

University of Technology Darmstadt  
Department of Computer Science  
Cryptography and Computeralgebra

Bachelor Thesis

September 2008

# Security Analysis of Quaternion Signatures



Desislava Ruseva

University of Technology Darmstadt  
Department of Mathematics

Supervised by Prof. Dr. Johannes Buchmann,  
Richard Lindner



## **Acknowledgements**

Foremost, I would like to thank Prof. Dr. Johannes Buchmann for giving me the opportunity to write this thesis. I am deeply grateful to my direct supervisor, Richard Lindner, for his detailed and constructive remarks, and for all his help and support throughout my work.

## **Warranty**

I hereby warrant that the content of this thesis is the direct result of my own work and that any use made in it of published or unpublished material is fully and correctly referenced.

Date: ..... Signature: .....



## Abstract

Digital signatures are probably the most important and widely used cryptographic primitive enabled by public key technology. They are building blocks of many modern distributed computer applications like electronic contract signing, certified email and secure web browsing. However, the hardness of many existing signature schemes lies on the intractability of problems in number theory. Since the invention of the RSA scheme by Rivest, Shamir and Adleman (1978) research has focused on improving the efficiency of these schemes. In this paper I am going to review the original OSS (Ong–Schnorr–Shamir) signature scheme [1], and also describe the first two improvements of this scheme—the Birational Permutation signature scheme, introduced in 1993 by Shamir [2] and the Quaternion OSS, proposed in 1997 by Satoh and Araki [3]. Furthermore, I will focus on the recently introduced generalized version of the OSS signature scheme, proposed by Hashimoto and Sakurai. Finally, I will explain the attacks, which render the first three signature schemes insecure and will analyse the security of the latest improvement.



# Contents

<b>Introduction</b>	<b>1</b>
<b>1 Mathematical Definitions and Notations</b>	<b>2</b>
<b>2 Signature Schemes</b>	<b>4</b>
2.1 Ong–Schnorr–Shamir . . . . .	5
2.2 Birational Permutations . . . . .	7
2.3 Quaternion OSS . . . . .	10
2.4 Generalized OSS . . . . .	12
<b>3 Security Issues</b>	<b>14</b>
<b>Conclusion</b>	<b>19</b>



## Introduction

Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation. One of their most significant applications is the certification of public keys in large networks. Certification is a means for a trusted third party (TTP) to bind the identity of a user to a public key, so that at some later time, other entities can authenticate a public key without assistance from a TTP.

The concept and utility of a digital signature was recognized several years before any practical realization was available. The first method discovered was the RSA signature scheme, which is based on the difficulty of factoring large numbers. It still remains one of the most practical and versatile techniques available [4].

The purpose of this paper is to review the original OSS signature scheme and its first two extensions, which were proposed a few years later; as well as to describe the attempts of breaking these schemes. Moreover, it is focused on the latest improvement of the OSS scheme and its security issues. In comparison with the RSA system, the OSS signature scheme is faster and can be easily implemented in software on microprocessors. Furthermore, according to [1] it is particularly suited to mobile items such as smart cards, cellular phones, data collection terminals, portable computers and remotely controlled devices, where authentication and signature schemes are essential. If it can be shown that this scheme is able to withstand specific cryptanalytic attacks and therefore considered to be secure, it could turn into a practical and efficient solution for a lot of unforgeable authentication problems.

# 1 Mathematical Definitions and Notations

Cryptography is considered a branch of both mathematics and computer science. Therefore, recalling some basic definitions and properties of important algebraic concepts would be really helpful for a deep understanding and close investigation of the discussed signature schemes.

**Definition 1.1.** Let  $n$  be a positive integer. Then the set  $Z_n = Z/nZ$  of integers modulo  $n$  forms a ring with  $n$  elements.

The notation  $Z/nZ$  is used, because it is the factor ring of  $Z$  by the ideal  $nZ$  containing all integers divisible by  $n$ . The modular arithmetic can be handled mathematically by introducing the idea of a *congruence relation* on the set of integers that is compatible with all the operations of the ring of integers. So for a fixed modulus  $n$ , it is defined as follows.

**Definition 1.2.** Two integers  $a$  and  $b$  are said to be congruent modulo  $n$ , if their difference  $(a - b)$  is an integer multiple of  $n$ . We write  $a \equiv b \pmod{n}$ .

Another important concept, which is clarified by the next definition, is that of the inverse element.

**Definition 1.3.** An integer  $a$  is considered as the *inverse* of an integer  $b$  modulo  $n$ , if  $ab \equiv 1 \pmod{n}$ .

Moreover, we say that an integer  $a$  is invertible modulo  $n$ , if and only if  $\gcd(n, a) = 1$ . The set of all invertible elements of  $(Z/nZ)$  is denoted by  $(Z/nZ)^*$  and forms a finite abelian group with respect to multiplication.

In order to become more acquainted with the concept of rings we should consider the following definition:

**Definition 1.4.** A ring  $R$  is called *left Euclidean*, if we could define a function  $\varphi$  on it mapping all non-zero elements of  $R$  into a well-ordered set that satisfies the following property. For all  $a, b$  in  $R$ ,  $b \neq 0$  there exist  $q$  and  $r$  in  $R$  such that  $a = qb + r$  and either  $r = 0$  or  $\varphi(r) < \varphi(b)$ .

This definition applies of course to non-commutative rings as well. If we want to be precise we will say that  $R$  is left Euclidean for  $\varphi$ , where  $\varphi$  is also called a *valuation*. We also say that the remainder  $r$  has  $\varphi$ -size smaller than the  $\varphi$ -size of the divisor  $b$ .

