bmatrix} = \widehat{\mathbf{U}} \begin{bmatrix}\mathbf{M}_d \\ \mathbf{0}_{(o-l)\times d}\end{bmatrix}.$$

Thus we have

$$\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i = \widehat{\mathbf{U}} \begin{bmatrix}\mathbf{M}_d \\ \mathbf{0}_{(o-l)\times d}\end{bmatrix} \mathbf{F}^{*0} \begin{bmatrix}\mathbf{M}_d^\top & \mathbf{0}_{d\times(o-l)}\end{bmatrix} \widehat{\mathbf{U}}^\top.$$

Therefore, we may compute

$$\begin{bmatrix}\mathbf{M}_d \\ \mathbf{0}_{(o-l)\times d}\end{bmatrix} \mathbf{F}^{*0} \begin{bmatrix}\mathbf{M}_d^\top & \mathbf{0}_{d\times(o-l)}\end{bmatrix} = \widehat{\mathbf{U}}^{-1} \left(\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i\right) \widehat{\mathbf{U}}^{-\top}, \tag{4}$$

Now, by taking the top left $d \times d$ submatrix, we recover $\mathbf{M}_d\mathbf{F}^{*0}\mathbf{M}_d^\top$. Finally, by multiplying on the left by $\mathbf{M}_d^{-1}$ and on the right by $\mathbf{M}_d^{-\top}$, we recover $\mathbf{F}^{*0}$.

5.5 Unmixing the Rainbow and Plus Polynomials

Having identified the vinegar subspace of linear forms on the input variables, we can identify the Rainbow polynomials as those linear combinations of the public polynomials which become linear when their inputs are restricted to the kernel of those linear forms. In other words, we can find the Rainbow polynomials by linearly solving for t_i such that:

$$\begin{bmatrix}\mathbf{0}_{(o-l)\times d}\mathbf{I}_{o-l}\end{bmatrix} \widehat{\mathbf{U}}^{-1} \left(\sum_{i=0}^{m-1} t_i\mathbf{P}_i\right) \widehat{\mathbf{U}}^{-\top} \begin{bmatrix}\mathbf{0}_{d\times(o-l)} \\ \mathbf{I}_{o-l}\end{bmatrix} = 0. \tag{5}$$

A basis $t_{i,j}$ of the solution space of this equation forms the columns $d{+}1$ through $d{+}o{+}r$ of $\mathbf{T}^{-1}$. We can place any selection of column vectors in the last s columns of $\mathbf{T}^{-1}$ making it full rank, since no party is concerned with the values of the plus polynomials.

Having recovered the complete transformation $\mathbf{T}^{-1}$, we can compute the Rainbow and Plus part of the central map by

$$\begin{aligned}&(\mathbf{F}_{s,0}, \ldots, \mathbf{F}_{S,d-1}, \mathbf{F}_{R,0}, \ldots, \mathbf{F}_{R,o+r-1}, \mathbf{F}_{P,0}, \ldots, \mathbf{F}_{P,s-1}) \\ &= (\widehat{\mathbf{U}}^{-1}\mathbf{P}_0\widehat{\mathbf{U}}^{-\top}, \ldots, \widehat{\mathbf{U}}^{-1}\mathbf{P}_m\widehat{\mathbf{U}}^{-\top})\mathbf{T}^{-1}.\end{aligned} \tag{6}$$

Algorithm 1 shows the process of our attack in algorithmic form. In the appendix of this paper, we illustrate our attack using a toy example.

Algorithm 1 Our Key Recovery Attack on SRP

Input: SRP parameters (o, d, r, s, l), SRP public key $\mathcal{P} : \mathbb{F}^{n'} \to \mathbb{F}^m$
Output: equivalent private key $(\mathcal{T}, (\mathcal{F}_S, \mathcal{F}_R, \mathcal{F}_P), \mathcal{U})$

