J. Cryptology (2001) 14: 77–85
DOI: 10.1007/s001450010006

Journal of
CRYPTOLOGY

Weakness in Quaternion Signatures

Don Coppersmith
IBM Research, T. J. Watson Research Center,
Yorktown Heights, NY 10598, U.S.A.
copper@watson.ibm.com

Communicated by Andrew Odlyzko

Received 9 December 1998 and revised 14 December 1998
Online publication 21 March 2000

Abstract. This note continues a sequence of attempts to define efficient digital signature schemes based on low-degree polynomials, or to break such schemes. We consider a scheme proposed by Satoh and Araki [5], which generalizes the Ong–Schnorr–Shamir scheme to the noncommutative ring of quaternions. We give two different ways to break the scheme.

Key words. Signatures, Polynomials, Noncommutative.

1. Introduction

The present note continues a sequence of attempts to define efficient digital signature schemes based on low-degree polynomials, or to break such schemes.

Ong, Schnorr, and Shamir [3] presented a signature scheme based on low-degree polynomials modulo a composite n of secret factorization, namely, $x^2 + ky^2 \equiv m \pmod{n}$. This scheme was subsequently broken by Pollard and Schnorr [4], who used a method of descent to solve this particular polynomial.

A similar scheme was put forth by Shamir [6] and soon broken by Coppersmith, et al. [2]. These researchers did not solve for the secret key, but found a polynomial satisfied by that key. By an analogy to Galois theory, they adjoined to $\mathbf{Z}/n$ a formal root of this polynomial, performed calculations in this extension ring, and found that the root itself was not required.

A common problem with low-degree polynomial signature schemes is that each signature reveals a polynomial equation satisfied by the secret key. If one collects enough signatures, one can combine the resulting polynomials to gather information about the secret key. We take this route to analyze the present scheme.

This paper involves a scheme proposed by Satoh and Araki [5], based on the noncommutative ring of quaternions; this scheme is a generalization of the Ong–Schnorr–Shamir [3] scheme. In our solution we gather three legitimate signatures on arbitrary messages.

Each signature gives an equation satisfied by the secret key τ. Combining the three, we can find some scalar multiple π of τ^{-1}, such that $\pi\tau$ is an unknown square root of a known element of $\mathbf{Z}/n$. Working in the quaternions we are able to get around this square root, producing a key ν which will work equally as well as τ for signing future messages.

Our paper is organized as follows. In Section 2 we review the ring of quaternions, especially as used with the integers mod n. Section 3 reviews the Pollard–Schnorr attack. Section 4 describes the Satoh–Araki scheme. In Section 5 we show how to collect and solve equations involving the secret key τ, and produce the equivalent key ν, with which future messages can be signed. A second solution is given in Section 6, which does not need to see legitimate signatures, but which requires a bit of computation to produce each new signature. Section 7 demonstrates that we cannot push these attacks further; we cannot obtain the secret key, either for this scheme or the original Ong–Schnorr–Shamir scheme. We conclude in Section 8.

2. Quaternions mod *n*

The Satoh–Araki signature scheme operates in a ring R of quaternions modulo a composite number n. The factorization of n is secret. Even the legitimate user need not know the factorization.

An element α of the ring R is a 4-tuple (a, b, c, d) of elements of $\mathbf{Z}/n$ (the integers modulo n). This element is usually written as $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. The special elements $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ satisfy the noncommutative multiplication rules:

$$\begin{aligned} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 &= -1, \\ \mathbf{ij} &= \mathbf{k} = -\mathbf{ji}, \\ \mathbf{jk} &= \mathbf{i} = -\mathbf{kj}, \\ \mathbf{ki} &= \mathbf{j} = -\mathbf{ik}. \end{aligned}$$

Greek letters $\alpha, \beta, \ldots$ represent elements of R, while Roman letters $a, b, c, \ldots$ represent elements of $\mathbf{Z}/n$. We denote by α^* the *Hermite conjugate* of α:

$$(a, b, c, d)^* = (a, -b, -c, -d);$$

by $N(\alpha)$ the *norm* of α:

$$N(a, b, c, d) = (a, b, c, d)(a, b, c, d)^* = a^2 + b^2 + c^2 + d^2 \in \mathbf{Z}/n;$$

and by α^{T} the *transpose* of α:

$$(a, b, c, d)^{\mathrm{T}} = (a, b, -c, d).$$

Elements of the form $(a, b, 0, d)$ are termed *symmetric* because they satisfy $\alpha = \alpha^{\mathrm{T}}$. Elements of the form $(a, 0, 0, 0) \in \mathbf{Z}/n$ are called *scalars*.

