International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **3(A)**, March **2012**

 ISSN 1349-4198
pp. 1645–1663

# A NOVEL DIGITAL SIGNATURE SCHEME BASED ON CUBIC RESIDUE WITH PROVABLE SECURITY

Hsiu-Feng Lin[1], Chiou-Yueh Gun[2,3] and Chih-Ying Chen[2]

[1]Department of Information Engineering and Computer Science
[2]Department of Communications Engineering
Feng-Chia University
No. 100, Wen-Hwa Road, Taichung 40724, Taiwan
{ hflin; chihchen }@fcu.edu.tw

[3]Department of Mechanical Engineering
Nan-Kai University of Technology
No. 568, Zhongzheng Road, Caotun Township, Nantou County 54243, Taiwan
moon384@nkut.edu.tw

Received December 2010; revised July 2011

Abstract. *Since a single computationally hard problem today may possibly be solved efficiently in the future, many researchers endeavored in recent years to base their cryptosystem security on solving two or more hard problems simultaneously to enhance the system security. However, it is found that many previously suggested signature schemes with their (1) security based on integer factorization and discrete logarithm problems and with (2) verification equation using exponential quadratic forms were not as secure as claimed and gave no provable security under the random oracle model. We, therefore, use the theory of cubic residues to present a new signature scheme with an exponential cubic verification equation to prevent the attack from Pollard-Schnorr's congruence solutions and give a formal proof of the scheme security by random oracle modeling. We formally prove that, based on solving the discrete logarithm problem with a composite modulus (which has been shown by Bach in 1984 to be exactly as hard as simultaneously solving the integer factorization and the discrete logarithm with a prime modulus), the proposed scheme is resistant against both no-message and adaptively chosen-message attacks.*

**Keywords:** Cubic residue, Discrete logarithm problem with a composite modulus, Provable security, Random oracle model

1. **Introduction.** In 1976, the concept of digital signatures with a public-key cryptosystem (PKC) was proposed by Diffie and Hellman [1]. Although several other researchers such as Rivest-Shamir-Adleman (RSA) [2], Rabin [3], Ong et al. [4], ElGamal [5] and Schnorr et al. [6] followed up with alternative schemes, they all shared the same trait of relying on only one computationally infeasible mathematical problem, e.g., the discrete logarithm problem (DLP) or integer factorization problem (FAC), for their security. Even though the assumption that the single underlying mathematical problem is computationally infeasible remains mostly valid today, it may diminish in the future because of the possibility of great progress in efficiency of problem solving algorithms or ability of computing systems, which is a fact that many experts fear will soon render the current single-problem schemes inaptly insecure. This has led many authors to come up with PKC schemes based on multiple hard problems [7-12] to avoid the increasing security risk.

The first design that emerged from this new school of multiple-hard-problem signature schemes was a key distribution scheme by McCurley [13] in 1988. Ever since McCurley's

proposal, several variants have also been suggested. In 1992, for example, Brickell and McCurley [9] constructed an interactive identification scheme in which the security was based on both discrete logarithm and factorization. Harn [8] did the same in his new signature scheme that combined RSA [2] and ElGamal [5] signature schemes, which, unfortunately, was later discovered in 1996 by Lee and Hwang [14] to be flawed since the integrity of the signature could be compromised if its discrete logarithm was solved. In 1997, Laih and Kuo [15] also presented a new signature scheme that was also based on two hard problems. However, their scheme suffered from large computational and memory requirements for key production.

In 1998, Shao [11] also proposed two two-hard-problem digital signature schemes. However, Li and Xiao [16] revealed that the two schemes were insecure. If one valid signature is known, the attacker can forge a valid signature for any message. Furthermore, in 1999, Lee [17] also demonstrated that Shao's schemes could be broken if the factorization problem was solved because the signer's secret key could be recovered with a known signature.

He [12] in 2001 proposed a scheme intended to overcome the weakness in Shao's design. However, Sun [18] indicated that He's scheme was only discrete logarithm based. Although Hwang et al. [19] proposed a scheme to improve the efficiency of He's scheme, in the same year, Ding and Laih [20] and Shao [21] also found that He's scheme was not as secure as claimed.

Like He, Tzeng et al. [22] in 2004 proposed a new scheme said to be more optimal than Shao's [21], which he demonstrated to be resistant to at least three forms of attacks. Shao [23], however, argued that, contrary to the claim, the new scheme of Tzeng et al. [22] was vulnerable to signature forging using a probabilistic algorithm by Pollard and Schnorr [24] if the solutions to the discrete logarithm problems were found. In addition, the private keys of legal signers may also be recovered if the attacker could successfully factor the composite number. In the same year, Chang et al. [25] also attempted an improvement since they claimed He's scheme [12] contained a flaw in which not only could the forgers forge valid signatures, but a public key might also have more than one corresponding secret key.

In 2007, Lin et al. [26] presented an improvement on Shao's signature schemes [11] and showed that it was tamper-resistant to Lee's attack [17]. However, to forge a valid signature for a given message using Lin et al.'s method [26], the attacker would only have to solve the factorization problem.

Using the quadratic residues theory, Wei [27] also improved Shao's schemes in 2007 to propose two new schemes based on two hard problems. Yet, Zheng et al. [28] in 2008 broke the Wei's digital signature schemes: the attacker can forge signatures for any arbitrary message without any knowledge about the private keys. More recently, Lin et al. [29] found another vital flaw in Wei's digital signature schemes from its exponential quadratic form based verification equation. One can forge a valid signature of any message by using Pollard-Schnorr's method [24], and neither the discrete logarithm nor the factoring problem needed to be solved.

From the discussion above, we see that many of the published signature schemes based on both factorization and discrete logarithm problems have suffered from security flaws and that, in addition, seldom gave provable security using a random oracle.

Among these schemes, it is also found that some signature schemes having their verification equations based on exponential quadratic form can be easily defeated by the method of Pollard-Schnorr's congruence solution. Such flawed signature schemes include Ong et al. [4] in 1984, Shao in 1998, He in 2001, Tzeng in 2004 and Wei in 2007, etc. The design in this paper, therefore, will extend the verification equation from exponential quadratic form to the cubic form by taking advantage of the cubic residue theory, which

forms the core for a new digital signature that will be discussed in the following sections. The security in our proposed scheme is based on solving the discrete logarithm with a composite modulus, which has been shown by Bach [30] in 1984 to be exactly as hard as simultaneously solving the integer factorization problem and the discrete logarithm problem with a prime modulus. The Random Oracle modeling and the Forking Lemma technique by Pointcheval-Stern [31] will be used to demonstrate the security strength of the proposed scheme.

The structure of this paper is organized as follows. Section 2 reviews the definition of provable security and the random oracle model. In Section 3, we will introduce some mathematical properties of cubic residues that will be used to create an environment suitable for our signature scheme in the next section. Section 4 describes the proposed signature scheme, where Section 5 explains why our verification equation in exponential cubic form can be immune to Pollard-Schnorr's [24] congruence solution attack. It also provides a security proof against existential forgery under no-message as well as adaptive chosen-message attacks under the random oracle model. Finally, concluding remarks are given in Section 6.