1: Solve a MinRank problem on the m public polynomials with target rank 1. Denote the solution by $v \in \mathbb{E}^m$.
2: Define the elements of the $m \times d$ matrix $\hat{\mathbf{T}}'$ by $\hat{t_{ij}}' = v_i^{q^{j-1}}$ $(j = 1, \ldots, d)$.
3: Compute the first d columns of the matrix $\mathbf{T}^{-1}$ by $\mathbf{T}'^{-1} = \hat{\mathbf{T}} \cdot \mathbf{M}_d^{-1}$.
4: Let $\mathbf{K}$ be the $(n-1) \times n$ matrix representing the left kernel of the low rank matrix $\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i$ and choose an element $w \in \mathbb{F}^n$ of its right kernel.
5: Define the elements of the $n \times d$ matrix $\mathbf{W}$ by $w_{ij} = w_i^{q^{j-1}}$ $(j = 1, \ldots, d)$
6: Recover the first d columns of the matrix $\mathbf{U}$ by equation (3).
7: Extend $\mathbf{U}$ to an invertible $n \times n$ matrix $\widehat{\mathbf{U}}$ and $\widehat{\mathbf{U}}$ to a full rank $n \times (d+o)$ matrix $\mathbf{U}$.
8: Recover the map $\mathcal{F}_S$ by equation (4).
9: Compute the columns $d+1, \ldots, d+o+r$ of the matrix $\mathbf{T}^{-1}$ by solving the linear system of equation (5). Append randomly columns to get an invertible $m \times m$ matrix $\mathbf{T}^{-1}$.
10: Recover the matrices representing the Rainbow and plus polynomials by equation (6).

6 Complexity of Attack

To estimate the complexity of our attack, we compute the Hilbert series of the ideal generated by the 2×2 minors of

$$\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i.$$

We can then recover the degree of regularity d_{reg} explicitly.

Theorem 3 *Let $\mathbb{E}[T] = \mathbb{E}[t_{0,0}, \ldots, t_{m-1,0}]$. Let I be the ideal generated by the system of minors arising from the minors modeling variant of the KS-attack on SRP(q, d, o, r, s, l) with $d > l$, $n = d + o - l$ and $m = d + o + r + s$. Then the Hilbert series of I (that is, the Hilbert Series of $\mathbb{E}[T]/I$) is*

$$\text{Hilbertseries}(t) = 1 + mt.$$

Consequently the degree of regularity of the minors system is $d_{reg} = 2$.

Proof. Consider the ideal I generated by the 2×2 minors over $\mathbb{E}[T]$. There are $\binom{n}{2}^2/2$ distinct 2×2 minors in an $n \times n$ symmetric matrix; however, each such minor of the above matrix is a homogeneous quadratic polynomial in m variables. Thus the dimension of the span of the 2×2 minors is $\binom{m}{2} + m = \binom{m+1}{2}$. As a consequence, $\binom{m+1}{2}$ randomly chosen minors should be linearly independent with probability approximately $1 - \frac{1}{q}$.
Since I contains all linear combinations of the minors, I contains all quadratic

monomials in $\mathbb{E}[T]$. Thus $\mathbb{E}[T]/I$ contains representatives of exactly all equivalence classes of degree less than two. Therefore, the Hilbert Series of $\mathbb{E}[T]/I$ is

$$HS(t) = 1 + mt.$$

Technically, the ideal I in Theorem 3 is not what we use in the attack. We use $I' = \langle I, t_{0,0} - 1 \rangle$, for example. However, adding polynomials to I cannot increase the degree of regularity; thus, the degree of regularity in the actual attack is still two.

This fact proves that we actually require no Gröbner basis algorithm for the attack. Simple linearization and Gaussian elimination are effective in breaking all parameters.

Specifically, recalling that with one variable fixed we have only $m - 1$ variables, we may use the above calculation to estimate the complexity of recovering the first column of $\widehat{\mathbf{T}}$ using the minors modeling variant of the KS-attack.

Unmixing the Rainbow and plus polynomials only requires $2m$ matrix multiplications of dimension n matrices and solving a linear system in m variables. The complexity of these operations is on the order of $m^{\omega+1}$, and is therefore dominated by the minors modeling step. Thus we obtain the following

Theorem 4 *The complexity of our key recovery attack on SRP(q, d, o, r, s, l) with $d > l$, $n = d+o-l$ and $m = d+o+r+s$ using the minors modeling variant of the KS-attack is*

$$\mathcal{O}\left(\binom{m+1}{2}^{\omega}\right),$$

where $2 < \omega \leq 3$ is the linear algebra constant.

7 Experimental Results

In order to estimate the complexity of our attack in practice, we created a straightforward implementation of the key generation process of SRP and our attack in MAGMA Code. The experiments run on a server with 16 AMD Opteron processors(2.4 GHz) and 128 GB of RAM. However, for our experiments, we used only a single core.