Multiplication is noncommutative.

The multiplicative group of invertible elements of R is denoted $R^\times$. The inverse is computed by

$$\alpha^{-1} = (\alpha^*\alpha)^{-1}\alpha^* = N(\alpha)^{-1}\alpha^*$$

whenever it exists, that is, whenever $N(\alpha)$ is relatively prime to n; recall that $N(\alpha)$ is a scalar so that its inversion is easy.

The transpose satisfies $(\alpha\beta)^{\mathrm{T}} = \beta^{\mathrm{T}}\alpha^{\mathrm{T}}$. We also have $(\alpha^{\mathrm{T}})^{-1} = (\alpha^{-1})^{\mathrm{T}}$.

The powers of any element α are integer linear combinations of 1 and α. In particular, if $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$,

$$\alpha^2 = \alpha(2a - \alpha^*) = -N(\alpha) + 2a\alpha,$$

so that α^2 is a linear combination of 1 and α, and the other powers follow by induction.

3. The Pollard–Schnorr Result

We use the result due to Pollard and Schnorr [4]:

Theorem 1. *Suppose the Generalized Riemann Hypothesis holds. Then there is a probabilistic algorithm which, upon input k, m, and n with* $\gcd(km, n) = 1$, *will solve* $x^2 + ky^2 \equiv m \pmod{n}$ *with an expected number of* $O((\log n)^2 |\log\log |k||)$ *arithmetical operations on* $O(\log n)$*-bit numbers.*

We also use a generalization due to Adleman et al. [1]:

Theorem 2. *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* $O(\log(\varepsilon^{-1}\log n)\log^4 n)$ *arithmetic operations on integers of size* $O(\log n)$ *bits that will give a solution to* $f(x, y) \equiv 0 \pmod{n}$ *with probability* $1 - \varepsilon$.

Remark. The generalization of Theorem 1 to general quadratic forms (Theorem 2) is achieved by completing the square, but Theorem 2 also dispenses with the Generalized Riemann Hypothesis.

4. The Satoh–Araki Scheme

The Satoh–Araki scheme generalizes the Ong–Schnorr–Shamir scheme to the ring of quaternions mod n. In this scheme n is a large composite modulus whose factorization is not public; even the legitimate user need not know the factorization. The private key is a random ring element $\tau \in R^{\times}$. The public key κ is the symmetric ring element

$$\kappa = -(\tau^{\mathrm{T}})^{-1}\tau^{-1}. \tag{1}$$

A message μ is encoded as a *symmetric* element of R. A signature (σ_1, σ_2) of μ is computed as follows: Pick $\rho \in R^{\times}$ randomly. Compute $\sigma_1 = \rho^{-1}\mu + \rho^{\mathrm{T}}$ and $\sigma_2 =$

$\tau(\rho^{-1}\mu - \rho^{\mathrm{T}})$. The signature is verified when the equation $4\mu = \sigma_1^{\mathrm{T}}\sigma_1 + \sigma_2^{\mathrm{T}}\kappa\sigma_2$ is satisfied.

5. Breaking the Scheme

For our first solution we need to see the signatures of three arbitrary messages. Each signature (σ_1, σ_2) satisfies the important property that

$$\sigma_1^{\mathrm{T}}\tau^{-1}\sigma_2 \text{ is symmetric.} \tag{2}$$

We verify this as follows:

$$\begin{aligned}
\sigma_1^{\mathrm{T}}\tau^{-1}\sigma_2 &= (\rho^{-1}\mu + \rho^{\mathrm{T}})^{\mathrm{T}}(\tau^{-1})(\tau(\rho^{-1}\mu - \rho^{\mathrm{T}})) \\
&= (\mu(\rho^{\mathrm{T}})^{-1} + \rho)(\rho^{-1}\mu - \rho^{\mathrm{T}}) \\
&= \mu(\rho^{-1})^{\mathrm{T}}\rho^{-1}\mu - \mu(\rho^{\mathrm{T}})^{-1}\rho^{\mathrm{T}} + \rho\rho^{-1}\mu - \rho\rho^{\mathrm{T}} \\
&= \mu(\rho^{-1})^{\mathrm{T}}\rho^{-1}\mu - \mu + \mu - \rho\rho^{\mathrm{T}} \\
&= \mu(\rho^{-1})^{\mathrm{T}}\rho^{-1}\mu - \rho\rho^{\mathrm{T}}
\end{aligned}$$

and each term is manifestly symmetric. (Recall that μ is symmetric.)

