A Secure Variant of the SRP Encryption Scheme with Shorter Private Key

Bo Lv, Zhiniang Peng and Shaohua Tang *

School of Computer Science & Engineering,
South China University of Technology, Guangzhou, China
shtang@IEEE.org, csshtang@scut.edu.cn

Abstract. The study of multivariate encryption algorithm is an important topic of multivariate public key cryptography research. However, quite few secure and practical multivariate encryption algorithms have been found up to now. The SRP encryption scheme is a multivariate encryption scheme that combines Square, Rainbow and the Plus method technique, which is of high efficiency and resistant to existing known attacks against multivariate schemes. In this paper, an improved SRP scheme with shorter private key and higher decryption efficiency is proposed. We introduce rotation relations into parts of the private key, which enables us to reduce the private key size by about 61%. And the decryption speed is 2.1 times faster than that of the original SRP. In terms of theory and experiment, we analyze the security of the improved SRP for several attacks against SRP. The results show that our modifications do not weaken the security of the original schemes.

Keywords: Multivariate Public Key Algorithm, SRP Encryption, Quantum-safe Public Key Cryptography, Shorter Private Key

1 Introduction

Multivariate public key cryptography is one of the promising candidates for quantum-safe public key cryptography. And its security depends on the difficulty of solving a set of multivariate polynomial equations over a finite field. Multivariate schemes have fast computational speed and take fewer computational resources, so it is very suitable for resource-limited environments such as wireless sensor network environment.

There exist many multivariate encryption and signature schemes such as MI[13], HFE[16], PMI+[2], ABC[22], ZHFE[19], SRP[26], UOV[12], QUARTZ[17], Rainbow[3], STS[24], RGB[20], Gui[18] and so on. However, most schemes are compromised by a variety of attacks, such as Direct attack[6][7][5], Differential attack[10] [21], Rank attack [1][9][25][8], Linearization Equation attack [15] and so on. At present, practical multivariate signature schemes mainly include UOV, Rainbow, Gui , etc., while the secure and practical multivariate encryption

* Corresponding Author: Shaohua Tang.

scheme is quite rare. Therefore, the study of multivariate encryption scheme is a key point of multivariate public key cryptography research.

In 2015, Yasuda et al. [26] proposed a multivariate encryption scheme which combines Square and Rainbow. The scheme is highly efficient and can resist all existing attacks. In 2016, Duong et al. [4] proposed a method that insert circular series into the public key matrix to reduce the size of the public key and improve the speed of encryption.

In this paper, the rotation method is applied to the private key to reduce the size of the private key by making the rotation relation appearing among the different polynomials of the central map. At the same time, this relationship benefits us in getting some better structure in the process of decryption, thus improving the speed of decryption. By using our construction it can reduce the size of the private key by about 61%. Furthermore, the special structure obtained in the process of decryption allows us to speed up the decryption process of the scheme by up to 68%. Through security analysis, our improvements will not affect the security of the original scheme.

The rest of this paper is arranged as follows. Section 2 concisely introduces scheme theory of SRP encryption scheme. Section 3 describes the construction of our improved SRP and the influence of the improved method on SRP, including the efficiency of decryption, the probability of decryption success and the size of the private key. The impact of the improved method on the original scheme is analyzed from the security aspect in Section 4. In Section 5, the improved scheme and the original scheme are compared with the key size and the performance of decryption. And Section 6 draws conclusions.

2 Preliminaries

We describe the basic theory of the encryption and decryption of SRP[26] in this section. The SRP encryption scheme combines Square and Rainbow. So the decryption of SRP is efficient.

2.1 Notations for SRP

Let $K = GF(q)$ be a finite field of odd characteristic and cardinality $q(q \equiv 3 \ mod \ 4)$, E be an extension of degree d over K, and ϕ be an isomorphism between the field E and the vector space K^d. Let $o_1, ..., o_h, r, s$ and l be non-negative integers, and $n = d + o_1 + ... + o_h - l$, $n' = d + o_1 + ... + o_h$, $m = d + o_1 + ... + o_h + hr + s$. The number of equations is m and number of variables is n.