**Definition 1.5.** An *algebraic variety* is a set of points, where a polynomial attains a value of zero.

A rational map is a kind of partial function between two algebraic varieties. If a rational mapping has a rational inverse mapping as well, it is called a *birational function*.

There is just one more important definition, namely that of a quaternion, that should be introduced before describing the OSS signature scheme and its improvements.

**Definition 1.6.** A *quaternion number* is defined as  $q := a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$  where  $a, b, c, d \in \mathbb{R}$  and  $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$  is the basis of the quaternion algebra, given by

$$\mathbf{i} := \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \mathbf{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} := \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

The basis elements satisfy the non-commutative multiplication rules:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Moreover, there is a 1-to-1 correspondence between the quaternion numbers and the  $2 \times 2$  complex matrices:

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \leftrightarrow \begin{pmatrix} a + b\sqrt{-1} & c\sqrt{-1} + d \\ -c\sqrt{-1} + d & a - b\sqrt{-1} \end{pmatrix},$$

which allows us to consider the transposition  $q^t$ , the Hermitian conjugate  $q^* = \bar{q}^t$  and the inverse  $q^{-1}$  as those of the corresponding matrix respectively. The *norm*  $N(q)$  of  $q$  is defined as  $qq^*$ . Furthermore, the powers of each quaternion number  $q$  are linear combinations of 1 and  $q$ .

For convenience we may also write a quaternion number  $q$  as  $(a, b, c, d)$ . Moreover, quaternions of the form  $(a, b, 0, d)$  are termed *symmetric* since they satisfy  $q = q^t$ . Quaternions of the form  $(a, 0, 0, 0)$  are called *scalars*.

## 2 Signature Schemes

A digital signature, an asymmetric cryptographic scheme, is used to simulate the security properties of a handwritten signature on paper. It is used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital signature scheme consists of at least three algorithms.

- **A key generation algorithm** that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- **A signature algorithm** which, given a message and a private key, produces a signature.
- **A verification algorithm** which given a message, public key and a signature, either accepts or rejects.

According to [5] a digital signature should have the following properties.

1. The signature is *authentic*. It convinces the verifier that the signer deliberately signed the document.
2. The signature is *unforgeable*. It is a proof that the signer, and no one else, deliberately signed the document.
3. The signature is not *reusable*. It is a part of a specific document and an unscrupulous person cannot move it to a different document.
4. The signed document is *unalterable*. After the document is signed, it cannot be altered.
5. The signature cannot be *repudiated*. The signature and the document are physical things. The signer cannot later claim that he or she did not sign it.

## 2.1 Ong–Schnorr–Shamir

The OSS signature scheme, named after its founders Ong, Schnorr and Shamir, was first proposed in 1984. The idea is following. The signer, Alice, publishes a key, which consists of two numbers  $k$  and  $n$  that are at least 1000 bits long. The first one is called *multiplier* and the second one, which is a composite number whose factorization should remain secret, is called *modulus*. The messages  $m$  that are going to be signed are numbers in the range  $0 \leq m < n$ . The signature of each message consists of a pair of numbers  $s_1, s_2$  in the same range. A signature is considered valid if the following modular equation holds:

$$m = s_1^2 + ks_2^2 \pmod{n}$$

Knowing both  $k$  and  $n$  the verifier, Bob, can easily verify Alice's signature by simply performing three modular multiplications and one modular addition [1]. So the various components of the original OSS signature scheme can be summarized as follows:

### Key Generation:

1. Choose two prime numbers  $p$  and  $q$ , each at least 500 bits long.
2. Calculate  $n = pq$ .
3. Pick number  $u$ , relatively prime to  $n$ , randomly <sup>1</sup>.
4. Compute  $k = -1/u^2 \pmod{n}$ .
5. Publish  $(n, k)$  and keep  $u$  secret.

### Signature Generation:

1. Choose a random number  $r$ , relatively prime to  $n$ .
2. Compute the signature pair  $(s_1, s_2)$  as:

$$s_1 = (m/r + r)/2 \pmod{n}$$

$$s_2 = (m/r - r) * u/2 \pmod{n}$$

### Signature Verification:

1. Compute  $s_1^2 + ks_2^2 \pmod{n}$ .
2. If the result is  $m$ , the signature is valid.

In order to get a more clear idea of the introduced signature scheme, consider the following very simple example.

---

<sup>1</sup>In this paper under *randomly* I mean *uniformly at random*

*Example.* We choose  $p$  to be equal to 3 and  $q$  to 5. So we get  $n = 15$ . We put  $u = 2$ , which is relatively prime to  $n$ , and compute  $k = -\frac{1}{4} = 14\frac{3}{4} \pmod{15}$ . Thus, we have the pair  $(15, 59/4)$  as public key and  $u = 2$  as private key. In order to sign the message  $m = 8$ , we set  $r = 4$  and compute the signature  $(s_1, s_2)$  by using the formula given above:

$$\begin{aligned} s_1 &= (8/4 + 4)/2 \pmod{15} = 3 \pmod{15} \\ s_2 &= (8/4 - 4) * 2/2 \pmod{15} = -2 = 13 \pmod{15}. \end{aligned}$$

Now the verifier, who has received the signature  $(3, 13)$ , simply uses the public key to compute  $3^2 + \frac{59}{4} * 13^2 = 9 + \frac{59}{4} * 4 \pmod{15} = 8 \pmod{15}$ . Since  $m = 8$  the signature  $(3, 13)$  is considered valid.