Table 1 shows, for different parameter sets, the results of our experiments. The numbers in rows 3 and 10 show the time needed to solve the MinRank problem and to recover the maps $\mathcal{F}_S$ and $\mathcal{U}$ as well as the first d columns of the matrix $\mathbf{T}^{-1}$. The numbers in row 4 and 11 show the time needed to recover the remaining columns of $\mathbf{T}^{-1}$ and the maps $\mathcal{F}_R$ and $\mathcal{F}_P$. The numbers in the fifth and twelfth row show the overall running time of our attack.

parameters (q,d,o,r,s,l)	(31,16,16,8,3,8)	(31,24,24,12,4,12)	(31,35,35,15,5,15)
(m, n)	(43,24)	(64,36)	(90,55)
time for recovering $\mathcal{F}_S$ (s)	10.0	74.5	1,295
time for recovering $\mathcal{F}_R$ and $\mathcal{F}_P$ (s)	0.5	2.5	16.5
time (overall) (s)	10.5	77.1	1,313
memory (MB)	354.6	1,970.3	11,867
claimed security level (bit)	80	112	160
parameters(q,d,o,r,s,l)	(31,33,32,16,5,16)	(31,47,47,22,5,22)	(31,71,71,32,5,32)
(m, n)	(86,49)	(121,72)	(179,110)
time for recovering $\mathcal{F}_S$ (s)	487.0	9,705	
time for recovering $\mathcal{F}_P$ and $\mathcal{F}_R$	10.0	69.1	
time (overall)	497.0	9,777	100,000[1]
memory (MB)	8,518.5	47,988	300,000[1]

Table 1. Running time of the proposed attack

[1)] conjectured values

As the second column of the table shows, doubling the parameters leads to an increase of the running time and memory requirements of our attack by factors of about 50 and 25, which corresponds to our theoretical estimations.[4]

The parameter sets shown in the bottom half of Table 1 are those proposed by the authors of [7] for security levels of 80, 112 and 160 bit respectively. As the table shows, we can (even with our limited resources and poorly optimized attack) break the parameter sets proposed for 80 and 112 bit security in very short time. For the parameters proposed for 160 bit of security, we estimate a running time of our attack of about one day with 300 GB of memory required. While breaking this instance lies beyond our possibilities, it is completely practical for organizations with better equipment.

8 Conclusion

In this paper we propose a practical attack against the SRP encryption scheme of Yasuda and Sakurai [7]. Our attack uses the min-Q-rank property of the scheme to recover parts of the linear transformation $\mathcal{T}$, the transformation $\mathcal{U}$ and the Square part $\mathcal{F}_S$ of the central map. Following this, we use the known structure of the Rainbow polynomials to recover the second half of the map $\mathcal{T}$ as well as the Rainbow and Plus part of the central map. Our attack is very efficient and breaks the SRP instances proposed in [7] for 80 and 112 bit security in very short time.

Therefore, our attack shows that the security of a weak multivariate scheme

[4] For larger parameters, the memory access time plays a major role in the overall running time. Therefore the corresponding factors are much larger.

like Square is not automatically increased by combining it with another (secure) scheme.

Acknowledgements

We thank the anonymous reviewers for their comments which helped to improve the paper.