## 2. **The Concept of Provable Security.** In this section, we will first review the concept of provable security of signature schemes and then the random oracle model.

### 2.1. **Provable security.** In order to safeguard information from possible malicious attackers, information security has become the main field of research aimed to solve such issues. We usually illustrate the security of a digital signature system via the technique of problem reduction, and in order to prove that a signature scheme S is indeed secure, we must refer to:

1). Clearly define what the security of the signature system is.
2). Describe what related information of the system an attacker may request to obtain when attacking a scheme S.
3). Select an acknowledged computationally hard problem H.
4). Reduce "solving this hard problem H" to "breaking the scheme S". This means that if one can break the scheme S then he can solve the hard problem H by using the same breaking algorithm.

From the security aspect, some cryptographic algorithms and protocols today offer few securities. Cryptographic schemes usually follow a development cycle of trial-and-error at the expense of individual and corporate users. To provide an even more reliable cryptosystem security measure, security implementers are increasingly demanding mathematically proven guarantees.

That a given digital signature scheme is proven secure often refers to the accepted assumption that the underlying mathematical algorithms are sufficiently 'hard' to solve – which implies the protection of data. Digital signature algorithms typically include computing the discrete logarithm, factoring a composite number, inverting the RSA function [2] and computing the Diffie-Hellman problem [1], etc. Although the relationship between provable security and the complexity theory has yet to be fully understood, most modern security proofs accept this reduction approach that relies on the assumption of the hardness of the aforementioned mathematical problems [32]. Provable security is of course not completely secure, but it is the most acceptable level of security for the time being.

The standard security definition of signature schemes was given by Pointcheval and Stern [33]. There are two specific kinds of attacks against signature schemes: the no-message attack and the known-message attack. In the first scenario, the attacker only knows the public key of the signer; in the second one, the attacker has access to a list

of message-signature pairs. The strongest known-message attack is called the adaptively chosen-message attack, in which the attacker can ask the signer to sign any message if he has knowledge of the signer's public key. He can then adapt his queries according to previous message-signature pairs.

2.2. **Random oracle.** There are many real world random functions whose inputs and outputs defy statistical correlations. An ideal application for these random functions is the production of digital signatures. In the context of cryptographic proof, random oracles are often used in place of real life random hash functions, i.e., if a scheme is proven secure under the random oracle model, it is believed to be equally as secure when hash functions are used in its place.

In 1993, Bellare and Rogaway [34] proposed the random oracle paradigm in which a theoretical random function $h$ that maps each input to a truly random output was used for cryptographic proofs. In practice, however, $h$ is set to some specific function derived in some way from a standard cryptographic hash function H like SHA-1, MD5, RIPEMD-160 or others. Bellare and Rogaway claimed that the random oracle model was efficient and guaranteed security. Although the random oracle model is not at the same level as those of the standard provable security approach, it is arguably superior to those provided by totally ad hoc protocol design, provided that the instantiating function $h$ was carefully chosen. Bellare and Rogaway conjectured that the resulting protocol was secure as long as the protocol and the hash function were sufficiently independent.

However, many experts questioned Bellare and Rogaway's random oracle model. Canetti et al. [35], for instance, demonstrated in 2004 that it was possible to have a scheme proven secure under the random oracle model and yet insecure when a specific hash function was used. Pointcheval and Stern [33] also showed how a scheme proven secure under the random oracle model could have its discrete logarithm problem solved by the oracle replay attack using the Forking Lemma technique.

For a digital signature scheme to be proven secure under the random oracle model, it generally needs to have the following properties by referring to [36].

1). The random oracle model assumes a publicly accessible oracle that everyone can access (it is callable to all participants in the scheme), including the signer, the verifier and the attacker.
2). In order for a given scheme to be secure, one must prove, using the problem reduce method under the random oracle model, that "if there exists at least one attacker with a non-negligible probability of success of breaking the scheme in question, then it is also true that the attacker can execute a algorithm of his own design with a non-negligible probability of success in solving the underlying mathematical algorithm of the scheme".
3). From a theoretical point of view, no (efficiently-computable) hash function can possibly be a random function. In reality, a cryptographic hash function is instantiated as the random oracle (the random oracle model is regarded as a bridge between theory and practice).
4). From a practical point of view, it is better to have a construction that can be proven secure in the random oracle model than to have a construction with no proof at all.
5). The theoretical random oracle model and a sufficiently random hash function are computationally interchangeable.

A scheme will only fit the framework of provable security under the random oracle model if it satisfies all of the above conditions. Although highly theoretical and not absolutely guaranteed, the security proof under the random oracle model still gives the

users a higher degree of confidence not afforded by most traditional designs. This is why the random oracle model is widely viewed as a bridge between theory and practice.

3. **The Concept and Mathematical Properties of Cubic Residues.** We will first introduce the definition and several important properties of cubic residues, since our proposed scheme in Section 4 is also based on cubic residues. In this section, we will briefly review some number theory propositions related to cubic residues. Propositions 3.1 to 3.6 are some basic properties about residue numbers, where the proofs can be found in [37].

3.1. **Cubic residue class ring over $Z[\omega]$.** Let $Z$ denote the ring of integers, i.e., the set of 0, $\pm 1$, $\pm 2$, $\cdots$ together with the usual definition of addition and multiplication, and let $\omega = \frac{-1+\sqrt{-3}}{2}$. Consider the set $D = Z[\omega] = \{a + b\omega | a, b \in Z\}$ and define $(a+b\omega)+(c+d\omega) = (a+c)+(b+d)\omega$ and $(a+b\omega)(c+d\omega) = (ad-bd)+(ad+bc-bd)\omega$, for all $a + b\omega$, $c + d\omega \in D$, then $D$ is a ring. If $\alpha = a + b\omega \in D$, then $\bar{\alpha} = a + b\bar{\omega} = a + b\omega^2 = (a-b) - b\omega \in D$, here $\bar{\alpha}$ means a complex conjugate of $\alpha$. For $\alpha = a + b\omega \in D$, we define the norm of $\alpha$ as $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 - ab$. Then, $D$ is a Euclidean domain under norm $N$ and $\alpha \in D$ is a unit iff $N(\alpha) = 1$. Thus, the units in $D$ are $\pm 1$, $\pm\omega$ and $\pm(1 + \omega)$. This implies that it is also a principle ideal domain and then an unique factorization domain, i.e., every element can be decomposed into a product of irreducible elements uniquely up to a unit element. Note that the primes in $Z$ need not be primes in $D$. For example, $7 = (3 + \omega)(2 - \omega)$. To avoid some confusion, we shall call the primes in $Z$ rational primes and refer to those in $D$ simply as primes. The following Propositions 3.1 to 3.6 are quoted from [39].

