Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 819182, 7 pages
http://dx.doi.org/10.1155/2014/819182

*Research Article*

# Signature Scheme Using the Root Extraction Problem on Quaternions

**Baocang Wang[1,2] and Yupu Hu[1]**

[1] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*
[2] *Guangxi Key Lab of Wireless Wide Band Communication and Signal Processing, Guilin University of Electronic Technology, Guilin 541004, China*

Correspondence should be addressed to Baocang Wang; bcwang79@aliyun.com

Received 6 February 2014; Accepted 19 May 2014; Published 28 May 2014

Academic Editor: Frank Werner



The root extraction problem over quaternion rings modulo an RSA integer is defined, and the intractability of the problem is examined. A signature scheme is constructed based on the root extraction problem. It is proven that an adversary can forge a signature on a message if and only if he can extract the roots for some quaternion integers. The performance and other security related issues are also discussed.

## 1. Introduction

Cryptographic algorithms are important tools to resolve the security issues in open networks, amongst which the public key cryptographic schemes [1] may be the most powerful tool. In a public key cryptosystem, two separate keys are deployed. One key is kept secret and can be used to decrypt ciphertexts or sign messages, and the other key can be published and is used for encrypting plaintexts or verifying signatures. It requires that it should be computationally infeasible to derive the secret key from the public key. In public key cryptography, three categories of algorithms are widely used in network and information security engineering according to their functionalities, namely, key exchange protocols [2], public key encryption schemes [3], and digital signature schemes [4]. The key exchange protocols are used to establish the shared keys between two communication parties. The public key encryption algorithm allows the encryption key to be published without compromising the security of the decryption key and hence does not require securely initializing a shared key between the communication sender and receiver. A digital signature scheme is used to create a digital signature on a message by using the secret key, so a signature scheme allows the authenticity of a message or a document by using the public key to verify the validity of the signature.

It is striking to note that most of the widely used unbroken public key cryptosystems are based on some number-theoretic intractability assumptions such as the integer factorization problem, the discrete logarithm problem defined over finite fields, and the elliptic curve discrete logarithm problem [1]. However, we have a strong desire to enrich the public key cryptographic toolkits to avoid putting all application-oriented eggs in one cryptographic basket. So tremendous efforts had been made to develop public key cryptosystems from other problems. In particular, it seems a nice idea to introduce some noncommutative algebraic structures [5–13] in the design of public key ciphers to destroy the commutativity property commonly shared in the widely used public key cryptosystems.

In the realm of noncommutative public key cryptography, some key exchange protocols and public key encryption schemes were developed, amongst which are the notable AAG commutator key exchange protocol [14] and its variants [15–17], the MOR encryption algorithm [18], the MST cryptosystems [19, 20], and the braid public key encryption schemes [21] and their instantiations on other generalized

noncommutative groups [7, 11–13]. On the one hand, many of the previous proposals were shown vulnerable to some attacks [22–34]. On the other hand, very few secure signature schemes were known in the literature of noncommutative public key cryptography [35–41]. The known signature schemes may have at least one of the flaws listed below.

(i) The security of the signature schemes cannot be mathematically proven [35–38]. Only the three schemes in [39–41] satisfy the provable security goals.

(ii) Some signature schemes [39–41] utilized some nonstandard intractability assumptions. These newly defined mathematical problems were not fully studied, so if the underlying intractability was not true, these schemes would be insecure.

(iii) The intractability problems were not tightly used in the construction of the signature schemes [35], which makes it possible for an adversary to forge a signature on a message just by solving an easy problem but not necessarily the underlying intractable problem [42, 43].

In this paper, we propose a novel signature scheme from the root extraction problem defined on the quaternion ring modulo an RSA integer. Our proposal overcomes the flaws existing in the known signature schemes.

(i) The security is based on the root extraction problem over quaternions, which can be seen as the generalizations of the standard RSA problem and the quadratic residue problem modulo an RSA modulus. So the intractability assumption of our proposal is well established.

(ii) The security of the proposed signature scheme is tightly dependent on the root extraction problem over quaternion rings. Any adversary must solve the underlying intractability problem in order to successfully recover the secret key or forge a signature.

(iii) The proposal is provably secure. We prove that an adversary can forge a signature for a given message if and only if he can extract the $e$-th root for a given quaternion number.

We also provide a thorough security scrutiny on the proposed signature scheme with respect to key recovery attacks and partial key exposure attacks. Performance analysis demonstrates that the proposal is efficient and practical.

The rest of the paper is organized as follows. In Section 2, we provide some preliminaries about the quaternion algebra, discuss the related root extraction problem, and provide the signature scheme. In Section 3, we analyze the proposal with respect to performance and security. Finally, we conclude the work in Section 4.

## 2. Proposal

We first review some definitions about quaternion algebra and then elaborate on the proposed signature scheme.

*2.1. Notations.* Throughout this paper, we use $\mathbb{R}$ to denote the field of real numbers and use the symbol $\mathbb{Z}$ to denote the ring of integers. For a positive integer $N \in \mathbb{Z}$, the modular reduction of an integer $a \in \mathbb{Z}$ modulo $N$ means the unique nonnegative least remainder $b \in \mathbb{Z}$ of $a$ divided by $N$ such that $b \in \mathbb{Z}_N = \{0, 1, \ldots, N-1\}$, and we denote $b = a \pmod N$. The greatest common divisor of two integers $a$ and $b$ is denoted by $\gcd(a, b)$. We use $\mathbb{Z}_N^*$ to denote the set $\{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$. For any integer $a \in \mathbb{Z}_N^*$ there exists a unique integer $b \in \mathbb{Z}_N^*$ called the modular inverse of $a$ modulo $N$ such that $ab = 1 \pmod N$, and we denote $b = a^{-1} \pmod N$.