The central map $F : K^{n'} \to K^m$ of SRP is the concatenation of three maps F_S, F_R and F_P . These maps are defined as follows.

The Square part $F_S : K^{n'} \to K^d$ is defined by:

$$F_S : K^{d+o_1+...+o_h} \xrightarrow{projection} K^d \xrightarrow{\phi^{-1}} E \xrightarrow{X \mapsto X^2} E \xrightarrow{\phi} K^d.$$

The Rainbow part $F_R : K^{n'} \to K^{d+o_1+...+o_h+hr}$ is constructed as follows. Let h be the number of layers in Rainbow. For each layer $k = 1, ..., h$, let $v_k = d + o_1 + ... + o_{k-1}$, $V_k = \{1, 2, ..., v_k\}$, $O_k = \{v_k + 1, ..., v_k + o_k\}$. The k^{th} layer consists of $o_k + r$ polynomials which are chosen by the multivariate quadratic polynomials of the form

$$f_R{}^k(x_1, ..., x_{n'}) = \sum_{i \in O_k, j \in V_k} \alpha_{ij} x_i x_j + \sum_{i,j \in V_k, i<j} \beta_{ij} x_i x_j + \sum_{i \in O_k \cup V_k} \gamma_i x_i + \eta,$$

where $\alpha_{ij}, \beta_{ij}, \gamma_i, \eta$ are randomly chosen in K.

The Plus part $F_P : K^{n'} \to K^s$ consist of randomly chosen s multivariate quadratic polynomials of the form

$$f_P(x_1, ..., x_{n'}) = \sum_{1 \le i \le j \le n'} \alpha_{ij} x_i x_j + \sum_{1 \le i \le n'} \beta_i x_i + \gamma(\alpha_{ij}, \beta_i, \gamma \in K),$$

The central map $F = F_S||F_R||F_P$. Randomly chooses an affine embedding $T : K^n \to K^{n'}$ of full rank and an invertible affine map $S : K^m \to K^m$. The public key is given by $P = S \circ F \circ T : F^n \to F^m$ and the private key includes of S, F and T.

2.2 SRP Encryption

For a given message $M \in K^n$, the ciphertext C corresponding to M is obtained by the polynomial evaluation

$$C = P(M) \in K^m.$$

2.3 SRP Decryption

For a ciphertext $C \in K^m$, the decryption is executed as follows.

Step 1. Compute $Y = (y_1, ..., y_m) = S^{-1}(C)$ and $X = \phi^{-1}(y_1, ..., y_d)$.

Step 2. Compute $R = \pm X^{(q^d+1)/4}$ and $D_0 = \phi(R)$.

Step 3. For $k = 1$ to h do:

(3-1) For $Y_k = (y_{t_k+1}, ..., y_{t_k+o_k+r})$, where $t_k = v_k + (k-1)r$, substitute D_{k-1} into $f_R{}^k$ to get a system of linear equations with respect to $X_k = (x_{v_k+1}, ..., x_{v_k+o_k})$,

$$f_R{}^k(D_{k-1}, X_k) = Y_k.$$

(3-2) Solve the system using Gauss Elimination and denote the solution by D'_k. Let $D_k = D_{k-1}||D'_k$.

Step 4. Compute $M' = T^{-1}(D_h)$, which is the corresponding plaintext.

3 Our Improved Scheme

In [4], Duong et al. proposed a method to reduce the public key size of SRP by applying the idea of circulation. Inspired by this idea, we propose a method to reduce the size of the private key and improve the speed of decryption.