**Proposition 3.1** (Proposition 9.1.3. [37]). *If $\pi \in D$ such that $N(\pi) = p$ is a rational prime, then $\pi$ is a prime in $D$.*

**Proposition 3.2** (Proposition 9.1.4. [37]). *Suppose that $p \equiv 1 \bmod 3$ is a rational prime, then $p = N(\pi) = \pi\bar{\pi}$ where $\pi$ is a prime in $D$.*

If $\alpha$, $\beta$, $\gamma \in D$ and $\gamma \neq 0$ is not a unit, we say that $\alpha$ is congruent to $\beta$ modulo $\gamma$ if $\gamma | \alpha - \beta$, where we write $\alpha \equiv \beta \bmod \gamma$. Just as in $Z$, the congruence classes modulo $\gamma$ made into a ring $D_\gamma = D/\gamma D$ is called the residue class ring modulo $\gamma$.

**Proposition 3.3** (Proposition 9.2.1. [37]). *Let $\pi \in D$ be a prime, then $D_\pi := D/\pi D$ is a finite field with $N(\pi)$ elements.*

Let $\pi$ be a prime in $D$. Then, $D_\pi^*$, the multiplicative group of $D_\pi$, forms a cyclic group with $N(\pi)-1$ elements. The following proposition is similar to the famous Fermat's Little Theorem.

**Proposition 3.4** (Proposition 9.3.1. [37]). *Let $\pi \in D$ be a prime and $\alpha \in D$. If $\pi \nmid \alpha$, then $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$.*

If $N(\pi) \neq 3$, it is easily seen that the residue class of 1, $\omega$, $\omega^2$ are distinct in $D_\pi$. Consequently, we have the following proposition.

**Proposition 3.5** (Proposition 9.3.2. [37]). *Suppose that $Z_m$ is a prime in $D$ such that $N(\pi) \neq 3$ and $\alpha \in D$ such that $\pi \nmid \alpha$, then there is a unique integer $m = 0$, 1 or 2 such that $\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \bmod \pi$.*

**Definition 3.1.** *If $\pi$ is a prime in $D$ such that $N(\pi) \neq 3$ and $\alpha \in D$, the cubic residue character of $\alpha$ modulo $\pi$, denoted as $\left(\frac{\alpha}{\pi}\right)_3$, is given by*

(a) $\left(\frac{\alpha}{\pi}\right)_3 = 0$ *if* $\pi|\alpha$.
(b) $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \bmod \pi$ *if* $\pi \nmid \alpha$.

Notice that with Proposition 3.5, $\left(\frac{\alpha}{\pi}\right)_3 = \omega^m$, $m = 0$, 1 or 2, if $\pi \nmid \alpha$.

We say that $\alpha$ is a cubic residue mod $\pi$ if $x^3 \equiv \alpha \bmod \pi$ is solvable. The cubic residue character plays the same role in the theory of cubic residues as the Legendre symbol does in the theory of quadratic residues.

**Proposition 3.6** (Proposition 9.3.3. [37])**.** *Let $\pi$ be a prime in $D$ such that $N(\pi) \neq 3$ and $\alpha, \beta \in D$. Then,*
(a) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *iff $\alpha$ is a cubic residue.*
(b) $\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \bmod \pi$.
(c) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.
(d) *If* $\alpha \equiv \beta \bmod \pi$, *then* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

3.2. **Cubic residue mod *pq*.** Suppose that $p$ and $q$ are distinct rational primes. If $p \equiv 1 \bmod 3$ and $q \equiv 1 \bmod 3$, then by Proposition 3.2, there are two primes $\pi$ and $\pi'$ in $D$ such that $p = N(\pi) = \pi\bar{\pi}$ and $q = N(\pi') = \pi'\bar{\pi}'$. In the following theorem, we want to show that $D_{\pi\pi'}$ is ring isomorphic to $Z_{pq}$.

**Theorem 3.1.** *Let $p \equiv 1 \bmod 3$ and $q \equiv 1 \bmod 3$ be distinct rational primes. Let $\pi$ and $\pi'$ be two primes in $D$ such that $p = N(\pi) = \pi\bar{\pi}$ and $q = N(\pi') = \pi'\bar{\pi}'$, respectively. Then, $D_{\pi\pi'}$ is ring isomorphic to $Z_{pq}$.*

**Proof:** Since $p \equiv 1 \bmod 3$ and $q \equiv 1 \bmod 3$ are distinct rational primes, by Proposition 3.2, there are two primes $\pi = a_1 + b_1\omega$ and $\pi' = a_2 + b_2\omega$ in $D$ such that $p = N(\pi) = \pi\bar{\pi}$ and $q = N(\pi') = \pi'\bar{\pi}'$. Let $\gamma = \pi\pi' = a_3 + b_3\omega$, so $N(\gamma) = N(\pi\pi') = N(\pi) \cdot N(\pi') = pq$. Note that $\gcd(b_3, pq) = 1$. Since $pq = N(\gamma) = a_3^2 + b_3^2 - a_3b_3 > |a_3b_3| \geq |b_3|$ implies $\gcd(b_3, pq) \neq pq$, if $\gcd(b_3, pq) = p$(or $q$) then $p|\, a_3$ and $p|\, \gamma$ so that $p^2|\, \gamma\bar{\gamma} = pq$, which is impossible. Accordingly, for every $u = m + n\omega \in D$, there is a unique element $c \in Z_{pq}$ such that $cb_3 \equiv n \bmod pq$; that is, $u - c\gamma \equiv m - ca_3 \bmod pq$ and $u \equiv m - ca_3 \bmod \gamma$.

Since $m - ca_3$ is a rational integer, we may define a mapping $\phi$ from $D$ into $Z_{pq}$ by $\phi(u) = m - ca_3 \bmod pq$, where $u = m + n\omega \in D$ and $c$, $a_3$ are defined as the above. Firstly, we show that $\phi$ is well defined, namely, for $u, u' \in D$, if $u = u'$ we have $\phi(u) = \phi(u')$. Let $u \equiv r \bmod \gamma$ and $u' \equiv r' \bmod \gamma$. If $u = u'$, then $r \equiv r' \bmod \gamma$ and there exists a $\alpha \in D$ such that $r - r' = \alpha\gamma$. Since $N(r - r') = (r - r')^2 = N(\alpha)N(\gamma) = pqN(\alpha)$, and $p$, $q$ are rational primes, we have $pq|r - r'$, which implies $r \equiv r' \bmod pq$. We thus have $\phi(u) = r \bmod pq \equiv r' \bmod pq = \phi(u')$.

Secondly, it is obvious that $\phi$ is a ring homomorphism.

Thirdly, we show that $\phi$ is onto as follows. For any $r \in Z_{pq}$, since $\gcd(a_3, pq) = 1$, we may solve $ca_3 \equiv m - r \bmod pq$ for some $c$, where $m$ is any rational integer. Let $u = m + n\omega \in D$, where $n \equiv cb_3 \bmod pq$. Then, $u - c\gamma \equiv r \bmod pq$, and thus, $u \equiv r \bmod \gamma$. Accordingly, by the definition of $\phi$, $\phi(u) = r$ means that $\phi$ is onto.