*2.2. Arithmetic Operations on Quaternions.* The number system of quaternions is the extension of the number system of complex numbers. Formally, we denote the set of quaternions as

$$\mathbb{H} = \left\{\mathbf{a} = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k} : a_1, a_2, a_3, a_4 \in \mathbb{R}\right\}. \quad (1)$$

We define three operations on quaternions, namely, addition, scalar multiplication, and quaternion multiplication. For two quaternions $\mathbf{a} = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$ and $\mathbf{b} = b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}$ in $\mathbb{H}$, their sum is defined as $\mathbf{c} = c_1 + c_2\mathbf{i} + c_3\mathbf{j} + c_4\mathbf{k}$ with $c_i = a_i + b_i$ for $1 \le i \le 4$. We define the scalar multiplication of $\mathbf{a} = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k} \in \mathbb{H}$ and $a \in \mathbb{R}$ as $a\mathbf{a} = aa_1 + aa_2\mathbf{i} + aa_3\mathbf{j} + aa_4\mathbf{k}$. The quaternion multiplication is somewhat more complicated to define. We first define $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$ and then we can derive the following relations:

$$\begin{aligned} &\mathbf{ij} = \mathbf{k}, \quad &&\mathbf{ji} = -\mathbf{k}, \quad &&\mathbf{jk} = \mathbf{i}, \\ &\mathbf{kj} = -\mathbf{i}, \quad &&\mathbf{ki} = \mathbf{j}, \quad &&\mathbf{ik} = -\mathbf{j}, \end{aligned} \quad (2)$$

from which we can easily see that quaternion multiplication is noncommutative. So the product of $\mathbf{a} = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$ and $\mathbf{b} = b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}$ can be easily computed via

$$\begin{aligned} \mathbf{ab} &= a_1\mathbf{b} + a_2\mathbf{ib} + a_3\mathbf{jb} + a_4\mathbf{kb} \\ &= a_1b_1 + a_1b_2\mathbf{i} + a_1b_3\mathbf{j} + a_1b_4\mathbf{k} \\ &\quad + a_2b_1\mathbf{i} + a_2b_2\mathbf{i}^2 + a_2b_3\mathbf{ij} + a_2b_4\mathbf{ik} \\ &\quad + a_3b_1\mathbf{j} + a_3b_2\mathbf{ji} + a_3b_3\mathbf{j}^2 + a_3b_4\mathbf{jk} \\ &\quad + a_4b_1\mathbf{k} + a_4b_2\mathbf{ki} + a_4b_3\mathbf{kj} + a_4b_4\mathbf{k}^2 \\ &= \left(a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4\right) \\ &\quad + \left(a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3\right)\mathbf{i} \\ &\quad + \left(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2\right)\mathbf{j} \\ &\quad + \left(a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1\right)\mathbf{k}. \end{aligned} \quad (3)$$

The norm and conjugate of $\mathbf{a} = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$ are defined as $\|\mathbf{a}\| = \sqrt{a_1^2 + a_2^2 + a_3^2 + a_4^2}$ and $\mathbf{a}^* = a_1 - a_2\mathbf{i} - a_3\mathbf{j} - a_4\mathbf{k}$, respectively. It is easy to verify that $\|\mathbf{a}\| = \sqrt{\mathbf{aa}^*} = \sqrt{\mathbf{a}^*\mathbf{a}}$.

For a positive integer $N \in \mathbb{Z}$ and a quaternion $\mathbf{a} = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$, we define $\mathbf{a}$ modulo $N$ as

$$\begin{aligned}\mathbf{a} \pmod N = {} & a_1 \pmod N + a_2 \pmod N \mathbf{i} \\ & + a_3 \pmod N \mathbf{j} + a_4 \pmod N \mathbf{k}.\end{aligned} \tag{4}$$

Thus, we can define the set $\mathbb{H}_N = \{\mathbf{a} \pmod N : \mathbf{a} \in \mathbb{H}\}$. We call a quaternion $\mathbf{a}$ invertible modulo $N$ if and only if there exists a quaternion $\mathbf{b}$ such that $\mathbf{ab} = \mathbf{ba} = 1 \pmod N$, and we denote $\mathbf{b} = \mathbf{a}^{-1} \pmod N$. We use the symbol $\mathbb{H}_N^*$ to denote the set consisting of all the invertible quaternions in $\mathbb{H}_N$. It is easy to verify that a quaternion $\mathbf{a} \in \mathbb{H}_N$ is invertible if and only if $\gcd(\|\mathbf{a}\|, N) = 1$. When $\gcd(\|\mathbf{a}\|, N) = 1$, the inverse of $\mathbf{a}$ modulo $N$ is easy to compute; namely, $\mathbf{a}^{-1} = \|\mathbf{a}\|^{-2}\mathbf{a}^* \pmod N$, where $\|\mathbf{a}\|^{-1}$ denotes the modular inverse of $\|\mathbf{a}\|$ modulo $N$.

*2.3. Root Extraction Problem over $\mathbb{H}_N$.* We define the $e$-th root extraction problem over $\mathbb{H}_N$.