During the SRP decryption process, the inverse process of the central map is divided into two parts, Square part and Rainbow part, while the private key only needs to store the OV polynomials coefficients of the Rainbow. Therefore, we aim to reduce the size of the private key. In the inverse process of Rainbow, we need to plug in the Vinegar variables layer by layer, and thus calculate Oil variables of the corresponding layer, namely solving $Lx = u$, in which L is a coefficient matrix of size $(o_k+r)*o_k$ obtained by substituting Vinegar variables into the OV polynomials. The Rainbow part of SRP has an extra r OV equations per layer compared to the original Rainbow scheme. Because the Vinegar variable of the scheme is not selected randomly, it increase the number of equations to reduce the probability of degeneration. Here, we introduce rotation relations into parts of the private key so that L becomes a Toeplitz matrix. We define a $(o_k + r) * o_k$ Toeplitz matrix L take the form:

$$L = \begin{bmatrix} l_1 & l_2 & \cdots & l_{o_k-1} & l_{o_k} \\ l_{o_k+1} & l_1 & \cdots & l_{o_k-2} & l_{o_k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ l_{2o_k-1} & l_{2o_k-2} & \cdots & l_{o_k+1} & l_1 \\ l_{2o_k} & l_{2o_k-1} & \cdots & l_{o_k+2} & l_{o_k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ l_{2o_k+r-1} & l_{2o_k+r-2} & \cdots & l_{o_k+r+1} & l_{o_k+r} \end{bmatrix} \tag{1}$$

3.1 Construction

First, for each central polynomial, its coefficient matrix is represented by M, as is shown in figure 1. Among them, VV denotes the coefficients of Vinegar-Vinegar cross-terms and VO denotes Oil-Vinegar quadratic cross-terms coefficients. V stands for the coefficients of the linear term of Vinegar variables and O stands for the coefficients of the linear term of Oil variables, C denote the constant term. The white area stands for zero elements.

To suit L for the above form, for each layer of Rainbow, we construct the central map as follows.

(i) For the k^{th} layer, we randomly select the first central Oil-Vinegar equation. In other words, all non-zero elements of M_{k1} are randomly selected. Shown as the follows:

$$VV_1^k = (\mathbf{vv}_1^k, \mathbf{vv}_2^k, \cdots, \mathbf{vv}_{v_k}^k),$$

$$VO_1^k = (\mathbf{vo}_1^k, \mathbf{vo}_2^k, \cdots, \mathbf{vo}_{o_k}^k),$$

$$V_1^k = (\alpha_1^k, \alpha_2^k, \cdots, \alpha_{v_k}^k)^T,$$

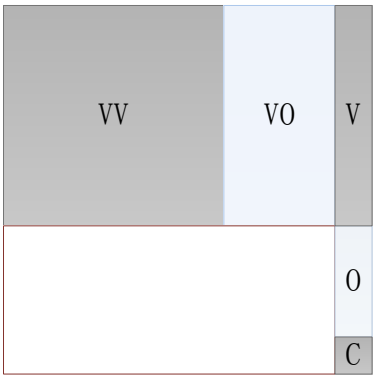

Fig. 1. Coefficient matrix of central polynomial

$$O_1^k = (\beta_1^k, \beta_2^k, \cdots, \beta_{o_k}^k)^T,$$
$$C_1^k = c_1^k.$$

(ii) For the next o_k+r-1 Oil-Vinegar polynomials, we first arbitrarily choose VV_i^k, V_i^k and $C_i^k (i = 2, \cdots, o_k + r - 1)$, then, we let

$$\begin{aligned}
&VO_2^k = (\mathbf{vo}_{o_k+1}^k, \mathbf{vo}_1^k, \cdots, \mathbf{vo}_{o_k-1}^k)\\
&VO_3^k = (\mathbf{vo}_{o_k+2}^k, \mathbf{vo}_{o_k+1}^k, \mathbf{vo}_1^k, \cdots, \mathbf{vo}_{o_k-2}^k)\\
&\vdots\\
&VO_{o_k}^k = (\mathbf{vo}_{2o_k-1}^k, \mathbf{vo}_{2o_k-2}^k, \cdots, \mathbf{vo}_{o_k+1}^k, \mathbf{vo}_1^k)\\
&VO_{o_k+1}^k = (\mathbf{vo}_{2o_k}^k, \mathbf{vo}_{2o_k-1}^k, \cdots, \mathbf{vo}_{o_k+1}^k)\\
&\vdots\\
&VO_{o_k+r}^k = (\mathbf{vo}_{2o_k+r-1}^k, \mathbf{vo}_{2o_k+r-2}^k, \cdots, \mathbf{vo}_{o_k+r}^k).
\end{aligned}$$