We would like to calculate τ or τ^{-1}, but this seems too hard. Instead, we find an element π which is a scalar multiple of τ^{-1}. Each such scalar multiple $\pi = \ell\tau^{-1}$, $\ell \in \mathbf{Z}/n$, also satisfies the property that $\sigma_1^{\mathrm{T}}\pi\sigma_2$ is symmetric. This is a linear homogeneous condition on the coefficients of π.

Suppose we see three signatures $(\sigma_1^{(i)}, \sigma_2^{(i)})$ on three messages $\mu^{(i)}$, $i = 1, 2, 3$. Each gives a linear homogeneous relation on the coefficients of π, namely, that $(\sigma_1^{(i)})^{\mathrm{T}}\pi\sigma_2^{(i)}$ is symmetric. By experiment we see that these three relations are in general nonredundant.

Remark. The three equations being redundant would correspond to the vanishing of a certain 3×3 determinant modulo p, where p is one of the unknown factors of the integer n. This determinant is a polynomial of low degree d in several random variables. The fact that the determinant failed to vanish in our experiments, implies that the determinant is not identically $0 \pmod{p}$, which implies that its probability of vanishing is $O(d/p)$. Since p is so large we can safely ignore this probability of failure. Even in the remote case of failure, if a determinant vanished modulo p but not modulo q, then the Euclidean algorithm would allow us to factor n via $\gcd(\det, n) = p$. A similar situation will hold whenever we "hope" that something does not "accidentally" vanish.

Since the three relations are nonredundant, they restrict the space of possible π to a one-dimensional space. That is, they determine π up to an unknown multiplicative scalar ℓ: $\pi = \ell\tau^{-1}$, $\ell \in \mathbf{Z}/n$. We select one such representative π.

We know the public key $\kappa = -(\tau^{\mathrm{T}})^{-1}\tau$. So we can compute

$$\begin{aligned}
z &= (\pi^{\mathrm{T}})^{-1}\kappa\pi^{-1} \\
&= \ell^{-1}\tau^{\mathrm{T}}\left(-(\tau^{\mathrm{T}})^{-1}\tau^{-1}\right)\tau\ell^{-1} \\
&= -\ell^{-2} \in \mathbf{Z}/n.
\end{aligned}$$

We know z but not ℓ. It is infeasible to take square roots in $\mathbf{Z}/n$, so that we cannot compute ℓ from z. However, in the quaternions we can easily find an element with a given norm, and this will serve in place of finding a square root.

Here we use a special case of the Pollard–Schnorr attack (Theorem 1) where $k = 1$, to find integers c, d satisfying

$$c^2 + d^2 \equiv -z^{-1} \pmod{n}.$$

Then

$$(c + d\mathbf{j})^{\mathrm{T}}(c + d\mathbf{j}) = (c - d\mathbf{j})(c + d\mathbf{j}) = c^2 + d^2 \equiv -z^{-1} \pmod{n}.$$

We can now define our "equivalent key" ν:

$$\nu = \pi^{-1}(c + d\mathbf{j}).$$

Equation (1) relating κ and τ can be restated as

$$\begin{aligned} \kappa &= -(\tau^{\mathrm{T}})^{-1}\tau^{-1}, \\ -1 &= \tau^{\mathrm{T}}\kappa\tau. \end{aligned}$$

We show that this equation is also satisfied by ν in place of τ:

$$\begin{aligned} \nu^{\mathrm{T}}\kappa\nu &= (c + d\mathbf{j})^{\mathrm{T}}(\pi^{-1})^{\mathrm{T}}\kappa\pi^{-1}(c + d\mathbf{j}) \\ &= (c - d\mathbf{j})\left((\pi^{-1})^{\mathrm{T}}\kappa\pi^{-1}\right)(c + d\mathbf{j}) \\ &= (c - d\mathbf{j})z(c + d\mathbf{j}) \\ &= (c - d\mathbf{j})(c + d\mathbf{j})z \\ &= (c^2 + d^2)z \\ &\equiv -1 \pmod{n}. \end{aligned}$$

Thus the "private key" ν corresponds to the public key κ in the prescribed manner. This implies that the attacker can use ν to create signatures, exactly as the legitimate user uses τ.