References

1. Bernstein, D.J., Buchmann, J., Dahmen, E., eds.: Post-quantum cryptography. Springer (2009).
2. Chen, A.I.T., Chen, M.S., Chen, T.R., Cheng, C.M., Ding, J., Kuo, E.L.H., Lee, F.Y.S., Yang, B.Y.: SSE implementation of Multivariate PKCs on modern x86 CPUs. CHES 2009, LNCS vol. 5747, pp. 33 -48. Springer (2009).
3. Bogdanov, A., Eisenbarth, T., Rupp, A., Wolf, C.: Time-Area optimized public-key engines: MQ-Cryptosystems as replacement for elliptic curves? CHES 2008, LNCS vol. 5154, pp. 45 -61. Springer (2008).
4. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206 - 222. Springer (1999).
5. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. ACNS 2005, LNCS vol. 3531, pp. 164 - 175. Springer (2005).
6. Petzoldt, A., Chen, M.S., Yang, B.Y., Tao, C., Ding, J.: Design principles for HFEv- based multivariate signature schemes. ASIACRYPT 2015 (Part 1), LNCS vol. 9742 , pp. 311 -334. Springer (2015).
7. Yasuda, T., Sakurai, K.: A multivariate encryption scheme with Rainbow. ICISC 2015, LNCS vol. 9543, pp. 222 - 236. Springer (2015).
8. Clough, C., Baena, J., Ding, J., Yang, B.Y., Chen, M.S.: Square, a new multivariate encryption scheme. CT-RSA 2009, LNCS vol. 5473, pp. 252 - 264. Springer (2009) .
9. Ding, J., Gower, J.E., Schmidt, D.S.: Multivariate public key cryptosystems. Advances in Information Security vol. 25. Springer (2006).
10. Garey, M.R., Johnson, D.S.: Computers and intractability: A guide to the theory of NP-completeness. A Series of Books in the Mathematical Sciences, W. H. Freeman and Company (1979).
11. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by Relinearization. CRYPTO 1999, LNCS vol. 1666, pp. 19 - 30. Springer (1999).
12. Faugére, J.C.: Algebraic cryptanalysis of Hidden Field Equations (HFE) using Gröbner bases. CRYPTO 2003, LNCS vol. 2729, pp. 44 - 60. Springer (2003).
13. Bettale, L., Faugére, J., Perret, L.: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Designs Codes and Cryptography 69 (2013), pp. 1 - 52.
14. Cabarcas, D., Smith-Tone, D., Verbel, J.A.: Key recovery attack for ZHFE. PQCrypto 2017, LNCS vo. 10346, pp. 289 - 308. Springer (2017).
15. Vates, J., Smith-Tone, D.: Key recovery for all parameters of HFE-. PQCrypto 2017, LNCS 10346, pp. 272 -288. Springer (2017).

A Toy Example

In the following we illustrate our attack using a toy example with small parameters.

A.1 Key Generation

For our toy example we use GF(7) as the underlying field. We choose the parameters of SRP as $(d, o, r, s, l) = (2, 2, 1, 1, 1)$.[5] Therefore our public key consists of six equations in three variables. The Square map is defined over the extension field GF(7)[X] / $\langle X^2 + 6X + 3 \rangle$. For simplicity, we restrict to linear maps $\mathcal{T}$ and $\mathcal{U}$ as well as homogeneous quadratic maps $\mathcal{F}_R$ and $\mathcal{F}_P$. By doing so, the public key $\mathcal{P}$ of our scheme will be homogeneous quadratic, too.

Let the linear maps $\mathcal{T}$ and $\mathcal{U}$ be given by the matrices

$$\mathbf{T} = \begin{pmatrix} 1\,5\,1\,6\,3\,3 \\ 5\,3\,5\,2\,2\,5 \\ 0\,4\,0\,4\,5\,0 \\ 0\,6\,6\,2\,4\,3 \\ 3\,3\,6\,3\,6\,3 \\ 5\,3\,5\,0\,4\,6 \end{pmatrix} \in \mathbb{F}^{6\times 6} \quad \text{and} \quad \mathbf{U} = \begin{pmatrix} 6\,0\,3\,2 \\ 2\,0\,0\,4 \\ 4\,1\,1\,0 \end{pmatrix} \in \mathbb{F}^{3\times 4}.$$

The Square map $\mathcal{F}_S(X) = X^2$ is given by the matrix $\mathbf{F} = \begin{pmatrix} 1\,0 \\ 0\,0 \end{pmatrix} \in \mathbb{F}^{2\times 2}$. Let the three Rainbow polynomials be given by the 4×4 matrices

$$\mathbf{F}_{R,0} = \begin{pmatrix} 2\,6\,2\,3 \\ 6\,1\,6\,0 \\ 2\,6\,0\,0 \\ 3\,0\,0\,0 \end{pmatrix}, \; \mathbf{F}_{R,1} = \begin{pmatrix} 2\,1\,5\,1 \\ 1\,5\,0\,6 \\ 5\,0\,0\,0 \\ 1\,6\,0\,0 \end{pmatrix}, \text{ and } \mathbf{F}_{R,2} = \begin{pmatrix} 5\,4\,3\,0 \\ 4\,2\,0\,1 \\ 3\,0\,0\,0 \\ 0\,1\,0\,0 \end{pmatrix}.$$