and

$$\begin{aligned}
&O_2^k = (\beta_{o_k+1}^k, \beta_1^k, \cdots, \beta_{o_k-1}^k)^T\\
&O_3^k = (\beta_{o_k+2}^k, \beta_{o_k+1}^k, \beta_1^k, \cdots, \beta_{o_k-2}^k)^T\\
&\vdots\\
&O_{o_k}^k = (\beta_{2o_k-1}^k, \beta_{2o_k-2}^k, \cdots, \beta_{o_k+1}^k, \beta_1^k)^T\\
&O_{o_k+1}^k = (\beta_{2o_k}^k, \beta_{2o_k-1}^k, \cdots, \beta_{o_k+1}^k)^T\\
&\vdots\\
&O_{o_k+r}^k = (\beta_{2o_k+r-1}^k, \beta_{2o_k+r-2}^k, \cdots, \beta_{o_k+r}^k)^T.
\end{aligned}$$

Where $\mathbf{vo}_{o_k+i}^k$ and $\beta_{o_k+i}^k$ $(i = 1, 2, \cdots, o_k + r - 1)$ are random selected.

3.2 Inverting the Central Map

In the process of decryption, take the inverse of the Square part as the Vinegar variable of the first layer, and substitute it into the central polynomials, and

solve the linear system. The calculation result and the Vinegar variable of the layer together are substituted into the central polynomials of the next layer as the Vinegar variable of the next layer, and thus continuing the same process until the calculation result of the last layer is generated. If the Vinegar variable of the k^{th} layer is $\mathbf{v} = (v_1, \cdots, v_{v_k})$, we plug it into the central polynomial and a linear equation system of $o_k + r$ linear equations in o_k variable can be got.

$$\underbrace{\mathbf{v}^T \cdot VV_i^k \cdot \mathbf{v} + \mathbf{v}^T \cdot V_i^k + C_i^k}_{\text{constant}} + \underbrace{\mathbf{v}^T \cdot VO_i^k \cdot \mathbf{o} + O_i^k \cdot \mathbf{o}}_{\text{linear in } \mathbf{o}} = y_{t_k+i} (i = 1, \cdots, o_k + r).$$

Let

$$e_{t_k+i} = y_{t_k+i} - (\mathbf{v}^T \cdot VV_i^k \cdot \mathbf{v} + \mathbf{v}^T \cdot V_i^k + C_i^k),$$

We have

$$\underbrace{\begin{bmatrix} \mathbf{v}^T \cdot VO_1^k + O_1^k \\ \mathbf{v}^T \cdot VO_2^k + O_2^k \\ \vdots \\ \mathbf{v}^T \cdot VO_{o_k}^k + O_{o_k}^k \\ \mathbf{v}^T \cdot VO_{o_k+1}^k + O_{o_k+1}^k \\ \vdots \\ \mathbf{v}^T \cdot VO_{o_k+r}^k + O_{o_k+r}^k \end{bmatrix}}_{L} \begin{bmatrix} x_{t_k+1} \\ x_{t_k+2} \\ \vdots \\ x_{t_k+o_k} \end{bmatrix} = \begin{bmatrix} e_{t_k+1} \\ e_{t_k+2} \\ \vdots \\ e_{t_k+o_k} \\ e_{t_k+o_k+1} \\ \vdots \\ e_{t_k+o_k+r} \end{bmatrix}.$$

and L is a $(o_k + r) * o_k$ Toeplitz matrix:

$$\begin{bmatrix} V^T \cdot \mathbf{vo_1^k} + \beta_1^k & V^T \cdot \mathbf{vo_2^k} + \beta_2^k & \cdots & V^T \cdot \mathbf{vo_{o_k}^k} + \beta_{o_k}^k \\ V^T \cdot \mathbf{vo_{o_k+1}^k} + \beta_{o_k+1}^k & V^T \cdot \mathbf{vo_1^k} + \beta_1^k & \cdots & V^T \cdot \mathbf{vo_{o_k-1}^k} + \beta_{o_k-1}^k \\ \vdots & \vdots & \ddots & \vdots \\ V^T \cdot \mathbf{vo_{2o_k-1}^k} + \beta_{2o_k-1}^k & V^T \cdot \mathbf{vo_{2o_k-2}^k} + \beta_{2o_k-2}^k & \cdots & V^T \cdot \mathbf{vo_1^k} + \beta_1^k \\ V^T \cdot \mathbf{vo_{2o_k}^k} + \beta_{2o_k}^k & V^T \cdot \mathbf{vo_{2o_k-1}^k} + \beta_{2o_k-1}^k & \cdots & V^T \cdot \mathbf{vo_{o_k+1}^k} + \beta_{o_k+1}^k \\ \vdots & \vdots & \ddots & \vdots \\ V^T \cdot \mathbf{vo_{2o_k+r-1}^k} + \beta_{2o_k+r-1}^k & V^T \cdot \mathbf{vo_{2o_k+r-2}^k} + \beta_{2o_k+r-2}^k & \cdots & V^T \cdot \mathbf{vo_{o_k+r}^k} + \beta_{o_k+r}^k \end{bmatrix}$$

The matrix L that is constructed at this point is exactly what we want.

Computing L: It can be seen from the structure of L that we have to compute only $2o_k + r - 1$ elements of L. The rest of L are generated by shift operations. Consequently, large amount of time and cost could be saved.

Solving the linear equation system: In general, solution for x can be calculated by Gaussian elimination. By our construction, we only need to solve a Toeplitz system which would be easier. There are many methods which can be used to solve a Toeplitz systems [27][11][14]. Therefore, we can obtain the solution in $O(n^2)$ time.

3.3 Probability of Decryption Success

In order to get the unique correct plaintext in the decryption process of SRP, the inverse result of the central map is hoped to be unique. Given that any ciphertext

is generated from a certain plaintext, it can be concluded that $Lx = u$ has at least one solution. For such a solvable linear equation system of $o_k + r$ equations in o_k variables, to make it have a unique solution, the rank of matrix L must be o_k. In the case of random selection of L, the probability that the rank is o_k is $(1 - q^{-o_k - r})(1 - q^{-o_k - r + 1} \cdots (1 - q^{-r-1}))$. Based on the three sets of security parameters given by [26], the probability of full rank of a random matrix of size $(o_k + r) * o_k$ and a Toeplitz matrix of size $(o_k + r) * o_k$ are tested respectively. The results of our test are averaged over 10^5 set test results. The probability of full rank of different types of matrices is displayed in Table 1. As is presented, under the three sets of parameters, the probability of the full rank is very close to 1.

Table 1. The Probability of Full Rank of Different Types of Matrices

$(K, d, h, \{o_1, \cdots\}, r, s, l)$	Security Level	Random Matrix $((o_1 + r) * o_1)$	Toeplitz Matrix $((o_1 + r) * o_1)$
$(GF(31), 33, 1, \{32\}, 16, 5, 16)$	80-bit	1.0000	1.0000
$(GF(31), 47, 1, \{47\}, 22, 5, 22)$	112-bit	1.0000	1.0000
$(GF(31), 71, 1, \{71\}, 32, 5, 32)$	160-bit	1.0000	1.0000

3.4 Key Sizes of Our Improved SRP

Compared with the original SRP scheme, our improved scheme only needs to store the following items for each layer of the Rainbow Part: $VV_i^k (i = 1, \cdots, o_k + r)$, $V_i^k (i = 1, \cdots, o_k + r)$, $C_i^k (i = 1, \cdots, o_k + r)$, $\mathbf{vo}_i^k (i = 1, \cdots, 2o_k + r - 1)$, $\beta_i^k (i = 1, \cdots, 2o_k + r - 1)$. Therefore,

The size of the private key of our improved scheme is :

$$m \cdot (m+1) + (n+l) \cdot (n+1) + \sum_{k=1}^{h} ((r + o_k) \cdot (\frac{v_k \cdot (v_k + 1)}{2} + v_k + 1) + (v_k + 1) \cdot (2o_k + r - 1))$$

field elements.