Although computing  $k$  from  $u$  is quite easy, recovering  $u$  from  $k$  is really difficult since one cannot extract easily square roots in  $\mathbb{Z}_n^*$  without knowing the factorization of  $n$ .

In comparison with the RSA system, OSS signatures are not uniquely associated with messages. The reason is that the number of possible messages is  $n$  while the number of possible signature pairs is  $n^2$ . This means that each message has about  $n$  different signatures. However, the probability for a randomly chosen pair  $(s_1, s_2)$  to be a valid signature of a given  $m$  is negligible.

An important remark that should be made here is that each time when Alice wants to sign a message, she have to choose a different  $r$ . Otherwise an attacker, having access to two different messages and their corresponding signatures, both generated with the same  $r$ , would be able to compute her private key. Moreover, messages which are not relatively prime to  $n$  should not be signed. However, the probability for any such messages to occur is negligible.

## 2.2 Birational Permutations

The first improvement of the OSS signature scheme was proposed in 1993 by Shamir. It is based on the idea of birational permutations. More specifically speaking, the algorithm relies on the notion of multivariate mappings  $f(x_1, \dots, x_k) = (v_1, \dots, v_k)$  where the  $x_i$  and the  $v_i$  are numbers modulo a large integer  $n$ , since the solution of general algebraic equations of this type was considered to be as hard as the factorization of the modulus. The signature scheme can be summerized as follows:

### Key Generation:

1. Choose two large primes  $p, q$ .
2. Calculate  $n = pq$ .
3. Pick an integer  $k \geq 2$ <sup>2</sup> randomly.
4. Choose two random invertible matrices  $A, B \in \mathbb{Z}_n^{k \times k}$ .
5. Consider the birational permutation

$$G = g(y_1, \dots, y_k) = (w_1, \dots, w_k) \pmod{n} \text{ with}$$

$$g_i(y_1, \dots, y_i) = \begin{cases} y_1 & (i = 1) \\ y_1 y_2 & (i = 2) \\ u_i(y_1, \dots, y_{i-1})y_i + z_i(y_1, \dots, y_{i-1}) & (i \geq 3) \end{cases}$$

where  $u_i$  is a linear form and  $z_i$  is a quadratic form, both with coefficients in  $\mathbb{Z}_n$ , defined by

$$u_i : \mathbb{Z}_n^{i-1} \rightarrow \mathbb{Z}_n \\ (y_1, \dots, y_{i-1}) \mapsto u_1^{(i)} y_1 + \dots + u_{i-1}^{(i)} y_{i-1}$$

and

$$z_i : \mathbb{Z}_n^{i-1} \rightarrow \mathbb{Z}_n \\ (y_1, \dots, y_{i-1}) \mapsto z_{11}^{(i)} y_1^2 + \dots + z_{1(i-1)}^{(i)} y_1 y_{i-1} + z_{21}^{(i)} y_2 y_1 + \dots + z_{(i-1)(i-1)}^{(i)} y_{i-1}^2$$

6. For each  $i$ ,  $3 \leq i \leq k$ , choose a vector  $u^{(i)} \in \mathbb{Z}_n^{i-1}$  and a matrix  $z^{(i)} \in \mathbb{Z}_n^{(i-1) \times (i-1)}$  at random.
7. Apply the variable transformation  $y_i = Ax_i \pmod{n}$  for  $i = 1, \dots, k$ , where  $y_i$  and  $x_i$  are both unknown column vectors.
8. Apply the birational permutation  $G$  in order to get a system of equations of the form  $g(y_1, \dots, y_k) = (w_1, \dots, w_k) \pmod{n}$ .

---

<sup>2</sup>The case  $k = 2$  is equivalent to the original OSS signature scheme

9. Finally, apply the mixing transformation  $f_i = Bg_i$  ( $i = 1, \dots, k$ ).
10. Substitute consequently with the corresponding expressions of  $g_i$  and  $y_i$  to get  $k$  different polynomials  $v_i$  ( $i = 1, \dots, k$ ).
11. Discard the first polynomial.
12. Publish the rest of them as a public key.
13. Keep  $A, G, B$  secret.

**Signature Generation:**

1. Hash the message  $m$  into  $k - 1$  numbers  $(v_2, \dots, v_k)$  between 0 and  $n$ .
2. Choose  $v_1 \in \mathbb{Z}_n$  at random.
3. Substitute the obtained values of  $(v_2, \dots, v_k)$  into the public key.
4. Apply the mapping  $T = A^{-1} \circ G^{-1} \circ B^{-1}$  to the resulting equations.
5. The signature is the obtained solution  $X = (x_1, \dots, x_k)$  of the published equations.

**Signature Verification:**

1. Substitute the  $x_i$  values in the public key.
2. If the result is  $m$ , the signature is valid.

A validly generated signature is verified as correct.

In order to get a more clear idea of the procedure let us consider the following example, borrowed from [2].