Finally, since the kernel of $\phi$ is

$$\text{Ker } \phi = \{m + n\omega \in D \,|\phi(m + n\omega) = 0\}$$

$$
\begin{aligned}
&= \{m + n\omega \in D \,|m - ca_3 \equiv 0 \bmod pq \text{ and } n \equiv cb_3 \bmod pq\} \\
&= \{m + n\omega \in D \,|m + n\omega = c(a_3 + b_3\omega) = c\,\gamma\} \\
&= \gamma D,
\end{aligned}
$$

by the ring isomorphism theorem $D_{\pi\pi'} = D_\gamma = D/\gamma D = D/\mathrm{Ker}\phi$, $\phi$ induces the ring isomorphism $\bar{\phi} : D_{\pi\pi'} \to Z_{pq}$ defined by $\bar{\phi}(u + \pi\pi' D) = \phi(u)$ for all $u \in D$ so that $D_{\pi\pi'}$ and $Z_{pq}$ are ring isomorphic.

Since $D_{\pi\pi'}$ is ring isomorphic to $Z_{pq}$, we infer that $D_{\pi\pi'}$ has $N(\pi\pi') = pq$ elements.

Furthermore, in the proof of Theorem 3.1, we have shown that each element of $D$ is congruent to a rational integer mod $\pi\pi'$ in $D_{\pi\pi'}$, say $r$ mod $\pi\pi'$, which is then mapped to $r$ mod $pq$ in $Z_{pq}$ to establish the isomorphism between $D_{\pi\pi'}$ and $Z_{pq}$. Accordingly, we may identify $r$ mod $\pi\pi'$ in $D_{\pi\pi'}$ as $r$ mod $pq$ in $Z_{pq}$.

Similarly, by mapping the coset of a rational integer $\gamma$ in $D^*_{\pi\pi'}$ to the coset of $r$ in $Z^*_{pq}$, we have the following corollary.

**Corollary 3.1.** *$D^*_{\pi\pi'}$ and $Z^*_{pq}$ are multiplicative group isomorphic. Furthermore, $D^*_{\pi\pi'}$ has $[N(\pi) - 1] \times [N(\pi') - 1] = (p-1)(q-1)$ elements.*

Since $\pi(\pi')$ is a prime in $D$, by Proposition 3.3, $D_\pi(D_{\pi'})$ is a finite field with $N(\pi) = \pi\bar{\pi} = p(N(\pi') = \pi'\bar{\pi}' = q)$ elements. We observe that $D_\pi$ and $Z_p$, $D_{\pi'}$ and $Z_q$, $D^*_\pi$ and $Z^*_p$, $D^*_{\pi'}$ and $Z^*_q$ are also isomorphic, respectively.

Since, by Theorem 3.1, each element $u$ of $D$ is congruent to a rational integer $r$ mod $\pi\pi'$, we may suppose that $\omega \equiv e \bmod \pi\pi'$, where $e$ is a rational integer. Thus, $\omega \equiv e_1 \bmod \pi$ and $\omega \equiv e_2 \bmod \pi'$, where $e_1 \equiv e \bmod \pi$ and $e_2 \equiv e \bmod \pi'$. Furthermore, since $D_\pi(D_{\pi'})$ and $Z_p(Z_q)$ are isomorphic, we may identify $\omega \equiv e_1 \bmod \pi$ in $D_\pi$ and $\omega \equiv e_2 \bmod \pi'$ in $D_{\pi'}$, as $e \equiv e_1 \bmod p$ in $Z_p$ and $e \equiv e_2 \bmod q$ in $Z_q$, respectively. In addition, by using the cubic residue character $\left(\frac{u}{\pi}\right)_3 \equiv \omega^i \bmod \pi \equiv e_1^i \bmod \pi$ in $D^*_\pi$ and $\left(\frac{u}{\pi'}\right)_3 \equiv \omega^i \bmod \pi' \equiv e_2^i \bmod \pi'$ in $D^*_{\pi'}$, $i = 0, 1, 2$, we may define the cubic residue character $\left(\frac{r}{p}\right)_3 \equiv e_1^i \bmod p$ in $Z^*_p$ and $\left(\frac{r}{q}\right)_3 \equiv e_2^i \bmod q$ in $Z^*_q$, $0 \le i \le 2$ where $r = \phi(u)$ of Theorem 3.1. In addition, it can be pointed out that the characters of the cubic residue play the same role in the theory of cubic residues as the Legendre symbols do in the theory of quadratic residues.

Now, let $Z_{i,j}(pq) = \left\{ r \in Z^*_{pq} \middle| \left(\frac{r}{p}\right)_3 \equiv e_1^i \bmod p, \left(\frac{r}{q}\right)_3 \equiv e_2^j \bmod q \right\}$ for $0 \le i,\ j \le 2$, then $Z^*_{pq}$ can be divided into nine disjoint equivalence classes; that is $Z^*_{pq} = \bigcup_{i=0}^{2} \bigcup_{j=0}^{2} Z_{i,j}(pq)$, and each $Z_{i,j}(pq)$ has $\frac{1}{9}(p-1)(q-1)$ elements. Furthermore, $r \in Z^*_{pq}$ is a cubic residue mod $pq$ if and only if $r \in Z_{0,0}(pq)$.

In the following paragraphs, we will focus our attention on how to obtain a representative value $c_{i,j}$ from $Z_{i,j}(pq)$ for $0 \le i,\ j \le 2$. This will be beneficial for the application of Theorem 3.2 we will give later on.

Note first that in the RNS (Residue Number System), an integer $r$ is represented according to a basis $B = \{p, q\}$ of two relatively primes modului by the ordered pair $\langle r_1, r_2 \rangle$ where $r_1 \equiv r \bmod p$, $r_2 \equiv r \bmod q$ are positive integers. The Chinese Remainder Theorem ensures the uniqueness of this representation within the range $0 \le r < pq$. If $x$ and $y$ are given in the RNS of the form $\langle x_1, x_2 \rangle$ and $\langle y_1, y_2 \rangle$ respectively, one has

$$
\begin{aligned}
x \pm y \bmod pq &= \langle x_1 \pm y_1 \bmod p, x_2 \pm y_2 \bmod q \rangle \\
xy \bmod pq &= \langle x_1 y_1 \bmod p, x_2 y_2 \bmod q \rangle.
\end{aligned}
$$

Let $p \equiv 1 \bmod 3$, $q \equiv 1 \bmod 3$ be distinct rational primes, and let $\pi = a_1 + b_1\omega$, $\pi' = a_2 + b_2\omega$ be primes in $D$ such that $p = N(\pi) = \pi\bar{\pi}$ and $q = N(\pi') = \pi'\bar{\pi}'$ according

to Theorem 3.1. Then, $\omega \equiv e_1 \bmod \pi$ and $\omega \equiv e_2 \bmod \pi'$, where $e_1 = -a_1 b_1^{-1}$ and $e_2 = -a_2 b_2^{-1}$. Therefore, we have $\left(\frac{r}{p}\right)_3 \equiv e_1^i \bmod p$ and $\left(\frac{r}{q}\right)_3 \equiv e_2^i \bmod q$, $0 \leq i \leq 2$, for all $r \in Z_{pq}^*$.