The size of the public key of our improved scheme is: $m \cdot \frac{(n+1) \cdot (n+2)}{2}$ field elements.

4 Security Analysis

In order to study the impact of the proposed method on the security of the original SRP scheme, existing mainstream attacks are applied to carry out the security analysis from the theoretical and experimental aspects.

4.1 Direct Attack

The basic principle of direct attack is to compute the plaintext by directly solving the equation system obtained by the ciphertext and the public key. This is also the most intuitive way. The direct attack algorithm includes F4/F5 algorithm, XL algorithm, Zhuang-Zi algorithm and so on. Currently, the most effective direct attack method is F4/F5 algorithm. Therefore, we carried out a number of experiments using the Magma implementation of F4. The results of our experiments against the original SRP scheme and our improved scheme are displayed in Table 2.

Table 2. Timing Results of the Direct Attack using Magma

q, d, o, r, s, l	m, n	Random System	The Original SRP	Our Improved SRP
31, 11, 10, 6, 5, 6	32, 15	0.839 s	0.841 s	0.843 s
31, 11, 10, 6, 5, 4	32, 17	37.765 s	37.127 s	37.127 s
31, 11, 10, 6, 5, 3	32, 18	105.864 s	104.742 s	104.826 s
31, 11, 11, 6, 5, 6	33, 16	2.333 s	2.385 s	2.391 s
31, 13, 10, 6, 5, 6	34, 17	27.238 s	27.318 s	27.312 s

4.2 Linearization Equation Attack

The linearization equation attack was first applied to break MI. Its basic idea is to obtain the potential linear relationship between the input and the output of the public key polynomial by analyzing the special structure of the central map, as is shown below:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_i y_j + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{m} c_j y_j + d.$$

Where, $Y = \{\mathrm{y}_1, ..., \mathrm{y}_m\}$ is comprised of m polynomials on $k[\mathrm{x}_1, ..., \mathrm{x}_n]$. This linear relationship is derived from that the central map also suits the linear relationship similar to the above form. In fact, the linear affine will not change the linear relation of this form in the process of constructing a public key. The coefficients in the linear relationship can be solved as long as the attacker has obtained enough plaintext-ciphertext pairs in advance. For SRP or improved SRP, the Rainbow part and the Plus part of central map are immune to this attack. we generate enough plaintext-ciphertext pairs and substitute them into the equations for solving. Experimental results show that there exists no linear relationship between the plaintext and ciphertext. Actually, there is no special relationship between the input variable and the output variable of the central map of our improved SRP, which means linear relationship or higher order linear equations is inexistent. Therefore, it can resist the linearization equation attack and the high order linearization equation attack.

4.3 Differential Attack

Given the public key P, the difference equation is defined as follows:

$$DP(A, X) = P(X + A) - P(X) - P(A) + P(0).$$

Differential attack can be used to find the invariant space of the simple Square scheme to recover the key of simple Square. However, the singature schemes UOV and Rainbow can resist against the differential attack. The SPR scheme introduces the central map F_R, F_P, therefore, differential attack is not feasible for SRP or improved SRP scheme.