*Example.* Assume that  $k = 3$  and  $n = 101$ . Let  $A \in \mathbb{Z}_n^{3 \times 3}$  be a randomly chosen matrix. We apply the linear change of variables  $y_i = Ax_i$  for  $i = 1, 2, 3$  and obtain the following system of equations:

$$\begin{aligned} y_1 &= x_1 + 25x_2 + 73x_3 && \pmod{101} \\ y_2 &= x_1 + 47x_2 + 11x_3 && \pmod{101} \\ y_3 &= x_1 + 83x_2 + 17x_3 && \pmod{101} \end{aligned}$$

The second step is to apply the mapping  $G(y) := (g_1, g_2, g_3)$  to get:

$$\begin{aligned} g_1(y_1) &= y_1 = w_1 \pmod{101} \\ g_2(y_1, y_2) &= y_1 y_2 = w_2 \pmod{101} \\ g_3(y_1, y_2, y_3) &= (29y_1 + 43y_2)y_3 + (71y_1^2 + 53y_2^2 + 89y_1 y_2) = w_3 \pmod{n} \end{aligned}$$

and thus after substituting the the  $y_i$ 's with their corresponding expressions from above we obtain:

$$\begin{aligned}
x_1 + 25x_2 + 73x_3 &= w_1 \pmod{101} \\
x_1^2 + 64x_2^2 + 96x_3^2 + 72x_1x_2 + 84x_1x_3 + 70x_2x_3 &= w_2 \pmod{101} \\
83x_1^2 + 55x_2^2 + 16x_3^2 + 28x_1x_2 + 97x_1x_3 + 74x_2x_3 &= w_3 \pmod{101}.
\end{aligned}$$

With the help of a randomly chosen  $3 \times 3$  matrix  $B$  we mix the three expressions  $g_1, g_2$  and  $g_3$  in the following way:

$$\begin{aligned}
f_1 &= g_1 \pmod{101} \\
f_2 &= 39g_2 + 82g_3 \pmod{101} \\
f_3 &= 93g_2 + 51g_3 \pmod{101}.
\end{aligned}$$

So the resulting expressions are:

$$\begin{aligned}
x_1 + 25x_2 + 73x_3 &= v_1 \pmod{101} \\
78x_1^2 + 37x_2^2 + 6x_3^2 + 54x_1x_2 + 19x_1x_3 + 11x_2x_3 &= v_2 \pmod{101} \\
84x_1^2 + 71x_2^2 + 48x_3^2 + 44x_1x_2 + 33x_1x_3 + 83x_2x_3 &= v_3 \pmod{101}.
\end{aligned}$$

Let  $m$  be the message to be signed. Assume that  $v_2 = h(m, 2) = 12$  and  $v_3 = h(m, 3) = 34$ . For these values of  $v_2, v_3$  we now search a proper solution  $x_1, x_2, x_3$  for the two published equations. Choose  $v_1$  randomly. In this example let  $v_1$  to be equal to 99. Apply the inverse mixing transformation  $B^{-1}$  by computing:

$$\begin{aligned}
w_1 &= v_1 = 99 \pmod{101} \\
w_2 &= 8v_2 + v_3 = 29 \pmod{101} \\
w_3 &= 27v_2 + 18v_3 = 27 \pmod{101}.
\end{aligned}$$

Thus the equations in terms of the  $y_i$ 's are:

$$\begin{aligned}
y_1 &= 99 \pmod{101} \\
y_1y_2 &= 29 \pmod{101} \\
(29y_1 + 43y_2)y_3 + (71y_1^2 + 53y_2^2 + 89y_1 - 1y_2) &= 27 \pmod{101}.
\end{aligned}$$

After substituting  $y_1 = 99$  into the second equation, we get  $y_2 = 36$ . Then we substitute both  $y_1$  and  $y_2$  in the third one and obtain  $y_3 = 29$ . Finally, with the help of the inverse of the variable transformation  $A$  we change the solution  $Y := (y_1, y_2, y_3)$  into the  $X$  solution  $x_1 = 40, x_2 = 27$  and  $x_3 = 22$ . Thus the signature generation procedure has been completed successfully. Now the verifier has only to substitute the  $x_1, x_2$  and  $x_3$  into the already published equations and see whether they hold.

## 2.3 Quaternion OSS

The second improvement of the OSS signature scheme was proposed in 1997 by Satoh and Araki. It is a non-commutative version of the original scheme. Here, instead of the ring of rational integers, the ring of integral quaternions is used.

So let  $Z := (ae + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{Z})$ <sup>3</sup> with  $e = (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$  and consider the following signature scheme:

### Key Generation:

1. Choose two prime numbers  $p, q$ .
2. Calculate  $n = pq$ .
3. Let  $R := Z/nZ$  and pick a quaternion number  $u \in R^*$ .
4. Compute  $k = -(u^t)^{-1}u^{-1}$ .
5. Publish  $(n, k)$  and keep  $u$  secret.

### Signature Generation:

1. Encode the message to a symmetric element  $m \in R$ .
2. Choose a random quaternion number  $r \in R^*$ .
3. Compute the signature pair  $(s_1, s_2)$  as:

$$s_1 = r^{-1}m + r^t$$

$$s_2 = u(r^{-1}m - r^t)$$

### Signature Verification:

1. If the equation  $s_1^t s_1 + s_2^t k s_2 = 2(m^t + m) = 4m$  holds, the signature is considered valid.

*Proof. (of correctness)* In order to prove the correctness of the equation above we must first substitute  $s_1, s_2$  and  $k$  with their corresponding definitions and afterwards apply some of the most important properties of quaternion numbers. To obtain the desired result we ought to transform the equation having in mind that the multiplication of a quaternion number  $q_i$  with its inverse element gives us the identity matrix and the transposition of  $q_i$  is in fact an antihomomorphism, which means that  $(q_1 + q_2)^t = q_1^t + q_2^t$  and  $(q_1 q_2)^t = q_2^t q_1^t$ . So we have:

---

<sup>3</sup>Defined in this way  $Z$  is a left Euclidean ring with respect to the norm  $N$ . This is an important property for the complexity of this signature scheme.