*Definition 1* (the $e$-th root extraction problem over $\mathbb{H}_N$). Given two positive integers $N \in \mathbb{Z}$ and $2 \le e \in \mathbb{Z}$ and a quaternion $\mathbf{a} \in \mathbb{H}_N$, the $e$-th root extraction problem over $\mathbb{H}_N$ is defined as finding a quaternion $\mathbf{b} \in \mathbb{H}_N$ if any such that $\mathbf{b}^e = \mathbf{a} \pmod N$. In particular, when $e = 2$, the problem is called the quadratic root extraction problem over $\mathbb{H}_N$.

In this paper, we consider the case of $N$ being an RSA modulus, namely, $N = pq$ being the product of two distinct large primes $p$ and $q$. From the above definitions, we can see that when $e$ is relatively prime to $\phi(N) = (p-1)(q-1)$, the $e$-th root extraction problem over $\mathbb{H}_N$ is a generalization of the RSA problem, which asks for the $e$-th root $b$ for a given integer $a \in \mathbb{Z}_N$; namely, $a = b^e \pmod N$. The quadratic root extraction problem over $\mathbb{H}_N$ is a generalization of the quadratic residue problem, which is defined as finding an integer $b \in \mathbb{Z}_N$ such that $a = b^2 \pmod N$ for the given integer $a \in \mathbb{Z}_N$. The quadratic residue problem is proven to be equivalent to the problem of factoring the modulus $N$ in the construction of the Rabin public key cryptosystem [44]. We note that the RSA problem and the quadratic residue problem are widely believed as intractable and had been widely used in the design of public key cryptographic primitives. So we conjecture that the $e$-th root extraction problem over $\mathbb{H}_N$ is also intractable.

*2.4. Quaternion Signature Scheme.* Quaternion algebra had been used to design a signature scheme [35]. However, the signature scheme was soon broken [42, 43] by solving a quadratic congruence $x^2 + y^2 = m \pmod N$ with the Pollard-Schnorr algorithm [45].

We develop a new quaternion signature scheme in the sequel. To begin with, we first define three system parameters: the binary length $n \in \mathbb{Z}$ of the modulus $N$, the binary length $k \in \mathbb{Z}$ of the hashed value of a message $m \in \{0,1\}^*$, and $2 \le e \in \mathbb{Z}$. Typically, we set $n = 1024$, $k = 160$, and $e = 3$. We also define a hash function $H$ which maps a message bit string with an arbitrary length into a $k$-bit-long string; namely, $H : \{0,1\}^* \to \{0,1\}^k$. In this paper, we write a binary number as a string of symbols.

*2.4.1. Key Generation.* The key generation algorithm runs as follows. Firstly, the signer randomly chooses two distinct $n/2$-bit-long primes $p$ and $q$ and computes their product $N = pq$. Then, the signer randomly and uniformly chooses two quaternions $\mathbf{b} \in \mathbb{H}_N$ and $\mathbf{r} \in \mathbb{H}_N^*$ and computes $\mathbf{a} = \mathbf{rb}^e\mathbf{r}^{-1} \pmod N$. Finally, the signer publishes the public key as $(\mathbf{a}, N, H, e)$ and keeps the secret key as $(\mathbf{b}, \mathbf{r}^{-1})$.

*2.4.2. Signature.* To sign a message $m$, the signer firstly computes the hashed value of $m$; namely, $h = H(m)$. Then, the signer randomly and uniformly chooses a quaternion $\mathbf{s} \in \mathbb{H}_N^*$ and computes $\mathbf{t} = \mathbf{sr}^{-1} \pmod N$ and $\mathbf{u} = \mathbf{sb}^h\mathbf{s}^{-1} \pmod N$. Finally, the signer sends $(\mathbf{t}, \mathbf{u})$ to the verifier as the signature on the message $m$.

*2.4.3. Verification.* Upon receiving the signature $(\mathbf{t}, \mathbf{u})$, the verifier firstly computes $h = H(m)$ and $\mathbf{v} = \mathbf{a}^h \pmod N$. Then, the verifier decides whether or not the equation $\mathbf{u}^e = \mathbf{tvt}^{-1} \pmod N$ is satisfied. If the equation is satisfied, the verifier accepts $(\mathbf{t}, \mathbf{u})$ as a valid signature on the message $m$. Otherwise, the verifier refuses to accept $(\mathbf{t}, \mathbf{u})$ as a valid signature on $m$.

*2.4.4. Why Verification Works.* We explain why a valid signature $(\mathbf{t}, \mathbf{u})$ on the message $m$ can pass the verification equation $\mathbf{u}^e = \mathbf{tvt}^{-1} \pmod N$. Note that

$$\begin{aligned}\mathbf{tvt}^{-1} &= \left(\mathbf{sr}^{-1}\right)\mathbf{a}^h\left(\mathbf{sr}^{-1}\right)^{-1} = \mathbf{sr}^{-1}\left(\mathbf{rb}^e\mathbf{r}^{-1}\right)^h\mathbf{rs}^{-1} \\ &= \mathbf{sb}^{eh}\mathbf{s}^{-1} = \left(\mathbf{sb}^h\mathbf{s}^{-1}\right)^e = \mathbf{u}^e \pmod N.\end{aligned} \tag{5}$$

So a valid signature $(\mathbf{t}, \mathbf{u})$ on the message $m$ can pass the verification process.

## 3. Analysis

*3.1. Security.* We analyze the security of the proposed quaternion signature scheme.