4.4 MinRank Attack

MinRank attack transforms the security analysis of the scheme into the problem of MinRank, which is a very effective attack for multivarite public key cryptography. The principle of MinRank attack is to find a linear combination of the coefficient matrix corresponding to the public key polynomial, so that the rank of the obtained matrix is less than or equal to r. A partial key is restored by obtaining such a linear combination. By construction, we have $\text{rank}(f_s^i) \leq d$, $\text{rank}(f_r^{i,k}) \leq V_{k+1}$, $\text{rank}(f_p^i) \leq n'$ for the overall structure of SRP. Therefore, the MinRank attack against SRP is to look for a combination of the public key polynomials having a rank of at most d. Thomae and Wolf [23] adapt the method of [1] to analyze the complexity of MinRank attack against Double-Layer Square, which is also used in our scheme. For a random but fixed Sw, the probability that it lies in the kernel of a linear combination of $f_s^i (i = 1, .., d)$ is greater than $1/q$. Because T is a not a $n' \times n'$ square matrix but a $n' \times n$ matrix, so we will obtain q^l parasitic solutions. Therefore, the complexity of MinRank attack against SRP is approximately $O(d * q^{l+1} * m^3)$. It can be seen that the improved SRP does not affect the rank of $f_s^i (i = 1, .., d)$. As a result, the complexity of the MinRank attack is not reduced. So we conclude that the complexity of MinRank attack against the improved SRP is $O(d * q^{l+1} * m^3)$.

5 Experiments

To demonstrate the efficiency of our improved SRP, our improved scheme and the original scheme are compared with the key size and the performance of decryption. We implemented the three sets of secure parameters proposed in [4] with Sage, and performed 125 times for each set of parameters. The results of the experiment are given in Table 3. It can be seen from the table that the improved scheme has a significant improvement in performance. Under the 128-bit security level, the private key of our improved scheme can reduce by 61%, and the decryption speed is 2.1 times faster than that of the original scheme.

Table 3. Comparison between Our Improved SRP and the Original SRP

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
Security Level		80-bit	112-bit	160-bit
The Original SRP	Public Key Size(KB)	68.5	204.3	695.4
	Private Key Size (KB)	57.2	161.5	528.3
	Encryption (ms)	0.84	1.26	2.39
	Decryption (ms)	3.69	7.25	13.45
Our Improved SRP	Public Key Size (KB)	68.5	204.3	695.4
	Private Key Size (KB)	26.2	67.6	206.9
	Encryption (ms)	0.85	1.25	2.38
	Decryption (ms)	1.91	3.86	4.35

6 Conclusion

In this paper, we propose a SRP variant with shorter private key and higher decryption efficiency. The improved scheme can reduce the size of the private key by 61% and the speed of decryption is 2.1 times faster than the original scheme. Such improvements can make the SRP encryption scheme more applicable to resource-limited environments. We analyzed the improved scheme from the security perspective, and the results show that the improved scheme does not reduce the security of the scheme.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61632013, U1135004 and 61170080), 973 Program (No. 2014CB360501), Guangdong Provincial Natural Science Foundation (No. 2014A030308006), and Guangdong Provincial Project of Science and Technology (no. 2016B090920081).

References

1. Billet, O., Gilbert, H.: Cryptanalysis of Rainbow. In: Security and Cryptography for Networks: 5th International Conference, SCN 2006,. pp. 336–347. Springer Berlin Heidelberg (2006)
2. Ding, J., Gower, J.: Inoculating Multivariate Schemes Against Differential Attacks. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) Public Key Cryptography - PKC 2006, Lecture Notes in Computer Science, vol. 3958, pp. 290–301. Springer Berlin Heidelberg (2006)