$$\begin{aligned}
s_1^t s_1 + s_2^t k s_2 &= (r^{-1}m + r^t)^t (r^{-1}m + r) + (u(r^{-1}m - r^t))^t k (ur^{-1}m - ur^t) \\
&= ((r^{-1}m)^t + r)(r^{-1}m + r^t) + (r^{-1}m - r^t)^t u^t k (ur^{-1}m - ur^t) \\
&= (m^t (r^{-1})^t + r)(r^{-1}m + r^t) + ((r^{-1}m)^t - r) u^t (-(u^t)^{-1} u^{-1}) (ur^{-1}m - ur^t) \\
&= m^t (r^{-1})^t r^{-1}m + m^t (r^{-1})^t r^t + m r r^{-1} + r r^t - m^t (r^{-1})^t u^t (u^t)^{-1} u^{-1} ur^{-1}m + \\
&\quad + m^t (r^{-1})^t u^t (u^t)^{-1} u^{-1} ur^t + r u^t (u^t)^{-1} u^{-1} ur^{-1}m - r u^t (u^t)^{-1} u^{-1} ur^t \\
&= m^t (r^{-1})^t r^{-1}m + m^t + m + r r^t - m^t (r^{-1})^t r^{-1}m + m^t + m - r r^t \\
&= m^t + m + m^t + m \\
&= 2(m^t + m) \\
&= 4m
\end{aligned}$$

□

In this signature scheme it is essential to remember that one should always encode the message to a symmetric matrix  $m$  in order to ensure that there exists exactly one valid message for each signature.

## 2.4 Generalized OSS

The latest improvement of the OSS signature scheme was proposed recently by Hashimoto and Sakurai. It is, in fact, a non-commutative version of the birational permutation signature scheme. Therefore, the idea is almost the same.

Let  $K$  be an algebraic finite extension of  $\mathbb{Q}$ ,  $O$  the integer ring of  $K$  and  $R$  a non-commutative subring of  $Mat_k(O/nO)$  ( $k \geq 1$ ) such that  $a^t \in R$  for any  $a \in R$ . Moreover, we put  $\alpha_1, \dots, \alpha_r$  a subset of  $R$  satisfying

$$R = \left\{ \sum_{i=1}^r a_i \alpha_i \mid a_i \in \mathbb{Z} \right\}$$

and  $\alpha_i \neq \sum_{j \neq i} a_j \alpha_j$  for any  $1 \leq i \leq r$  and  $a_j \in \mathbb{Z}$ . The signature scheme is as follows:

### Key Generation:

1. Pick two prime ideals  $p, q \in O$ .
2. Calculate  $n = pq$ .
3. Choose two integers  $l \geq 2$  and  $1 \leq r \leq k$  randomly.
4. Choose two random invertible matrices  $A \in (\mathbb{Z}_n)^{r \times l}$  and  $B \in (\mathbb{Z}_n)^{r \times (l-1)}$ .
5. Consider the projections

$$\varphi((y_{11}, \dots, y_{1r}, y_{21}, \dots, y_{lr})) = (y_{11}\alpha_1 + \dots + y_{1r}\alpha_r, \dots, y_{l1}\alpha_1 + \dots + y_{lr}\alpha_r)$$

$$\psi(g_{21}\alpha_1 + \dots + g_{2r}\alpha_r, \dots, g_{l1}\alpha_1 + \dots + g_{lr}\alpha_r) = (g_{21}, \dots, g_{2r}, g_{31}, \dots, g_{lr})$$

and the mapping  $G(y) = (g_2, \dots, g_l)$  given as

$$g_i(y_1, \dots, y_i) := v_i(y_1, \dots, y_{i-1})^t y_i + y_i^t z_i(y_1, \dots, y_{i-1}) + w_i(y_1, \dots, y_{i-1}),$$

where  $v_i, z_i$  are linear forms and  $w_i$  is a quadratic form, each with coefficients in  $R$ , defined by  $v_i : \mathbb{Z}_n^{i-1} \rightarrow \mathbb{Z}_n$

$$(y_1, \dots, y_{i-1}) \mapsto v_1^{(i)} y_1 + \dots + v_{i-1}^{(i)} y_{i-1},$$

$$z_i : \mathbb{Z}_n^{i-1} \rightarrow \mathbb{Z}_n$$

$$(y_1, \dots, y_{i-1}) \mapsto z_1^{(i)} y_1 + \dots + z_{i-1}^{(i)} y_{i-1}$$

and

$$w_i : \mathbb{Z}_n^{i-1} \rightarrow \mathbb{Z}_n$$

$$(y_1, \dots, y_{i-1}) \mapsto y_1^t w_{11}^{(i)} y_1 + \dots + y_1^t w_{1(i-1)}^{(i)} y_{i-1} + y_2^t w_{21}^{(i)} y_1 + \dots + y_{i-1}^t w_{(i-1)(i-1)}^{(i)} y_{i-1}$$

6. For each  $i$ ,  $3 \leq i \leq k$ , choose vectors  $v^{(i)}, z^{(i)} \in \mathbb{Z}_n^{i-1}$  and a matrix  $w^{(i)} \in \mathbb{Z}_n^{(i-1) \times (i-1)}$  at random.
7. Publish the key  $S := B \circ \psi \circ G \circ \varphi \circ A$  and keep  $A, G$  and  $B$  secret.

**Signature Generation:**

Let  $m := (m_{22}, \dots, m_{lr})^t \in (\mathbb{Z}_n)^{r \times (l-1)}$  be the message to be signed.