*3.1.1. Key Security.* The secret key of the proposed signature scheme consists of $\mathbf{b} \in \mathbb{H}_N$ and $\mathbf{r} \in \mathbb{H}_N^*$. We have the following result with respect to the key security.

**Theorem 2.** *Any adversary can recover the secret key $(\mathbf{b}, \mathbf{r})$ from the public key $(\mathbf{a}, N, H, e)$ if and only if he can extract the $e$-th root for $\mathbf{a} \in \mathbb{H}_N$.*

*Proof.* We first prove the sufficiency of the theorem. Assume that the adversary can extract the $e$-th root for $\mathbf{a} \in \mathbb{H}_N$, and we denote it as $\mathbf{c} \in \mathbb{H}_N$; namely, $\mathbf{c}^e = \mathbf{a} \pmod N$. Then, we randomly choose $\mathbf{r} \in \mathbb{H}_N^*$ and compute $\mathbf{b} = \mathbf{r}^{-1}\mathbf{cr} \pmod N$. Then, $(\mathbf{b}, \mathbf{r})$ can serve as the secret key of the proposed

signature scheme; namely, $\mathbf{b}$ and $\mathbf{r}$ satisfy $\mathbf{a} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} (\mathrm{mod}\, N)$. This is because

$$\mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} = \mathbf{r}\left(\mathbf{r}^{-1}\mathbf{c}\mathbf{r}\right)^e\mathbf{r}^{-1} = \mathbf{r}\mathbf{r}^{-1}\mathbf{c}^e\mathbf{r}\mathbf{r}^{-1} = \mathbf{c}^e = \mathbf{a}\,(\mathrm{mod}\, N). \quad (6)$$

Then, we prove the necessity of the theorem. We assume that the adversary recovers the secret key $(\mathbf{b}, \mathbf{r})$. So $\mathbf{b}$ and $\mathbf{r}$ satisfy $\mathbf{a} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} (\mathrm{mod}\, N)$; namely, $\mathbf{a} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} = (\mathbf{r}\mathbf{b}\mathbf{r}^{-1})^e (\mathrm{mod}\, N)$, from which we immediately derive an $e$-th root $\mathbf{r}\mathbf{b}\mathbf{r}^{-1} (\mathrm{mod}\, N) \in \mathbf{H}_N$ for $\mathbf{a} \in \mathbb{H}_N$. □

**Theorem 3.** *Assume that there exists a polynomial-time algorithm $\mathscr{A}$ to break the key security of the proposed quaternion signature scheme. For any quaternion $\mathbf{a} \in \mathbb{H}_N$ such that $\mathbf{a}$ has an $e$-th root in $\mathbb{H}_N$, then there exists a polynomial-time algorithm $\mathscr{B}$ to determine the $e$-root of $\mathbf{a}$.*

*Proof.* We want to construct a polynomial-time algorithm $\mathscr{B}$ such that given the input $(\mathbf{a}, N, e)$, the algorithm $\mathscr{B}$ outputs the $e$-th root for $\mathbf{a} \in \mathbb{H}_N$. To do this, we just need to show that we can derive a public key from $(\mathbf{a}, N, e)$ and then access the algorithm $\mathscr{A}$ to recover the corresponding secret key.

We denote the $e$-th root of $\mathbf{a} \in \mathbb{H}_N$ as $\mathbf{c} \in \mathbb{H}_N$; namely, $\mathbf{c}^e = \mathbf{a} (\mathrm{mod}\, N)$ and $H$ is a hash function. Thus, we randomly choose $\mathbf{r} \in \mathbb{H}_N^*$, and from the proof of Theorem 2 we know that $\mathbf{b} = \mathbf{r}^{-1}\mathbf{c}\mathbf{r} (\mathrm{mod}\, N)$ and $\mathbf{r}$ can serve as the secret key of the signature scheme with the corresponding public key $(\mathbf{a}, N, H, e)$. So the algorithm $\mathscr{B}$ runs as follows. Firstly, $\mathscr{B}$ defines a hash function $H$; then the algorithm $\mathscr{B}$ feeds the public key $(\mathbf{a}, N, H, e)$ into the algorithm $\mathscr{A}$ to obtain the output $(\mathbf{b}, \mathbf{r})$ by the algorithm $\mathscr{A}$. Finally, the algorithm $\mathscr{B}$ computes and outputs $\mathbf{r}\mathbf{b}\mathbf{r}^{-1} (\mathrm{mod}\, N) \in \mathbf{H}_N$. It can be easily verified that $\mathbf{r}\mathbf{b}\mathbf{r}^{-1} (\mathrm{mod}\, N)$ is an $e$-root of $\mathbf{a}$ and that the algorithm $\mathscr{B}$ can be carried out in polynomial time. □

The above theorems say that if the adversary can break the key security of the proposed signature scheme, the adversary can also solve a random instance of the $e$-th root extraction problem over $\mathbb{H}_N$, which seems computationally intractable.

*3.1.2. Partial Key Exposure Attacks.* We discuss the attacks assuming that the adversary knows the quaternion $\mathbf{b}$ or $\mathbf{r}$. If the adversary knows the quaternion $\mathbf{r}$, the adversary can get $\mathbf{b}^e = \mathbf{r}^{-1}\mathbf{a}\mathbf{r} (\mathrm{mod}\, N)$. So the adversary needs to compute the $e$-root of the quaternion $\mathbf{r}^{-1}\mathbf{a}\mathbf{r} \in \mathbb{H}_N$ to derive $\mathbf{b}$, which seems computationally impossible. We also have the following result.