To compute ν we only needed to see three legitimate signatures and do a minimal amount of computation.

In some sense this attack is unsatisfactory. It depended on (2), which in turn depended on the very structured way that σ_1, σ_2 were computed. They could have been computed in a more random fashion; for example, σ_1 could have been left-multiplied by a random element β satisfying $\beta^{\mathrm{T}}\beta = 1$, freshly calculated for each message, which would not affect the validity of the signature, but would block the present attack. So in the next section we present an attack that does not depend on the particular method of generating signatures outlined in [5].

6. A Second Attack

In our second attack we do not need to see any legitimate signatures. We need only the public key κ (and modulus n). To sign a given message μ, we perform three Pollard–Schnorr computations.

We are given the public key κ and a message μ, both symmetric elements of R, and we are required to find elements σ_1, σ_2 of R satisfying $\sigma_1^{\mathrm{T}}\sigma_1 + \sigma_2^{\mathrm{T}}\kappa\sigma_2 = 4\mu$.

The space of symmetric elements of R is a three-dimensional linear space over $\mathbf{Z}/n$. With very high probability the three symmetric elements 1, κ, μ form a linear basis for this space; we assume this to be the case.

For unknown elements a, b, d of $\mathbf{Z}/n$, consider the product $S = (a + b\mathbf{i} + d\mathbf{k})^{\mathrm{T}}\kappa(a + b\mathbf{i} + d\mathbf{k})$. Being symmetric, S can be expressed as a linear combination of 1, $\mathbf{i}$, and $\mathbf{k}$, with coefficients being quadratic functions of a, b, d. That is,

$$(a + b\mathbf{i} + d\mathbf{k})^{\mathrm{T}}\kappa(a + b\mathbf{i} + d\mathbf{k}) = Q_1(a, b, d)1 + Q_2(a, b, d)\mathbf{i} + Q_3(a, b, d)\mathbf{k},$$
$$Q_i(a, b, d) = q_{i11}a^2 + q_{i12}ab + q_{i13}ad + q_{i22}b^2 + q_{i23}bd + q_{i33}d^2,$$
$$q_{ijk} \in \mathbf{Z}/n.$$

The entries q_{ijk} of Q_i are linear functions of the entries of κ.

A preview of the computation: We find a setting of a, b, d making S a linear combination of 1 and μ. This enables us to arrange that in our signature equation $4\mu \stackrel{?}{=} \sigma_1^{\mathrm{T}}\sigma_1 + \sigma_2^{\mathrm{T}}\kappa\sigma_2$, both sides lie in the two-dimensional subspace spanned by 1 and μ. We can select parameters to make the coefficients of μ agree, and then the coefficients of 1, so that the signature equation holds. At each stage we need to solve a Pollard–Schnorr equation.

Let $\mu = m_1 + m_2\mathbf{i} + m_3\mathbf{k}$ with $(m_2, m_3) \neq (0, 0)$, and set

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

$R(a, b, d)$ is a quadratic function of a, b, d. Our first task is to find a, b, d (not all zero) such that $R(a, b, d) \equiv 0 \pmod{n}$; this is equivalent to S being a linear combination of 1 and μ. For this purpose we use Theorem 2, with $d = 1$, $a = x$, $b = y$, and $R(a, b, 1) = f(x, y)$. For this theorem we need to assume that $\gcd(\Delta(f), n) = 1$, that is, that for each prime p dividing n, $\Delta f \neq 0 \pmod{p}$. However, each coefficient of $R(a, b, 1)$ is a polynomial of total degree 2 in the coefficients of μ and κ, so that Δf is a polynomial of total degree 6 in the coefficients of μ and κ. Also, Δf is not identically 0 (because it is nonzero in some experimental instances), so it will be $0 \pmod{p}$ with negligible probability $O(1/p)$. So with high probability Theorem 2 applies, and we can easily find a, b satisfying $R(a, b, 1) \equiv 0 \pmod{n}$.