1. Calculate  $m' = B^{-1}m$ .
2. Choose  $y_1 \in R$  randomly.
3. Determine  $y_2, \dots, y_l \in R$  recursively by solving  $g_i(y_1, \dots, y_i) = \psi^{-1}(m'_i)$ .
4. The signature is given by  $X = A^{-1}(\varphi^{-1}(y)) \in (\mathbb{Z}_n)^{r \times l}$

**Signature Verification:**

1. Verify whether  $S(X) = m$ .

A correctly generated signature is verified as valid.

### 3 Security Issues

One of the most important aspects of any digital signature is its security properties. Unfortunately, there are no security proofs for most signature schemes. However, there are security reductions. In such a security reduction it is proved that the signature scheme is secure as long as certain mathematical assumptions are true. An example of such an assumption is the hardness of the integer factoring problem. Moreover, if it can be shown that a given signature scheme could withstand concentrated cryptanalytic attacks for a reasonable period of time, this scheme is considered secure. In this section I am going to describe the attacks, which render the first three variants of the OSS signature scheme insecure, and to analyse the security of the latest improvement of that scheme.

Although it was considered that the security of the original OSS signature scheme was based on the difficulty of factoring the modulus  $n$ , Pollard and Schnorr broke this scheme in 1987 by solving the equation  $x^2 - Dy^2 = m \pmod{n}$  directly without factoring  $n$ . The algorithm is based on the following lemmas:

**Lemma 3.1.** *The product of two numbers, each of the form  $x^2 - Dy^2$ , can also be written in the same form.*

**Lemma 3.2.** *The substitution  $u = xy^2$ ;  $v = y^{-1}$  transforms an equation of the form*

$$x^2 - Dy^2 = m \pmod{n}$$

*to one of the form*

$$u^2 - mv^2 = D \pmod{n}$$

**Lemma 3.3.** *Given a solution of the congruence*

$$x^2 = D \pmod{p}$$

*one can find in polynomial time integers  $u$  and  $v$  such that*

$$u^2 - Dv^2 = \lambda p$$

*where  $\lambda \leq \frac{1}{4} + \sqrt{\frac{4|D|}{3}}$*

**Lemma 3.4.** *It is easy to find solutions to*

$$x^2 \pm y^2 = m \pmod{n}$$

Proofs of the lemmas can be found in [6].

The algorithm of Pollard and Schnorr can be summarized as follows:

**Step 1:** Find, by probabilistic prime tests, a small prime  $p = m \pmod{n}$  such that  $D$  is a quadratic residue of  $p$ .

**Step 2:** Solve  $x^2 - D = 0 \pmod{p}$  using any random polynomial time square-root algorithm.

**Step 3:** Use Lemma 3 and the solution from step 2 in order to find integers  $u$  and  $v$  such that  $u^2 - Dv^2 = \lambda p$ .

**Step 4:** We want to solve  $w^2 - Dz^2 = \lambda \pmod{n}$ . With the help of Lemma 2 we interchange the roles of  $D$  and  $\lambda$ . Thus we have obtained a congruence with much smaller coefficients, which according to Lemma 4 could be solved recursively. Finally, we interchange  $D$  and  $\lambda$  again and have already got a solution of  $w^2 - Dz^2 = \lambda \pmod{n}$ .

**Step 5:** We have  $(u^2 - Dv^2)(w^2 - Dz^2)^{-1} = p = m \pmod{n}$ . It follows from Lemma 1 that the left side of this equation is actually of the proper form.

Thus Pollard and Schnorr have shown that it is possible to solve an equation of the form  $x^2 - Dy^2 = m \pmod{n}$  without knowing the factorization of  $n$ .

The next signature algorithm, which I have introduced in section 2 of this paper, is the Birational Permutation signature scheme. In 1998 Coppersmith and Vaudenay showed that it is possible to break this scheme by first reducing it algebraically to the original OSS scheme and then applying the Pollard algorithm. The idea of this breaking algorithm is described next in details.

Let  $A_i$ ,  $2 \leq i \leq k$ , denote the  $k \times k$  symmetric matrix of the quadratic form  $f_i$ . Note that the kernel  $K_i$  of  $g_i$  is, in fact, the kernel of the linear mapping whose matrix is  $A_i$ . Moreover, one can express  $f_i$  in the following way:

$$f_i = \delta_i g_k + \sum_{j=2}^{k-1} \beta_{ij} g_j$$

Since coefficients has been chosen randomly, the probability for  $\delta_k$  to be equal to 0 is negligible. Therefore we can assume that  $\delta_k$  is not zero.

Let  $i < k$  and consider the quadratic form  $Q_i(\lambda) = f_i - \lambda f_k$ . One can easily see that for  $\lambda = \delta_i/\delta_k$  this form has a non-trivial kernel and therefore  $\delta_i/\delta_k$  is a root of the polynomial  $P_i(\lambda) = \det(Q_i(\lambda))$ . It can also be shown <sup>4</sup> that  $\delta_i/\delta_k = \lambda_i$  is actually a double root of the polynomial equation  $P_i(\lambda) = 0$ . Thus, if one computes the  $\gcd(P_i, P_i')$   $\pmod{n}$  with respect to  $\lambda$ , he can easily find  $\lambda_i$ . The next step is to set:

$$\tilde{f}_i = f_i - \lambda_i f_k \quad \text{for } 2 \leq i < k$$

and  $\tilde{f}_k = f_k$ . It is important to mention that all quadratic forms  $\tilde{f}_i$  have kernel  $K_{k-1}$ . Therefore one is allowed to pick a non-zero vector  $b_k$  in  $K_{k-1}$ .