**Theorem 4.** *There exist at least $\phi(N) = (p-1)(q-1)$ quaternions $\mathbf{r} \in \mathbb{H}_N^*$ such that $\mathbf{a} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} (\mathrm{mod}\, N)$. If the adversary knows $\mathbf{b} \in \mathbb{H}_N$, there exists an algorithm $\mathscr{A}$ to compute such an $\mathbf{r}$ at the cost of $\mathcal{O}(\log_2^3 N)$ bit operations.*

*Proof.* Note that the secret keys $\mathbf{b}$ and $\mathbf{r}$ satisfy $\mathbf{a} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} (\mathrm{mod}\, N)$. So we have $\gcd(\|\mathbf{r}\|, N) = 1$. Then, for an integer $\alpha \in \mathbb{Z}_N^*$, if we denote $\mathbf{r}_\alpha = \alpha\mathbf{r} (\mathrm{mod}\, N)$, we must have $\gcd(\|\alpha\mathbf{r}\|, N) = \gcd(\alpha\|\mathbf{r}\|, N) = 1$. So $\mathbf{r}_\alpha \in \mathbb{H}_N^*$ satisfies $\mathbf{r}_\alpha\mathbf{b}^e\mathbf{r}_\alpha^{-1} = \alpha\mathbf{r}\mathbf{b}^e(\alpha\mathbf{r})^{-1} = \alpha\mathbf{r}\mathbf{b}^e\alpha^{-1}\mathbf{r}^{-1} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} = \mathbf{a} (\mathrm{mod}\, N)$. Note that $\mathbb{Z}_N^*$ have $\phi(N) = (p-1)(q-1)$ distinct integers, so we conclude that there exist at least $\phi(N) = (p-1)(q-1)$ quaternions $\mathbf{r} \in \mathbb{H}_N^*$ such that $\mathbf{a} = \mathbf{r}\mathbf{b}^e\mathbf{r}^{-1} (\mathrm{mod}\, N)$.

If the adversary knows $\mathbf{b}$, we know that $\mathbf{a}\mathbf{r} = \mathbf{r}\mathbf{b}^e (\mathrm{mod}\, N)$, from which the adversary can obtain four linear congruences modulo $N$ by associating the constants and the coefficients of $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$. Thus, we solve the linear congruences by using, for example, the Gaussian elimination algorithm to obtain the coefficients of the quaternion $\mathbf{r}$, which only costs $\mathcal{O}(\log_2^3 N)$ bit operations. □

The above theorem says that we must keep $\mathbf{b}$ secret. Otherwise, the adversary can retrieve the whole secret key in polynomial time.

*3.1.3. Signature Forgery Attacks.* Given a message $m$, we discuss the difficulty for the adversary to forge a signature $(\mathbf{u}, \mathbf{t})$ on the message $m$ such that the signature $(\mathbf{u}, \mathbf{t})$ can pass the verification equation $\mathbf{u}^e = \mathbf{t}\mathbf{v}\mathbf{t}^{-1} (\mathrm{mod}\, N)$.

**Theorem 5.** *An adversary can produce a signature $(\mathbf{u}, \mathbf{t})$ on a given message $m$ if and only if he can extract the $e$-th root for $\mathbf{v} = \mathbf{a}^h = \mathbf{a}^{H(m)} (\mathrm{mod}\, N)$.*

*Proof.* We first prove the sufficiency. We assume that the adversary can extract the $e$-th root denoted as $\mathbf{w} \in \mathbb{H}_N$ for $\mathbf{v} = \mathbf{a}^h = \mathbf{a}^{H(m)} (\mathrm{mod}\, N)$; namely, $\mathbf{v} = \mathbf{a}^h = \mathbf{w}^e (\mathrm{mod}\, N)$. The adversary randomly chooses a quaternion $\mathbf{t} \in \mathbb{H}_N^*$ and computes $\mathbf{u} = \mathbf{t}\mathbf{w}\mathbf{t}^{-1} (\mathrm{mod}\, N)$. Note that

$$\mathbf{u}^e = \left(\mathbf{t}\mathbf{w}\mathbf{t}^{-1}\right)^e = \mathbf{t}\mathbf{w}^e\mathbf{t}^{-1} = \mathbf{t}\mathbf{v}\mathbf{t}^{-1}\,(\mathrm{mod}\, N). \quad (7)$$

So $(\mathbf{u}, \mathbf{t})$ can pass the verification equation $\mathbf{u}^e = \mathbf{t}\mathbf{v}\mathbf{t}^{-1} (\mathrm{mod}\, N)$; namely, a valid signature $(\mathbf{u}, \mathbf{t})$ on the message $m$ is forged.

Then, we prove the necessity. If the adversary forges a signature $(\mathbf{u}, \mathbf{t})$ on a given message $m$ satisfying $\mathbf{u}^e = \mathbf{t}\mathbf{v}\mathbf{t}^{-1} (\mathrm{mod}\, N)$, so $\mathbf{v} = \mathbf{t}^{-1}\mathbf{u}^e\mathbf{t} = (\mathbf{t}^{-1}\mathbf{u}\mathbf{t})^e (\mathrm{mod}\, N)$. Thus, an $e$-th root $\mathbf{t}^{-1}\mathbf{u}\mathbf{t} (\mathrm{mod}\, N)$ is determined for the quaternion $\mathbf{v} \in \mathbb{H}_N$. □

The above theorem says that there is only one way for the adversary to forge a signature $(\mathbf{u}, \mathbf{t})$ for a given message $m$, that is, to extract the $e$-th root for the quaternion $\mathbf{v} = \mathbf{a}^h = \mathbf{a}^{H(m)} (\mathrm{mod}\, N)$. However, the $e$-th root extraction problem over $\mathbb{H}_N$ is assumed to be intractable. So it is computationally infeasible to forge a signature for a given message.