This means that we have computed scalars a, b, c, e satisfying

$$(a + b\mathbf{i} + \mathbf{k})^{\mathrm{T}}\kappa(a + b\mathbf{i} + \mathbf{k}) = c + e\mu.$$

For scalars f, g, h, p yet undetermined, we are going to have

$$\sigma_1 = h + p\mathbf{j},$$
$$\sigma_2 = (a + b\mathbf{i} + \mathbf{k})(f + g\mu).$$

Then our desired signature equation will be

$$\begin{aligned} 4\mu &\stackrel{?}{=} \sigma_1^{\mathrm{T}}\sigma_1 + \sigma_2^{\mathrm{T}}\kappa\sigma_2 \\ &= (h + p\mathbf{j})^{\mathrm{T}}(h + p\mathbf{j}) + (f + g\mu)^{\mathrm{T}}(a + b\mathbf{i} + \mathbf{k})^{\mathrm{T}}\kappa(a + b\mathbf{i} + \mathbf{k})(f + g\mu) \\ &= (h^2 + p^2) + (f + g\mu)(c + e\mu)(f + g\mu) \\ &= (h^2 + p^2 + cf^2) + (2cfg + ef^2)\mu + (2efg + cg^2)\mu^2 + (eg^2)\mu^3. \end{aligned}$$

As noted in Section 2, μ^2 and μ^3 are linear combinations of μ and 1. Suppose we calculate

$$\begin{aligned} \mu^2 &= q\mu + r, \\ \mu^3 &= s\mu + t, \\ q, r, s, t &\in \mathbf{Z}/n. \end{aligned}$$

Then our desired equation is

$$\begin{aligned} 4\mu \stackrel{?}{=}\ & (h^2 + p^2 + cf^2 + r(2efg + cg^2) + t(eg^2)) \\ & + [2cfg + ef^2 + q(2efg + cg^2) + s(eg^2)]\mu. \end{aligned}$$

The free variables are f, g, h, p, and the known constants are c, e, q, r, s, t, and the ring element μ.

The coefficient of μ in the above equation is a quadratic in f, g. We use Theorem 2 to find f, g satisfying

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

Having done this, another application recovers unknowns h, p satisfying

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

Putting it all together, we have used the Pollard–Schnorr attack or its generalization (Adleman–Estes–McCurley) three times to find a signature (σ_1, σ_2) satisfying the signature equation for a given κ, μ.

Remark. The Pollard–Schnorr solution to the equation $x^2 + ky^2 \equiv m \pmod{n}$ requires that both k and m be nonzero. In each of our applications of the solution, this will be the case with high probability.

7. Impossibility Results

We collect here some impossibility results, showing that in some sense our attacks are the best possible.

In our first attack we found a scalar multiple of the secret key τ. We also found an "equivalent" secret key ν which we could use in place of τ to sign messages. However, it is infeasible to find an equivalent secret key which is simultaneously a scalar multiple

of the true secret key, even given the signatures of many chosen messages. The same is true of the original Ong–Schnorr–Shamir scheme.

In our second attack, knowing only the public key, we can generate valid signatures of arbitrary messages. However, without seeing signatures generated by the legitimate owner, it is infeasible to compute an equivalent secret key.

Theorem 3. *Assume it is infeasible to factor n. Then, given the legitimate signatures of polynomially many chosen messages, it is infeasible to find any quantity ν which is both a scalar multiple of the secret key τ and also an equivalent secret key.*

Proof. The legitimate secret key τ and nonce ρ generate a signature (σ_1, σ_2) on the message μ by

$$\begin{aligned} \sigma_1 &= \rho^{-1}\mu + \rho^{\mathrm{T}}, \\ \sigma_2 &= \tau(\rho^{-1}\mu - \rho^{\mathrm{T}}). \end{aligned}$$

Using the same process, an alternate secret key $\tau' = -\tau$ and nonce $\rho' = \mu(\rho^{-1})^{\mathrm{T}}$ would generate a signature (σ_1', σ_2') on the same message by

$$\begin{aligned} \sigma_1' &= \rho^{\mathrm{T}}\mu^{-1}\mu + \rho^{-1}\mu = \sigma_1, \\ \sigma_2' &= -\tau(\rho^{\mathrm{T}}\mu^{-1}\mu - \rho^{-1}\mu) = \sigma_2. \end{aligned}$$

So, with arbitrary chosen plaintext, we cannot distinguish between the secret keys τ and τ'.