Because $p \equiv 1 \bmod 3$, $q \equiv 1 \bmod 3$ and $\omega^3 = 1$, therefore, $\left(\frac{e_1}{p}\right)_3 = 1, e_1, e_1^2$ whenever $p \equiv 1 \bmod 9$, $p \equiv 4 \bmod 9$ and $p \equiv 7 \bmod 9$, respectively. In the same way, we obtain the same results for $\left(\frac{e_2}{q}\right)_3$. By pairing $p$ and $q$, we have a total of 9 possible cases which will be discussed below.

In particular, if we put $p \equiv q \equiv 4 \bmod 9$, then $\left(\frac{e_1}{p}\right)_3 = e_1$ and $\left(\frac{e_2}{q}\right)_3 = e_2$. Thus, if we set $c_{i,j} = \langle e_1^i, e_2^j \rangle$ (in RNS representation with base $B = \{p, q\}$), obviously, we have $c_{i,j} \in Z_{i,j}(pq)$, $0 \leq i, j \leq 2$. Generally speaking, this is the most popularly used case.

In the case $p \equiv q \equiv 7 \bmod 9$, we have results similar to the paragraph above where $p \equiv q \equiv 4 \bmod 9$.

Note that if $p \equiv 1 \bmod 9$ or $q \equiv 1 \bmod 9$, then $\left(\frac{e_1}{p}\right)_3 = 1$ or $\left(\frac{e_2}{q}\right)_3 = 1$. In this particular case, we must use the alternative method as follows.

Let $p = 3^{t+1}k + 1$ for some $t \geq 1$ and $3 \nmid k$. First, after solving the equation $a_1^{3^t} \equiv e_1 \bmod p$ (note that $\left(\frac{e_1}{p}\right)_3 = 1$ implies that $e_1$ is a cubic residue $\bmod p$), we have $\left(\frac{a_1}{p}\right)_3 \equiv a_1^{\frac{p-1}{3}} \bmod p \equiv a_1^{3tk} \bmod p \equiv e_1^k \bmod p = e_1$ or $e_1^2 \bmod p$. In the same way, let $q \equiv 3^{t'+1}k'+1$, for some $t' \geq 1$ and $3 \nmid k'$, and we obtain the same result $\left(\frac{a_2}{q}\right)_3 \equiv e_2$ or $e_2^2 \bmod q$, for some $a_2$ which satisfies $a_2^{3^{t'}} \equiv e_2 \bmod q$.

The following table lists a set of representative elements for each possible class of $Z_{pq}^*$ under the condition $p \equiv 1 \bmod 3$ and $q \equiv 1 \bmod 3$. Since the values of $c_{i,j}$ in each row are determined from the previously discussed results, they can only be one of the possible answers for that given row.

TABLE 1. The representative elements for each possible class of $Z_{pq}^*$

| Classification | $c_{i,j} \in Z_{i,j}(pq)$, $0 \leq i, j \leq 2$ |
|---|---|
| $p \equiv 1 \bmod 9$, $q \equiv 1 \bmod 9$ | $c_{i,j} = \langle a_1^i, a_2^j \rangle$, $\langle a_1^i, a_2^{2j} \rangle$, $\langle a_1^{2i}, a_2^j \rangle$ or $\langle a_1^{2i}, a_2^{2j} \rangle$ |
| $p \equiv 1 \bmod 9$, $q \equiv 4 \bmod 9$ | $c_{i,j} = \langle a_1^i, e_2^j \rangle$ or $\langle a_1^{2i}, e_2^j \rangle$ |
| $p \equiv 1 \bmod 9$, $q \equiv 7 \bmod 9$ | $c_{i,j} = \langle a_1^i, e_2^{2j} \rangle$ or $\langle a_1^{2i}, e_2^{2j} \rangle$ |
| $p \equiv 4 \bmod 9$, $q \equiv 1 \bmod 9$ | $c_{i,j} = \langle e_1^i, a_2^j \rangle$ or $\langle e_1^i, a_2^{2j} \rangle$ |
| $p \equiv 4 \bmod 9$, $q \equiv 4 \bmod 9$ | $c_{i,j} = \langle e_1^i, e_2^j \rangle$ |
| $p \equiv 4 \bmod 9$, $q \equiv 7 \bmod 9$ | $c_{i,j} = \langle e_1^i, e_2^{2j} \rangle$ |
| $p \equiv 7 \bmod 9$, $q \equiv 1 \bmod 9$ | $c_{i,j} = \langle e_1^{2i}, a_2^j \rangle$ or $\langle e_1^{2i}, a_2^{2j} \rangle$ |
| $p \equiv 7 \bmod 9$, $q \equiv 4 \bmod 9$ | $c_{i,j} = \langle e_1^{2i}, e_2^j \rangle$ |
| $p \equiv 7 \bmod 9$, $q \equiv 7 \bmod 9$ | $c_{i,j} = \langle e_1^{2i}, e_2^{2j} \rangle$ |

It is known in the theory of quadratic residues that for any $r \in Z_{pq}^*$, there is another $c \in Z_{pq}^*$ such that $rc$ is a quadratic residue. In cubic residues, we have a similar inference as follows.

**Theorem 3.2.** *Let $p \equiv 1 \bmod 3$, $q \equiv 1 \bmod 3$ be two distinct rational primes. For each $r \in Z_{pq}^*$, there exists a $c \in Z_{pq}^*$ such that $rc$ is a cubic residue* $\bmod pq$.

**Proof:** Suppose that $r \in Z_{i,j}(pq)$ for some $0 \le i,\ j \le 2$. Then, $\left(\frac{r}{p}\right)_3 \equiv e_1^i \bmod p$ and $\left(\frac{r}{q}\right)_3 \equiv e_2^j \bmod q$. For this pair $(i,j)$, there exists a pair $(i',j')$ $0 \le i',j' \le 2$, such that $i+i' \equiv 0 \bmod 3$ and $j+j' \equiv 0 \bmod 3$. Choose one $c \in Z_{i',j'}(pq)$, then $\left(\frac{c}{p}\right)_3 \equiv e_1^{i'} \bmod p$ and $\left(\frac{c}{q}\right)_3 \equiv e_2^{j'} \bmod q$. Therefore, $\left(\frac{rc}{p}\right)_3 = \left(\frac{r}{p}\right)_3 \left(\frac{c}{p}\right)_3 = e_1^{i+i'} \equiv 1 \bmod p$ and $\left(\frac{rc}{q}\right)_3 = \left(\frac{r}{q}\right)_3 \left(\frac{c}{q}\right)_3 = e_1^{j+j'} \equiv 1 \bmod q$. Accordingly, $rc \in \mathrm{Z}_{0,0}(pq)$ is, therefore, a cubic residue mod$pq$.