*3.2. Performance.* We analyze the performance of related issues.

*3.3. Quaternion Modular Exponentiation Operation.* In the proposed signature scheme, quaternion modular exponentiations are often used. For example, in the signature generation algorithm, we need to compute $\mathbf{b}^h (\mathrm{mod}\, N)$, and in the verification algorithm we also need to compute $\mathbf{v} = \mathbf{a}^h (\mathrm{mod}\, N)$. The quaternion modular exponentiation can be performed via a square-and-multiply approach. To illustrate, we let the

binary representation of $h$ be $h = h_{k-1} \cdots h_1 h_0 = \sum_{i=0}^{k-1} h_i 2^i$ with $h_i = 0$ or 1. Given $\mathbf{b} \in \mathbb{H}_N$, we firstly set $\mathbf{b}_0 = \mathbf{b}$ and compute $\mathbf{b}_i = \mathbf{b}_{i-1}^2 = \mathbf{b}^{2^i} \pmod N$ for $i = 1, \ldots, k-1$. Then, we compute

$$\mathbf{b}^h = \prod_{i=0}^{k-1} \mathbf{b}_i^{h_i} = \prod_{h_i=1} \mathbf{b}_i \pmod N. \tag{8}$$

This is because

$$\mathbf{b}^h = \mathbf{b}^{\sum_{i=0}^{k-1} h_i 2^i} = \prod_{i=0}^{n-1} \mathbf{b}^{h_i 2^i} = \prod_{i=0}^{n-1} \left(\mathbf{b}^{2^i}\right)^{h_i} = \prod_{i=0}^{k-1} \mathbf{b}_i^{h_i} \pmod N. \tag{9}$$

Therefore, to compute $\mathbf{b}^h \pmod N$ we firstly need to do $(k-1)$ quaternion modular multiplications to compute $\mathbf{b}_i$ and then on average $k/2$ quaternion modular multiplications to compute $\prod_{h_i=1} \mathbf{b}_i \pmod N$. The quaternion modular exponentiation $\mathbf{b}^h \pmod N$ needs about $3k/2$ quaternion modular multiplications.

*3.4. Computational Costs.* We consider the computational costs for signing a message and verifying a signature.

In the signature generation phase, we need to do the computations $\mathbf{t} = \mathbf{s}\mathbf{r}^{-1} \pmod N$ and $\mathbf{u} = \mathbf{s}\mathbf{b}^h\mathbf{s}^{-1} \pmod N$ (here we ignore the computational inexpensive hash operations), which are equivalent to 3 quaternion modular multiplications and one quaternion modular exponentiation. According to the aforementioned analysis, the total computations are equivalent about $3 + 3k/2$ quaternion modular multiplications. We recall the quaternion modular multiplicative operation in Section 2.2. One quaternion modular multiplication costs about 16 modular multiplications. However, we note that modular multiplication modulo $N$ achieves a quadratic complexity; namely, $\mathcal{O}(\log_2^2 N) = \mathcal{O}(n^2)$. So the computational complexity for the signature scheme is given as $\mathcal{O}(kn^2)$.

In the verification process, we need to compute $\mathbf{v} = \mathbf{a}^h \pmod N$ (a quaternion modular exponentiation), $\mathbf{u}^e \pmod N$ (two quaternion modular multiplications according to the square-and-multiply approach; namely, $\mathbf{u}_1 = \mathbf{u}^2 \pmod N$ and $\mathbf{u}^e = \mathbf{u}^3 = \mathbf{u}_1\mathbf{u} \pmod N$), and $\mathbf{t}\mathbf{v}\mathbf{t}^{-1} \pmod N$ (two quaternion modular multiplications). So the computational costs are about $4 + 3k/2$ quaternion modular multiplications. Therefore, the computational complexity for the verification algorithm is also $\mathcal{O}(kn^2)$.

## 4. Conclusion

In this paper, a quaternion signature scheme was proposed based on the root extraction problem defined over quaternion algebraic structures. The signature scheme only performs $\mathcal{O}(kn^2)$ bit operations to sign a message and to verify a signature, and hence the proposal is practical. We showed that the key security is equivalent to a random instance of the $e$-th root extraction problem defined over $\mathbb{H}_N$, and the signature forgery security is equivalent to extracting the $e$-th root for the quaternion $\mathbf{v} = \mathbf{a}^h = \mathbf{a}^{H(m)} \pmod N$. Hence, our proposal satisfies some provable security goals.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61173152 and 61173151), the 111 Project (no. B08038), the ISN Foundation (no. ISN1103007), the Fundamental Research Funds for the Central Universities (no. JY10000901009), and the Natural Science Basic Research Plan in Shaanxi Province of China (no. 2012JM8005).

## References

[1] N. Koblitz and A. J. Menezes, "A survey of public-key cryptosystems," *SIAM Review*, vol. 46, no. 4, pp. 599–634, 2004.