---

<sup>4</sup>see [7] for details

Recursively we obtain a sequence  $b_i$ ,  $3 \leq i \leq k$ , such that  $b_{i+1}, \dots, b_k$  spans  $K_i$  for  $i = 2, \dots, k-1$ . By choosing  $b_1$  and  $b_2$  randomly, we get another set of coordinates  $z_1, \dots, z_k$  such that  $\tilde{f}_2$  is a quadratic form in  $z_1, z_2$  and  $\tilde{f}_3, \dots, \tilde{f}_k$  is sequentially linearized (i.e. having solved the first equation  $\tilde{f}_2$  for  $z_1$  and  $z_2$ , we can then recursively solve the rest of the equations  $\tilde{f}_i$ ,  $i = 3, \dots, k$  as well). Then, from a sequence of prescribed values for  $\tilde{f}_2, \dots, \tilde{f}_k$ , we compute the corresponding values of  $\tilde{f}_2, \dots, \tilde{f}_k$ . With the help of the Pollard algorithm we solve the first equation, namely that of  $\tilde{f}_2$ . Having found the values of  $z_1$  and  $z_2$ , we are able to solve the rest of the equations. As a result we have obtained the values of all  $z_i$ ,  $i = 1, \dots, k$ , which can now be translated into  $x_i$  values,  $i = 1, \dots, k$ .

In this way Coppersmith and Vaudenay have found an algorithm, which renders the first improvement of the OSS signature scheme insecure.

The third signature algorithm, I have introduced in this paper, is the Quaternion signature scheme. In 1999 Coppersmith proposed two possible attacks on this scheme [8]. Now I am going to describe only the second one.

Given the public key  $(k, n)$  and a message  $m$ , we have to find elements  $s_1$  and  $s_2$  of  $R$ <sup>5</sup> satisfying  $s_1^t s_1 + s_2^t k s_2 = 4m$ . Since the space of symmetric elements of  $R$  is a 3-dimensional linear space over  $\mathbb{Z}_n$  and moreover, both  $m$  and  $k$  are symmetric, there is high probability that  $(1, k, m)$  form a linear basis for this space. Assume this to be the case and consider the product  $S = (a + b\mathbf{i} + d\mathbf{k})^t k (a + b\mathbf{i} + d\mathbf{k})$ <sup>6</sup>. Since  $S$  is symmetric, it can be expressed as:

$$\begin{aligned} S &= (a + b\mathbf{i} + d\mathbf{k})^t k (a + b\mathbf{i} + d\mathbf{k}) \\ &= Q_1(a, b, d)1 + Q_2(a, b, d)\mathbf{i} + Q_3(a, b, d)\mathbf{k}, \end{aligned}$$

where  $Q_i(a, b, d) = q_{i11}a^2 + q_{i12}ab + q_{i13}ad + q_{i22}b^2 + q_{i23}bd + q_{i33}d^2$  with  $q_{ijk} \in \mathbb{Z}_n$  for  $1 \leq i, j, k \leq 3$ . Thus,  $S$  is a linear combination of  $1, \mathbf{i}$  and  $\mathbf{k}$ . Our purpose now is to find values  $a, b, d$  such that  $S$  becomes a linear combination of  $1$  and  $m$ . So let  $m = m_1 + m_2\mathbf{i} + m_3\mathbf{k}$  with  $(m_2, m_3) \neq (0, 0)$  and consider the quadratic function  $R$  of  $a, b, d$ :

$$\begin{aligned} R(a, b, d) &= \det \begin{bmatrix} 1 & 0 & 0 \\ m_1 & m_2 & m_3 \\ Q_1(a, b, d) & Q_2(a, b, d) & Q_3(a, b, d) \end{bmatrix} \\ &= m_2 Q_3(a, b, d) - m_3 Q_2(a, b, d). \end{aligned}$$

In order to find  $a, b, d$  (not all zero) such that  $R(a, b, d) = 0 \pmod{n}$ , we use the following theorem.

---

<sup>5</sup>as defined in section 2.3

<sup>6</sup>Note that  $k$  denotes the public key, while  $\mathbf{i}$  and  $\mathbf{k}$  are basis elements of the quaternion algebra (see Def.1.6)

**Theorem 3.5 (8).** *Let  $n$  be an odd positive integer, and let  $f(x, y)$  be given by  $f(x, y) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F$ , and define  $\Delta(f)$ , the determinant of  $f$ , as follows:*

$$\Delta f = \det \begin{bmatrix} 2A & B & D \\ B & 2C & E \\ D & E & 2F \end{bmatrix}$$

*If  $\gcd(\Delta f, n) = 1$ , then there exists an algorithm requiring  $O(\log(e^{-1} \log n) \log^4 n)$  arithmetic operations on integers of size  $O(\log n)$  bits that will give a solution to  $f(x, y) = 0 \pmod{n}$  with probability  $1 - e$ .*

We set  $d = 1, a = x, b = y$  and  $R(a, b, 1) = f(x, y)$  and apply Theorem 3.5 to get  $a, b$  satisfying  $R(a, b, 1) = 0 \pmod{n}$ . In this way we have actually found scalars  $a, b, c, e$  for which the equation  $(a + \mathbf{b}\mathbf{i} + \mathbf{k})^t k (a + \mathbf{b}\mathbf{i} + \mathbf{k}) = c + em$  holds.