Based on the theorem above, we conclude that if $r \in Z_{pq}^* \cap Z_{i,j}(pq)$ for any $0 \le i,\ j \le 2$, then there exists $c_{i',j'} \in Z_{i',j'}(pq)$ with $i+i' \equiv 0 \bmod 3$ and $j+j' \equiv 0 \bmod 3$ such that $rc_{i',j'}$ is a cubic residue mod$pq$. The above discussions can be illustrated by the following small example.

**Example 3.1.** *Let $p = 7 = 3 \times 2 + 1$, $q = 13 = 3 \times 4 + 1$ be two distinct rational primes. Then, $p = \pi\bar{\pi} = (3+2\omega)(3+2\bar{\omega})$, $q = \pi'\bar{\pi}' = (4+\omega)\cdot(4+\bar{\omega})$ and $p \equiv q \equiv 1 \bmod 3$. We, therefore, have $e_1 = -3 \cdot 2^{-1} \equiv 2 \bmod 7$, $e_2 = -4 \cdot 1^{-1} \equiv 9 \bmod 13$. Since*

$$
\begin{aligned}
Z_0(7) &= \left\{r \in Z_7^* \middle| \left(\tfrac{r}{7}\right)_3 = 2^0\right\} = \{1,6\}, \quad & Z_0(13) &= \left\{r \in Z_{13}^* \middle| \left(\tfrac{r}{13}\right)_3 = 9^0\right\} = \{1,5,8,12\},\\
Z_1(7) &= \left\{r \in Z_7^* \middle| \left(\tfrac{r}{7}\right)_3 = 2^1\right\} = \{4,3\}, \quad & Z_1(13) &= \left\{r \in Z_{13}^* \middle| \left(\tfrac{r}{13}\right)_3 = 9^1\right\} = \{4,6,7,9\},\\
Z_2(7) &= \left\{r \in Z_7^* \middle| \left(\tfrac{r}{7}\right)_3 = 2^2\right\} = \{2,5\}, \quad & Z_2(13) &= \left\{r \in Z_{13}^* \middle| \left(\tfrac{r}{13}\right)_3 = 9^2\right\} = \{2,3,10,11\},
\end{aligned}
$$

*we find that $Z_{i,j}(91) = Z_i(7) \times Z_j(13)$. In particular,*

$$
\begin{aligned}
Z_{0,0}(91) &= \left\{r \in Z_{91}^* \middle| \left(\frac{r}{7}\right)_3 = 2^0, \left(\frac{r}{13}\right)_3 = 9^0\right\} = Z_0(7) \times Z_0(13)\\
&= \{\langle 1,1\rangle, \langle 1,5\rangle, \langle 1,8\rangle, \langle 1,12\rangle, \langle 6,1\rangle, \langle 6,5\rangle, \langle 6,8\rangle, \langle 6,12\rangle\}\\
&= \{1,57,8,64,27,83,34,90\}
\end{aligned}
$$

*has $\frac{(7-1)(13-1)}{9} = 8$ elements. If we let*

$$
\begin{aligned}
C = \{&c_{0,0} = \langle 1,1\rangle, c_{0,1} = \langle 1,4\rangle, c_{0,2} = \langle 1,2\rangle, c_{1,0} = \langle 4,1\rangle, c_{1,1} = \langle 4,4\rangle,\\
&c_{1,2} = \langle 4,2\rangle, c_{2,0} = \langle 2,1\rangle, c_{2,1} = \langle 2,4\rangle, c_{2,2} = \langle 2,2\rangle\}\\
= \{&1,43,15,53,4,67,79,30,2\}
\end{aligned}
$$

*be the set of representative elements for each partition class of $Z_{91}^*$. Then, $c_{i',j'} \cdot Z_{i,j}(91) = Z_{0,0}(91)$, for $i+i' \equiv j+j' \equiv 0 \bmod 3$. For example, let $i=0$, $j=1$, $i'=0$ and $j'=2$. Then,*

$$
\begin{aligned}
c_{0,2} \cdot Z_{0,1}(91) &= \langle 1,2\rangle \cdot \{\langle 1,4\rangle, \langle 1,6\rangle, \langle 1,7\rangle, \langle 1,9\rangle, \langle 6,4\rangle, \langle 6,6\rangle,\ \langle 6,7\rangle, \langle 6,9\rangle\}\\
&= \{\langle 1,8\rangle, \langle 1,12\rangle, \langle 1,1\rangle, \langle 1,5\rangle, \langle 6,8\rangle, \langle 6,12\rangle, \langle 6,1\rangle, \langle 6,5\rangle\}\\
&= \{8,64,1,57,34,90,27,83\}\\
&= Z_{0,0}(91).
\end{aligned}
$$

This example below shows how a cubic congruence equation is solved.

**Example 3.2.** *Let $p = 139 = 3 \times 46 + 1$, $q = 229 = 3 \times 76 + 1$ be two distinct rational primes. Then, $p = \pi\bar{\pi} = (13+10\omega)(13+10\bar{\omega})$, $q = \pi'\bar{\pi}' = (17+12\omega)\cdot(17+12\bar{\omega})$ and $p \equiv q \equiv 4 \bmod 9$. In addition, $e_1 = -13 \cdot 10^{-1} \bmod 139 = 96$ and $e_2 = -17 \cdot 12^{-1} \bmod 229 = 94$. As shown in the last paragraph just before Table 1, we set $c_{i,j} =$*

$\langle e_1^i \bmod p, e_2^i \bmod q\rangle = \langle 96^i \bmod 139, 94^j \bmod 229\rangle \in Z_{i,j}(pq)$, $0 \le i,\ j \le 2$. *Let*

$$\begin{aligned} C = &\{c_{0,0} = \langle 1,1\rangle, c_{0,1} = \langle 1,94\rangle, c_{0,2} = \langle 1,134\rangle, c_{1,0} = \langle 96,1\rangle, c_{1,1} = \langle 96,94\rangle,\\ &c_{1,2} = \langle 96,134\rangle, c_{2,0} = \langle 42,1\rangle, c_{2,1} = \langle 42,94\rangle, c_{2,2} = \langle 42,134\rangle\}\\ = &\{1, 20017, 23492, 19695, 7880, 11355, 459, 20475, 23950\}. \end{aligned}$$

*be the set of representative elements for* $Z_{i,j}(pq)$, $0 \le i,\ j \le 2$.

*We can obtain nine equivalence classes* $Z_{i,j}(pq) = c_{i,j}Z_{0,0}(pq) = \{c_{i,j} \cdot r^3 \bmod pq \,|r \in Z_{pq}^*\}$, $0 \le i,\ j \le 2$, *such that* $Z_{pq}^* = \bigcup_{0\le i,j\le 2} Z_{i,j}(pq)$.