The Plus polynomial is given by the 4×4 matrix

$$\mathbf{F}_{P_0} = \begin{pmatrix} 3\,4\,3\,2 \\ 4\,4\,0\,3 \\ 3\,0\,5\,0 \\ 2\,3\,0\,3 \end{pmatrix}.$$

We compute the public key of our scheme by $\mathcal{P} = \mathcal{T} \circ (\mathcal{F}_S, \mathcal{F}_R, \mathcal{F}_P) \circ \mathcal{U}$ and obtain the following 6 3×3 matrices representing $\mathcal{P}$

[5] Note that this parameter choice does not meet the description in Section 2.2, where d was required to be odd. However, an odd value of d is only needed for the efficient decryption. The scheme itself can be defined for any value of d.

$$\mathbf{P}_0 = \begin{pmatrix} 6\,6\,0 \\ 6\,6\,0 \\ 0\,0\,1 \end{pmatrix},\ \mathbf{P}_1 = \begin{pmatrix} 5\,2\,5 \\ 2\,3\,4 \\ 5\,4\,6 \end{pmatrix},\ \mathbf{P}_2 = \begin{pmatrix} 6\,4\,2 \\ 4\,0\,1 \\ 2\,1\,1 \end{pmatrix}$$
$$\mathbf{P}_3 = \begin{pmatrix} 4\,5\,3 \\ 5\,6\,3 \\ 3\,3\,3 \end{pmatrix},\ \mathbf{P}_4 = \begin{pmatrix} 5\,1\,5 \\ 1\,1\,4 \\ 5\,4\,3 \end{pmatrix},\ \text{and } \mathbf{P}_5 = \begin{pmatrix} 2\,4\,6 \\ 4\,3\,1 \\ 6\,1\,3 \end{pmatrix}.$$

A.2 Recovery of Transformation of Square Polynomials

In the first step of the attack, we have to solve a MinRank problem on the 6 matrices $\mathbf{P}_0, \ldots, \mathbf{P}_5$ with target rank 1. One solution is given by

$$v = (1, b^{19}, b^{13}, b^9, b^{47}, b^9),$$

where b is a generator of the extension field $\mathbb{E}$=GF(7^2).

From this, we obtain the first part of the linear transformation $\mathcal{T}$ which divides the Square part from the remaining polynomials. Let $\widehat{\mathbf{T}}'$ represent the first d columns of $\widehat{\mathbf{T}}$. We may recover the first d columns of $\mathbf{T}^{-1}$ via right multiplication by $\mathbf{M}_d^{-1}$.

$$\widehat{\mathbf{T}}' = \begin{pmatrix} 1 & 1 \\ b^{19} & b^{37} \\ b^{13} & b^{43} \\ b^9 & b^{15} \\ b^{47} & b^{41} \\ b^9 & b^{15} \end{pmatrix},\ \mathbf{T}^{-1\prime} = \widehat{\mathbf{T}}'\mathbf{M}_d^{-1} = \begin{pmatrix} 1\,1 \\ 1\,3 \\ 3\,3 \\ 0\,3 \\ 5\,2 \\ 0\,3 \end{pmatrix}.$$

Note that the entries in the second column of $\widehat{\mathbf{T}}'$ are just the Frobenius powers of the first column entries.

A.3 Recovery of the Input Transformation $\mathcal{U}$

Next we can use the first column, $[t_{i,0}]$, of $\widehat{\mathbf{T}}'$ to recover the first d columns of the matrix representation of the linear transformation $\mathcal{U}$, thus separating the vinegar subspace from the oil subspace. To accomplish this, we construct our rank one solution to the MinRank step

$$L = \sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i = \begin{pmatrix} b^{45} & b^3 & b^{18} \\ b^3 & b^9 & 6 \\ b^{18} & 6 & b^{39} \end{pmatrix}.$$

Let K be the left kernel of L and construct the reduced row echelon form matrix $\mathbf{K}$ whose rows form a basis of K.

$$\mathbf{K} = \begin{pmatrix} 1\,0\,b^3 \\ 0\,1\,b^9 \end{pmatrix}.$$

Any element in the right kernel of $\mathbf{K}$ forms the first column of $\mathbf{W}$. The second column is the first Frobenius power of the first. For a random selection we obtain

$$\mathbf{W} = \begin{pmatrix} b^{45} & b^{27} \\ b^{3} & b^{21} \\ b^{18} & b^{30} \end{pmatrix}.$$