Let  $s_1 = h + w\mathbf{j}$

$s_2 = (a + \mathbf{b}\mathbf{i} + \mathbf{k})(f + gm)$  where  $f, g, h, w$  are unknown scalars. By substituting the new expressions of  $s_1, s_2$  in the original signature equation we get:

$$\begin{aligned} 4m &= s_1^t s_1 + s_2^t k s_2 \\ &= (h + w\mathbf{j})^t (h + w\mathbf{j}) + (f + gm)^t (a + \mathbf{b}\mathbf{i} + \mathbf{k})^t k (a + \mathbf{b}\mathbf{i} + \mathbf{k}) (f + gm) \\ &= (h^2 + w^2 + cf^2) + (2cfg + ef^2)m + (2efg + cg^2)m^2 + (eg^2)m^3. \end{aligned}$$

Since  $m$  is a quaternion number,  $m^2$  and  $m^3$  are linear combinations of 1 and  $m$ . Therefore we can define them as:

$$\begin{aligned} m^2 &= zm = r \\ m^3 &= sm = t, \end{aligned}$$

where  $z, r, s, t \in \mathbb{Z}_n$ . After substituting  $m_2, m_3$  in the equation above, we get:

$$\begin{aligned} 4m &= (h^2 + w^2 + cf^2 + r(2efg + cg^2) + t(eg^2)) \\ &+ (2cfg + ef^2 + z(2efg + cg^2) + s(eg^2))m \end{aligned}$$

with  $f, g, h, w$  free variables and  $c, e, r, s, t, z$  known constants. With the help of Theorem 3.5, we find  $f$  and  $g$  satisfying

$$4 = 2cfg + ef^2 + z(2efg + cg^2) + s(eg^2).$$

Finally, we apply the same theorem again in order to get  $h$  and  $w$  satisfying:

$$0 = h^2 + w^2 + cf^2 + r(2efg + cg^2) + t(eg^2).$$

In this way Coppersmith has shown that it is possible to find a signature  $(s_1, s_2)$  satisfying the signature equation  $s_1^t s_1 + s_2^t k s_2 = 4m$  by knowing only the public key  $(k, n)$  and the message  $m$ .

The last signature scheme, introduced in this paper, is the Generalized OSS signature scheme. It is based on multivariate quadratic equations combining ideas of both Birational Permutation and Quaternion OSS signature schemes. The most important question regarding the security of this new signature algorithm is how one ought to define  $R$  in order to have a secure signature scheme. For  $R = \text{Mat}_k(\mathbb{Z}_n)$ ,  $k \in \mathbb{Z}$ ,  $k \geq 2$ , the signature scheme can be broken by simply expressing  $s_1$  and  $s_2$  as triangular and diagonal matrices respectively, and afterwards applying the Pollard-Schnorr algorithm  $k$ -times. Now assume that  $R \subset \text{Mat}_3(\mathbb{Z}_n)$  and let

$$g_1 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, g_2 := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, g_3 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$g_4 := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, g_5 := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Put  $R_3 = \{\sum_{i=1}^6 a_i g_i | a_i \in \mathbb{Z}_n\}$ . It is easy to see that  $R_3$  is a subring of  $\text{Mat}_3(\mathbb{Z}_n)$ . The identity element of  $R_3$  is  $I = g_1 + g_2 + g_3 - g_4 - g_5$ . Coppersmith's second attack, which I have already described, uses three main properties of the quaternion ring, namely:

- The symmetric elements of  $R$  are of the form  $(a, b, 0, d)$  with  $a, b, d \in \mathbb{Z}_n$ .
- The powers of any element  $m \in R$  are integer linear combinations of 1 and  $m$ .
- There exists  $\delta = \delta(x, y) \in R$  such that  $\delta^t \delta = x^2 + h y^2$  for some  $h \in \mathbb{Z}_n$ . [9]

According to [9] none of these properties holds for  $R = R_3$ . However, the question whether this new scheme could be considered secure is still open.

## Conclusion

In this paper I have introduced an efficient signature scheme, namely the Ong–Schnorr–Shamir signature scheme, and its three improvements. Unfortunately all these schemes, except for the latest one, have already been broken and therefore cannot be used in practice. It has been shown so far that the Generalized OSS signature scheme, OSS' recent version, could withstand all the attacks, which render the first three schemes insecure, if one chose properly the ring  $R$ , on which this scheme operates. However, this assumption has not been proven yet completely. Therefore the reader of this paper is encouraged to investigate the security of this scheme more closely by both analyzing the feasibility of the already known attacks and searching for other possible weaknesses.

## References

1. H. Ong, C.P. Schnorr and A. Shamir, "An efficient scheme based on quadratic equations", *Proc. 16th ACM Symp. Theory of Computation*, 1984
2. A. Shamir, "Efficient signature scheme based on birational permutations", *Advances in Cryptology - CRYPTO '93*, Springer
3. T. Satoh and K. Araki, "On construction of signature scheme over a certain non-commutative ring", *IEICE Trans. Fundamentals*, Vol. E80-A, No. 1, January 1997
4. A. Menezes, P. Van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", *CRC Press*, 1996
5. B. Schneier, "Applied Cryptography", *second ed. Wiley, New York*, 1996
6. J. Shallit, "An exposition of Pollard's algorithm for quadratic congruences", *University of Chicago*, 1984
7. D. Coppersmith, J. Stern and S. Vaudenay, "Attacks on the birational permutation signature schemes", Springer, 1998
8. D. Coppersmith, "Weakness in quaternion signatures", *Crypto '99, LNCS 1666*, 1999
9. Y. Hashimoto and K. Sakurai, "On construction of signature schemes based on birational permutations over non-commutative rings", *Institute of Systems and Information Technologies*, Japan, 2008
10. J.M. Pollard and C.P. Schnorr, "An efficient solution of the congruence  $x^2 + ky^2 = m \pmod{n}$ ", *IEEE Trans. Inf. Theory*, IT-33, 1987