[2] Z. Hao, S. Zhong, and N. Yu, "A multihop key agreement scheme for wireless Ad hoc networks based on channel characteristics," *The Scientific World Journal*, vol. 2013, Article ID 935604, 13 pages, 2013.

[3] Q. Zhang, X. Xue, and X. Wei, "A novel image encryption algorithm based on DNA subsequence operation," *The Scientific World Journal*, vol. 2012, Article ID 286741, 10 pages, 2012.

[4] R. Guo, Q. Wen, Z. Jin, and H. Zhang, "An efficient and secure certificateless authentication protocol for healthcare system on wireless medical sensor networks," *The Scientific World Journal*, vol. 2013, Article ID 761240, 7 pages, 2013.

[5] D. N. Moldovyan and N. A. Moldovyan, "A new hard problem over noncommutative finite groups for cryptographic protocols," in *Proceedings of the 5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS '10)*, vol. 6258 of *Lecture Notes in Computer Science*, pp. 183–194, Springer, St. Petersburg, Russia, 2010.

[6] A. A. Kamal and A. M. Youssef, "Cryptanalysis of lvarez et al. key exchange scheme," *Information Sciences*, vol. 223, no. 20, pp. 317–321, 2013.

[7] P. Pan, L. Wang, L. Wang, L. Li, and Y. Yang, "CSP-DHIES: a new public-key encryption scheme from matrix conjugation," *Security and Communication Networks*, vol. 5, no. 7, pp. 809–822, 2012.

[8] G. Baumslag, N. Fazio, A. R. Nicolosi, V. Shpilrain, and W. E. Skeith, "Generalized learning problems and applications to non-commutative cryptography," in *Proceedings of the 5th International Conference on Provable Security (ProvSec '11)*, vol. 6980 of *Lecture Notes in Computer Science*, pp. 324–339, Springer, Xian, China, 2011.

[9] P. Vitkus, E. Sakalauskas, N. Listopadskis, and R. Vitkiene, "Microprocessor realization of key agreement protocol based on matrix power function," *Elektronika ir Elektrotechnika*, no. 1, pp. 33–36, 2012.

[10] D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta, and F. Ulmer, "Key exchange and encryption schemes based on non-commutative skew polynomials," in *Proceedings of the 3rd International Workshop on Post-Quantum Cryptography (PQCrypto '10)*, vol. 6061 of *Lecture Notes in Computer Science*, pp. 126–141, Springer, Darmstadt, Germany, 2010.

[11] J. Climenta, P. R. Navarrob, and L. Tortosab, "Key exchange protocols over noncommutative rings. The case of *End*($\mathbb{Z}_p$ ×

$\mathbb{Z}_{p^2}$)," *International Journal of Computer Mathematics*, vol. 89, no. 13-14, pp. 1753–1763, 2012.

[12] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao, and Y. Yang, "New public key cryptosystems based on non-Abelian factorization problems," *Security and Communication Networks*, vol. 6, no. 7, pp. 912–922, 2013.

[13] L. Gu, Y. Pan, M. Dong, and K. Ota, "Noncommutative lightweight signcryption for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 818917, 10 pages, 2013.

[14] I. Ahshel, M. Anshel, and D. Goldfeld, "An algebraic method for public key cryptography," *Mathematical Research Letters*, vol. 6, pp. 287–291, 1999.

[15] I. Ahshel, M. Anshel, B. Fisher, and D. Goldfeld, "New key agreement protocols in braid group cryptography," in *Proceedings of the Cryptographers Track at RSA Conference on Topics in Cryptology (CT-RSA '01)*, vol. 2020 of *Lecture Notes in Computer Science*, pp. 13–27, Springer, San Francisco, Calif, USA, 2001.

[16] I. Anshel, M. Anshel, and D. Goldfeld, "Non-abelian key agreement protocols," *Discrete Applied Mathematics*, vol. 130, no. 1, pp. 3–12, 2003.

[17] I. Anshel, M. Anshel, and D. Goldfeld, "A linear time matrix key agreement protocol over small finite fields," *Applicable Algebra in Engineering, Communications and Computing*, vol. 17, no. 3-4, pp. 195–203, 2006.

[18] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, and C. Park, "New public key cryptosystem using finite non Abelian groups," in *Proceedings of the Advances in Cryptology (CRYPTO '01)*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 470–485, Springer, Santa Barbara, Calif, USA, 2001.

[19] S. S. Magliveras, D. R. Stinson, and T. Van Thing, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," *Journal of Cryptology*, vol. 15, no. 4, pp. 285–297, 2002.

[20] W. Lempken, T. Van Tran, S. S. Magliveras, and W. Wei, "A public key cryptosystem based on non-abelian finite groups," *Journal of Cryptology*, vol. 22, no. 1, pp. 62–74, 2009.

[21] K. H. Ko, S. J. Lee, and J. H. Cheon, "New public-key cryptosystem using braid groups," in *Proceedings of the Advances in Cryptology (CRYPTO '00)*, vol. 1880 of *Lecture Notes in Computer Science*, pp. 166–183, Springer, Santa Barbara, Calif, USA, 2000.

[22] J. Hughes, "A linear algebraic attack on the AAFG1 braid group cryptosystem," in *Proceedings of the 7th Australasian Conferenc on Information Security and Privacy (ACISP '02)*, vol. 2384 of *Lecture Notes in Computer Science*, pp. 176–189, Springer, Melbourne, Australia, 2002.