We next recover the first $d = 2$ columns of U via the relation

$$\mathbf{W}\mathbf{M}_d^{-1} = \mathbf{U} \begin{bmatrix} \mathbf{I}_d \\ \mathbf{0}_{o\times d} \end{bmatrix} = \begin{pmatrix} 5 & 5 \\ 4 & 5 \\ 1 & 2 \end{pmatrix}.$$

Extending this matrix, we construct the invertible

$$\widehat{\mathbf{U}} = \begin{pmatrix} 5 & 5 & 0 \\ 4 & 5 & 0 \\ 1 & 2 & 1 \end{pmatrix}.$$

We may now extend this matrix to any $n \times n + l$ matrix. The simplest way is to append zeros. This technique is always effective due to the isomorphism described at the beginning of Section 5. Thus we obtain

$$\mathbf{U} = \begin{pmatrix} 5 & 5 & 0 & 0 \\ 4 & 5 & 0 & 0 \\ 1 & 2 & 1 & 0 \end{pmatrix}.$$

A.4 Recovering $\mathcal{F}_S$

Knowing $\mathbf{T}^{-1'}$ and $\widehat{\mathbf{U}}$, we can recover the Square part of the central map. Specifically, we recover the top left 2×2 submatrix of $\widehat{\mathbf{U}}^{-1} L \widehat{\mathbf{U}}^{-\top}$:

$$\mathbf{F}^{*0} = \begin{pmatrix} b^{3} & 0 \\ 0 & 0 \end{pmatrix}.$$

A.5 Recovering $\mathcal{F}_R$ and $\mathcal{F}_P$

We solve the equation

$$\left[\mathbf{0}_{(o-l)\times d}\, \mathbf{I}_{o-l}\right] \widehat{\mathbf{U}}^{-1} \left(\sum_{i=0}^{m-1} t_i \mathbf{P}_i \right) \widehat{\mathbf{U}}^{-\top} \begin{bmatrix} \mathbf{0}_{d\times(o-l)} \\ \mathbf{I}_{o-l} \end{bmatrix}$$

for t_i and append $o + r = 3$ linearly independent solutions as column vectors onto $\mathbf{T}^{-1'}$. The final $s = 1$ column(s) of $\mathbf{T}^{-1}$can be chosen randomly to achieve full rank. Our random selection produces

$$\mathbf{T}^{-1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 5 \\ 1 & 3 & 0 & 0 & 0 & 6 \\ 3 & 3 & 2 & 6 & 4 & 3 \\ 0 & 3 & 1 & 5 & 4 & 6 \\ 5 & 2 & 2 & 0 & 2 & 1 \\ 0 & 3 & 1 & 0 & 2 & 1 \end{pmatrix}.$$

Now with $\mathbf{T}^{-1}$ we can recover explicitly the Rainbow and Plus polynomials. To do so, we compute

$$(\widehat{\mathbf{U}}^{-1}\mathbf{P}_0\widehat{\mathbf{U}}^{-\top}, \ldots, \widehat{\mathbf{U}}^{-1}\mathbf{P}_{m-1}\widehat{\mathbf{U}}^{-\top})\mathbf{T}^{-1}.$$

We may now express the Rainbow and Plus polynomials as quadratic forms in n variables by appending l rows and columns of arbitrary values, since our choice of $\mathbf{U}$ makes these entries obsolete. We obtain

$$\mathbf{F}_{R,0} = \begin{pmatrix} 0 & 5 & 2 & 0 \\ 5 & 4 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \ \mathbf{F}_{R,1} = \begin{pmatrix} 0 & 0 & 6 & 0 \\ 0 & 2 & 0 & 0 \\ 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \ \mathbf{F}_{R,2} = \begin{pmatrix} 5 & 4 & 0 & 0 \\ 4 & 4 & 5 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and

$$\mathbf{F}_{P,0} = \begin{pmatrix} 4 & 5 & 2 & 0 \\ 5 & 4 & 1 & 0 \\ 2 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Via composition, one verifies that

$$\mathcal{P} = \mathcal{T} \circ (\mathcal{F}_S, \mathcal{F}_R, \mathcal{F}_P) \circ \mathcal{U}.$$