*Now, for* $b = 23903 \in Z_{pq}^*$, *we want to find* $c \in C$ *such that cb is a cubic residue. First, we calculate* $\left(\frac{23903}{139}\right)_3 \equiv 23903^{\frac{139-1}{3}} \bmod 139 = 42$ *and* $\left(\frac{23903}{229}\right)_3 \equiv 23903^{\frac{229-1}{3}} \bmod 229 = 94$, *so we have* $b = 23903 \in Z_{2,1}(pq)$. *Therefore, we choose* $c = c_{1,2}$ *such that* $c_{1,2} \cdot b \bmod pq = 11355 \times 23903 \bmod 31831 = 27459$ *is a cubic residue. This means that* $x^3 \equiv 27459 \bmod 31831$ *is solvable. Let* $x_{00} = 31112 = \langle 115, 197\rangle$, *then we have*

$$\begin{aligned} x_{00}^3 &= \langle 115^3 \bmod 139, 197^3 \bmod 229\rangle\\ &= \langle 1520875 \bmod 139, 7645373 \bmod 229\rangle\\ &= \langle 76, 208\rangle = 27459. \end{aligned}$$

*Hence,* $x_{i,j} = c_{i,j} \cdot \langle 115, 197\rangle$, $0 \le i,\ j \le 2$ *are roots of the cubic congruence equation*

$$x^3 \equiv 27459 \bmod 31831$$

4. **The Proposed Scheme.** Using the cubic residue theory introduced in the preceding section, we now present a new signature scheme with an exponential cubic verification equation form and with security based on solving the discrete logarithm with a composite modulus.

Let us first give some theorems and definitions before we begin with our proposal.

**Theorem 4.1.** *Dirichlet's Theorem on Primes in Arithmetic Progressions (Theorem 2.9. [38]) Let* $(\mathrm{A}, \mathrm{B}) = 1$. *Then, the arithmetic progression* $\mathrm{A}\ell{+}\mathrm{B}$, $\ell = 1, 2, 3, \ldots$, *contains infinitely primes.*

For instance, let $\mathrm{A} = 5$ and $\mathrm{B} = 4$. It is obvious that there are infinitely primes in the form of $5\ell + 4$, e.g., 19, 29, 59, 79, 89, 109, 139, 149, 179, ....

**Definition 4.1.** *If* $m$, $n$ *are positive integers,* $a \in Z$ *and* $\gcd(a, m) = 1$, *we say that* $a$ *is an* $n$*-th power residue* mod$m$ *if* $x^n \equiv a \bmod m$ *is solvable.*

**Theorem 4.2** (Proposition 4.2.1. [37])**.** *If* $Z_m$ *possesses primitive roots and* $\gcd(a, m) = 1$, *then* $a$ *is an* $n$*-th power residue* mod$m$ *iff* $a^{\frac{\varphi(m)}{d}} \equiv 1 \bmod m$, *where* $d = \gcd(n, \varphi(m))$ *and* $\varphi(m)$ *is the Euler function.*

**Definition 4.2** ($\beta$-RSA modulus N)**.** *An integer* N *is called a* $\beta$-RSA *modulus if* $\mathrm{N} = p{\times}q$, *where* $p = 4p_1{+}1$, $q = 4q_1{+}1$, $p_1 \equiv q_1 \equiv 1 \bmod 3$, *and* $p$, $q$, $p_1$, $q_1$ *are large prime numbers. (According to Dirichlet's Theorem, we can find large prime numbers like* $p$, $q$, $p_1$, $q_1$*).*

**Definition 4.3** (Factoring problem with a $\beta$-RSA modulus N)**.** *Let* $\mathrm{N} = p{\times}q$, $p = 4p_1{+}1$, $q = 4q_1 + 1p_1 \equiv q_1 \equiv 1 \bmod 3$, *be a* $\beta$-RSA *modulus. We call it a factoring problem with a* $\beta$-RSA *modulus* $N$ *if* $N$ *is given while* $p$, $q$, $p_1$, $q_1$ *are unknown and we are asked to factor* $N$ *into the product of* $p$ *and* $q$.

**Definition 4.4** (Discrete logarithm problem with a $\beta$-RSA modulus N)**.** *Let* N *be a* $\beta$-RSA *modulus and* $G$ *be the cyclic multiplicative subgroup of* $Z_{\mathrm{N}}^*$ *with a generator* $g$ *of order* $p_1q_1$*. We call it a discrete logarithm problem with a* $\beta$-RSA *modulus* N *if* $a \in G$, $g$, N *are given and we are asked to find* $1 \le b < p_1q_1$ *such that* $a \equiv g^b \bmod \mathrm{N}$*.*

From the operational perspective, the proposed signature scheme can be presented in three phases: the initial phase, the signature generation phase and the verification phase.

**Initial phase**

The signer follows the steps below to set the signing environment.

(1) Choose a $\beta$-RSA modulus $\mathrm{N} = p \times q$, where $p = 4p_1 + 1$, $q = 4q_1 + 1$ and $p_1$, $q_1$ are large primes, such that $p_1 \equiv q_1 \equiv 1 \bmod 3$.
(2) Determine two primes $\pi = a_1 + b_1\omega$ and $\pi' = a_2 + b_2\omega \in D$ such that $p_1 = N(\pi) = \pi\pi'$ and $q_1 = N(\pi') = \pi'\bar{\pi}'$, respectively. Compute $e_1 \equiv -a_1b_1^{-1} \bmod p_1$ and $e_2 \equiv -a_2b_2^{-1} \bmod q_1$.
(3) For each $(i, j)$, $0 \le i, j \le 2$, choose one $c_{i,j} \in Z_{i,j}(p_1q_1) = \left\{ r \in Z_{p_1q_1}^* \middle| \left(\frac{r}{p_1}\right)_3 = e_1^i \text{ and } \left(\frac{r}{q_1}\right)_3 = e_2^j \right\}$ and set $C = \{c_{i,j} \,|0 \le i, j \le 2\}$.
(4) Choose an integer $g \in Z_{\mathrm{N}}^* = \{1 \le a < \mathrm{N} \,|\gcd(a, \mathrm{N}) = 1\}$ with order $\frac{1}{4} \times \mathrm{lcm}(p-1, q-1) = p_1q_1$.
(5) Select at random an integer $x \in Z_{p_1q_1}^*$ as the secret key and compute $y \equiv g^{x^3} \bmod \mathrm{N}$ as the public key.
(6) Let $H : \{0,1\}^* \times Z_{\mathrm{N}}^* \to Z_{p_1q_1}^*$ be a one-way hash function, where $\{0,1\}^*$ denotes the set of all binary bit strings.
(7) Publish N, $y$, $g$, $H$.

**Signature generation phase**

To create a signature for a message $m$, the signer does the following.