[23] S. J. Lee and E. Lee, "Potential weaknesses of the commutator key agreement protocol based on braid groups," in *Proceedings of the Advances in Cryptology (EuroCrypt '02)*, vol. 2332 of *Lecture Notes in Computer Science*, pp. 14–28, Springer, Amsterdam, The Netherlands, 2002.

[24] A. D. Myasnikov and A. Ushakov, "Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key exchange protocol," in *Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC '07)*, vol. 4450 of *Lecture Notes in Computer Science*, pp. 76–88, Springer, Beijing, China, 2007.

[25] A. D. Myasnikov and A. Ushakov, "Cryptanalysis of the Anshel-Anshel-Goldfeld-Lemieux key agreement protocol," *Groups, Complexity, Cryptology*, vol. 1, no. 1, pp. 63–75, 2009.

[26] C. Tobias, "Security analysis of the MOR cryptosystem," in *Proceedings of the 6th International Conference on Practice and Theory in Public-Key Cryptography (PKC '03)*, vol. 2567 of *Lecture Notes in Computer Science*, pp. 175–186, Springer, Miami, Fla, USA, 2002.

[27] I. Lee, W. Kim, D. Kwon, S. Nahm, N. Kwak, and Y. Baek, "On the security of MOR public key cryptosystem," in *Proceedings of Advances in Cryptology (AsiaCrypt '04)*, vol. 3329 of *Lecture Notes in Computer Science*, pp. 387–400, Springer, Jeju Island, Korea, 2004.

[28] A. Korsten, "Cryptanalysis of MOR and discrete logarithms in inner automorphism groups," in *Proceedings of the 2nd Western European Worksho on Research in Cryptology (WEWoRC '07)*, vol. 4954 of *Lecture Notes in Computer Science*, pp. 78–89, Springer, Bochum, Germany, 2008.

[29] J. Bohli, R. Steinwandt, M. I. G. Vasco, and C. Martínez, "Weak keys in MST 1," *Designs, Codes, and Cryptography*, vol. 37, no. 3, pp. 509–524, 2005.

[30] S. R. Blackburn, C. Cid, and C. Mullan, "Cryptanalysis of the MST3 public key cryptosystem," *Journal of Mathematical Cryptology*, vol. 3, no. 4, pp. 321–338, 2009.

[31] M. I. G. Vasco, A. L. P. Del Pozo, and P. T. Duarte, "A note on the security of MST 3," *Designs, Codes, and Cryptography*, vol. 55, no. 2-3, pp. 189–200, 2010.

[32] J. H. Cheon and B. Jun, "A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem," in *Proceedings of the Advances in Cryptology (CRYPTO '03)*, vol. 2729 of *Lecture Notes in Computer Science*, pp. 212–225, Springer, Santa Barbara, Calif, USA, 2003.

[33] E. Lee and J. H. Park, "Cryptanalysis of the public-key encryption based on braid groups," in *Proceedings of the Advances in Cryptology (EuroCrypt '03)*, vol. 2656 of *Lecture Notes in Computer Science*, pp. 477–490, Springer, Warsaw, Poland, 2003.

[34] A. Myasnikov, V. Shpilrain, and A. Ushakov, "A practical attack on a braid group based cryptographic protocol," in *Proceedings of the Advances in Cryptology (CRYPTO '05)*, vol. 3621 of *Lecture Notes in Computer Science*, pp. 86–96, Springer, Santa Barbara, Calif, USA, 2003.

[35] T. Satoh and K. Araki, "On construction of signature scheme over a certain non-commutative ring," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E80-A, no. 1, pp. 40–45, 1997.

[36] E. Sakalauskas, "New digital signature scheme in Gaussian monoid," *Informatica*, vol. 15, no. 2, pp. 251–270, 2004.

[37] E. Sakalauskas, "One digital signature scheme in semimodule over semiring," *Informatica*, vol. 16, no. 3, pp. 383–394, 2005.

[38] D. Kahrobaei and C. Kouppari, "Non-commutative digital signatures," *Groups, Complexity, Cryptology*, vol. 4, no. 2, pp. 377–384, 2012.

[39] B.-C. Wang and Y.-P. Hu, "Signature scheme based on the root extraction problem over braid groups," *IET Information Security*, vol. 3, no. 2, pp. 53–59, 2009.

[40] L. Wang, L. Wang, Z. Cao, Y. Yang, and X. Niu, "Conjugate adjoining problem in braid groups and new design of braid-based signatures," *Science in China F: Information Sciences*, vol. 53, no. 3, pp. 524–536, 2010.

[41] L. Wang, Z. Cao, P. Zeng, and X. Li, "One-more matching conjugate problem and security of braid-based signatures," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07)*, pp. 295–301, ACM, New York, NY, USA, March 2007.

[42] D. Coppersmith, "Weakness in quaternion signatures," in *Proceedings of the Advances in Cryptology (CRYPTO '99)*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 305–314, Springer, Santa Barbara, Calif, USA, 1999.

[43] D. Coppersmith, "Weakness in quaternion signatures," *Journal of Cryptology*, vol. 14, no. 2, pp. 77–85, 2001.

[44] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Technical Report, Massachusetts Institute of Technology, Cambridge, Mass, USA, 1979.

[45] J. M. Pollard and C. P. Schnorr, "An efficient solution of the congruence $x^2 + ky^2 \equiv m (\mathrm{mod}\, n)$," *IEEE Transactions on Information Theory*, vol. IT-33, no. 5, pp. 702–709, 1987.