3. Ding, J., Schmidt, D.: Rainbow, a New Multivariable Polynomial Signature Scheme. In: ACNS 2005. pp. 164–175 (2005)
4. Duong, D.H., Petzoldt, A., Takagi, T.: Reducing the Key Size of the SRP Encryption Scheme. In: Information Security and Privacy: 21st Australasian Conference, ACISP 2016. pp. 427–434. Springer International Publishing, Cham (2016)
5. Eder, C., Faugére, J.C.: A Survey on Signature-Based Algorithms for Computing Gröbner Bases. Journal of Symbolic Computation 80, 719 – 784 (2017)
6. Faugère, J.C.: A New Efficient Algorithm for Computing Gröbner Bases (F4). Journal of Pure and Applied Algebra 139(1), 61 – 88 (1999)
7. Faugère, J.C.: A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In: ACM ISSAC 2002. pp. 75–83 (2002)
8. Faugère, J.C., Din, M.S.E., Spaenlehauer, P.J.: On the complexity of the Generalized MinRank Problem. Journal of Symbolic Computation 55, 30–58 (2013)
9. Faugère, J.C., Levy-dit Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Advances in Cryptology – CRYPTO 2008. pp. 280–296. Springer Berlin Heidelberg (2008)
10. Fouque, P.A., Granboulan, L., Stern, J.: Differential Cryptanalysis for Multivariate Schemes. In: Advances in Cryptology – EUROCRYPT 2005. pp. 341–353. Springer Berlin Heidelberg (2005)
11. Gover, M.J.C., Barnett, S.: Inversion of Certain Extensions of Toeplitz Matrices. Journal of Mathematical Analysis & Applications 100(2), 339–353 (1984)
12. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar Signature Schemes. In: International Conference on Theory and Application of Cryptographic Techniques. pp. 206–222 (1999)
13. Matsumoto, T., Imai, H.: Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: The Workshop on Advances in Cryptology-Eurocrypt. pp. 419–453 (1988)
14. Ng, M.K., Rost, K., Wen, Y.W.: On Inversion of Toeplitz Matrices. Linear Algebra & Its Applications 348(1), 145–151 (2002)
15. Patarin, J.: Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt88. In: Advances in Cryptology CRYPT0 95. pp. 175–209. Springer Berlin Heidelberg (1995)
16. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. (ed.) Advances in Cryptology-EUROCRYPT '96. pp. 33–48. Springer Berlin Heidelberg (1996)
17. Patarin, J., Courtois, N., Goubin, L.: QUARTZ, 128-Bit Long Digital Signatures. In: CT-RSA 2001. vol. 2020, pp. 282–297 (2001)
18. Petzoldt, A., Chen, M.S., Yang, B.Y., Tao, C., Ding, J.: Design Principles for HFEv- Based Multivariate Signature Schemes. In: Advances in Cryptology – ASIACRYPT 2015. pp. 311–334. Springer Berlin Heidelberg (2015)
19. Porras, J., Baena, J., Ding, J.: ZHFE, a New Multivariate Public Key Encryption Scheme. In: International Workshop on Post-Quantum Cryptography. pp. 229–245 (2014)
20. Shen, W., Tang, S.: RGB, a Mixed Multivariate Signature Scheme. Computer Journal 59(4), 439–451 (2015)
21. Smith-Tone, D.: On the Differential Security of Multivariate Public Key Cryptosystems. In: International Workshop on Post-Quantum Cryptography. pp. 130–142. Springer Berlin Heidelberg (2011)
22. Tao, C., Diene, A., Tang, S., Ding, J.: Simple Matrix Scheme for Encryption. In: Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013. pp. 231–242. Springer Berlin Heidelberg (2013)

23. Thomae, E., Wolf, C.: Roots of Square: Cryptanalysis of Double-Layer Square and Square+. In: PQCrypto 2011. pp. 83–97. Springer Berlin Heidelberg (2011)
24. Wolf, C., An, B., Preneel, B.: On the Security of Stepwise Triangular Systems. Designs Codes & Cryptography 40(3), 285–302 (2006)
25. Yang, B.Y., Chen, J.M.: Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS. In: Information Security and Privacy: 10th Australasian Conference, ACISP 2005. pp. 518–531. Springer Berlin Heidelberg (2005)
26. Yasuda, T., Sakurai, K.: A Multivariate Encryption Scheme with Rainbow. In: Information and Communications Security: 17th International Conference, ICICS. pp. 236–251. Springer International Publishing (2016)
27. Zohar, S.: Toeplitz Matrix Inversion: The Algoritm of W. F. Trench. Journal of the ACM 16(4), 592–601 (1969)