Suppose (without loss of generality) that $n = pq$ is the product of two primes. Consider a third secret key τ'', satisfying

$$\tau'' \equiv \begin{Bmatrix} \tau & (\mathrm{mod}\ p) \\ \tau' & (\mathrm{mod}\ q) \end{Bmatrix}.$$

By the Chinese Remainder Theorem, τ'' would also be an acceptable secret key. It follows that the only "equivalent keys" which are scalar multiples of τ are $\pm\tau$ and $\pm\tau''$.

Suppose we are able to recover an equivalent secret key which is simultaneously a scalar multiple of the true secret key, using the signatures of polynomially many chosen messages. Then we can factor n. Namely, given n, we select τ and compute the public key κ, and begin producing signatures. (Recall that we do not need to know the factorization of n to do so.) Using the oracle, we recover a key, either $\pm\tau$ or $\pm\tau''$. The recovered key will be unequal to $\pm\tau$ with probability at least $1/2$; say the key is τ''. Each coordinate of $\tau'' - \tau$ is divisible by p, and at least one coordinate is not divisible by q, so that for the price of computing a few gcd's with n we will recover p. □

Remark. The same idea shows that in the original Ong–Schnorr–Shamir scheme, even with polynomially many signatures of chosen messages, it is infeasible to recover an "equivalent secret key," namely, a square root of the public key.

Our next result shows that, if we have no legitimate signatures, the second attack is the best we can hope for.

Theorem 4. *Given only the public key, we cannot find an equivalent secret key.*

Proof. An oracle to do so would enable us to factor n. Namely, select a random integer x and compute $z \equiv x^2 \pmod{n}$. Use the Pollard–Schnorr attack to find integers c, d satisfying $c^2 + d^2 \equiv z \pmod{n}$. Define a public key $\kappa = c + d\mathbf{i}$. Use the oracle to find a ring element τ satisfying $\tau^{\mathrm{T}}\kappa\tau = -1$. By multiplicativity of norm, we know that $N(\tau^{\mathrm{T}})N(\kappa)N(\tau) = N(-1)$. However, $N(\kappa) = c^2 + d^2 \equiv x^2 \pmod{n}$, whence $1 = N(\tau)^2 N(\kappa) = (N(u)x)^2 \pmod{n}$, so that $\gcd(n, N(u)x - 1)$ is (with probability at least $1/2$) a nontrivial factor of n. □

8. Conclusions

We have presented two solutions to the Satoh–Araki signature scheme. The first depended on the particular way of generating signatures outlined in [5] to generate linear equations on the coefficients of the secret key τ, giving us an unknown scalar multiple of τ, related by a square root. We finessed the square root calculation by taking advantage of the freedom of the quaternion ring. The second solution worked only from the public key and the message, with no need to see previous legitimate signatures, and worked with high probability, requiring only three applications of a Pollard–Schnorr solution. Both are computationally quite efficient.

References

[1] L.M. Adleman, D.R. Estes, and K.S. McCurley, Solving bivariate quadratic congruences in random polynomial time, *Math. Comput.* vol. 48 (1987), pp. 17–28.

[2] D. Coppersmith, J. Stern, and S. Vaudenay, Attacks on the birational permutation signature schemes, in *Advances in Cryptology – CRYPTO* '93, D.R. Stinson (ed.), pp. 435–443, LNCS 773, Springer-Verlag, Berlin. *J. Cryptology*, vol. 10, no. 3 (Summer 1997), pp. 207–221.

[3] H. Ong, C.P. Schnorr, and A. Shamir, An efficient signature scheme based on quadratic equations, in *Proc.* 16*th ACM Symp. Theory of Computation*, 1984, pp. 208–216.

[4] J.M. Pollard and C.P. Schnorr, An efficient solution of the congruence $x^2 + ky^2 \equiv m \pmod{n}$, *IEEE Trans. Inform. Theory*, vol. IT-33, (1987), pp. 702–709.

[5] T. Satoh and K. Araki, On construction of signature scheme over a certain noncommutative ring, *IEICE Trans. Fundamentals*, vol. E80-A, no. 1, (January 1997), pp. 40–45.

[6] A. Shamir, Efficient signature schemes based on birational permutations, in *Advances in Cryptology – CRYPTO* '93, D.R. Stinson (ed.), pp. 1–12, LNCS 773, Springer-Verlag, Berlin.