(1) Randomly choose an integer $t \in Z_{p_1q_1}^*$ and compute$r = g^{t^3} \bmod \mathrm{N}$.
(2) Choose a proper $c \in C = \{c_{i,j} | 0 \le i, j \le 2\}$ such that $[H(m, r^2)^3 - x^3r^3] \times t^{-3}c^{-1} \in \mathrm{Z}_{0,0}(p_1q_1)$.
(3) Compute and get $s \in Z_{p_1q_1}^*$ which satisfies $x^3r^3 + ct^3s^3 \equiv H(m, r^2)^3 \bmod p_1q_1$.
(4) The signature of message $m$ is $(c, r, s)$.

**Signature verification phase**

Anyone can do the following to verify the signature $(c, r, s)$.

(1) Compute and check if the following equation holds.

$$y^{r^3}r^{cs^3} \equiv g^{H(m,r^2)^3} \bmod \mathrm{N}$$

(2) The signature $(c, r, s)$ is valid if the above equation holds, otherwise we reject it.

5. **Security Analysis with Discussions.** In this section, we claim that our proposed scheme is secure against Pollard and Schnorr's attack [24], and that our scheme is also secure under the random oracle model against the two most frequently cited attack scenarios, the no-message attack and the adaptively chosen-message attack.

5.1. **Security against Pollard-Schnorr's attack.**

5.1.1. *Pollard-Schnorr's congruence solution attack.* Pollard and Schnorr [24] showed, in 1987, that a solution of the congruence equation $X^2 + kY^2 \equiv m \bmod n$ can easily be found if $k$ and $m$ are relative prime to $n$.

As aforementioned in Section 1, many previously suggested signature schemes with their verification equations based on exponential quadratic form were not as secure as

claimed since they were subject to Pollard-Schnorr's congruence solution attack [24], such as those proposed by Ong et al. [4] in 1984, Shao [11] in 1998, He [12] in 2001, Tzeng [22] in 2004 and Wei [27] in 2007, etc. By using Wei's method [27] as an example, we will briefly introduce the concept of cryptanalysis by Pollard-Schnorr's method.

In [27], Wei modified both of Shao's schemes [11] in attempt to resist Li and Xiao's attack [16]. In modified scheme 1, the verification equation is $u^{(u^2m^2)} \equiv v^{v^2} \cdot y^{s^2-r^2} \bmod p$; and in modified scheme 2 it is $u^{u^2m^4} \equiv v^{v^2m^2} \cdot y^{(s^2-r^2)} \bmod p$. It is obvious that both verification equations are of exponential quadric form. Therefore, by applying Pollard-Schnorr's method, Lin et al. [29] performed a cryptanalysis on both of Wei's modified schemes, and showed that they can forge a valid signature of an arbitrary message. Lin et al.'s cryptanalysis can be briefly reviewed as follows.

Aim at Wei's modified scheme 1, the attacker substitutes $u = y^2$, $v = y^3$ in the verification identity $u^{(u^2m^2)} \equiv v^{v^2} \cdot y^{s^2-r^2} \bmod p$ for any message $m$. He obtains $(y^2)^{u^2m^2} \equiv (y^3)^{v^2} \cdot y^{s^2-r^2} \bmod p$ or $2u^2m^2 - 3v^2 \equiv s^2 - r^2 \bmod p_1q_1$. If the condition $\gcd(2u^2m^2 - 3v^2, p_1q_1) = 1$ is satisfied, he can solve out $(r, s)$ from $s^2 - r^2 \equiv 2u^2m^2 - 3v^2 \bmod p_1q_1$ by using the method of Pollard and Schnorr. Otherwise, he can repeat to adjust the values of $u$ and $v$ until $\gcd(2u^2m^2 - 3v^2, p_1q_1) = 1$, so that he can forge a valid signature $(u, v, r, s)$ of an arbitrary message $m$. Similar to the modified scheme 2, the attacker can solve out $(r, s)$ from $s^2 - r^2 \equiv 2u^2m^4 - 3v^2m^2 \bmod p_1q_1$ again by letting $u = y^2$, $v = y^3$ and then using the method of Pollard and Schnorr. Thus, he can also forge a valid signature of any message from the modified scheme 2.

As a result, in the preceding section we prevent security risks from verification equations in exponential quadric form (here we specifically refer to those vulnerable to Pollard-Schnorr's congruence solution attack) by implementing ours in exponential cubic form.

5.1.2. *Security analysis of the proposed scheme against Pollard-Schnorr's attack.* Before we begin the security analysis of our scheme against Pollard-Schnorr's attack, we will introduce some related mathematical preliminaries.

In 1984, Goldwasser and Micali introduced the notation of computationally indistinguishable distributions which was presented in [39,40]. For a distribution $Q$, let $x \in_R Q$ denote that $x$ is generated by distribution $Q$. An ensemble of probability distributions $Q(x)$ is polynomial time sampleable if there is a probabilistic polynomial (in $|x|$) time machine that on input $x$ its output is distributed according to $Q(x)$. Thus, we may define a probabilistic polynomial time machine $D$ (called the distinguisher) that can recognize the language $Q(x)$ as follows:

$$D(x, y) = \begin{cases} 1, & \text{when input } y \in Q(x) \\ 0, & \text{when input } y \notin Q(x) \end{cases}$$

**Definition 5.1.** **[41]** *Two ensembles of probability distributions* $\mathrm{A}(x)$ *and* $\mathrm{B}(x)$ *are polynomial-time indistinguishable if for any distinguisher* $D$ *acts as follows:* $x \in_R D(n)$ *is generated and then* $D$ *is given the output generated by either* $\mathrm{A}(x)$ *or* $\mathrm{B}(x)$*, and* $|\Pr[(D(x, y) = 1 | y \in_R \mathrm{A}(x)] - \Pr[D(x, y) = 1 \ | y \in_R \mathrm{B}(x)]| < \frac{1}{p(n)}$ *for all polynomials* $P$ *and for all sufficiently large* $n$.

As shown in the initial phase of our scheme, let $p_1$ and $q_1$ denote two distinct large primes such that $p_1 \equiv q_1 \equiv 1 \bmod 3$; $\pi = a_1 + b_1\omega \in D$ and $\pi' = a_2 + b_2\omega \in D$ such that $p_1 = N(\pi) = \pi\bar{\pi}$, $q_1 = N(\pi') = \pi'\bar{\pi}'$, $e_1 \equiv -a_1b_1^{-1} \bmod p_1$, $e_2 \equiv -a_2b_2^{-1} \bmod q_1$ and $Z_{i,j}(p_1q_1) = \left\{ r \in Z^*_{p_1q_1} \middle| \left(\frac{r}{p_1}\right)_3 \equiv e_1^i \bmod p_1, \left(\frac{r}{q_1}\right)_3 \equiv e_2^j \bmod q_1 \right\}$ for $0 \le i, j \le 2$. Then, $Z_{i,j}(p_1q_1)$, $0 \le i, j \le 2$, constitute a partition of $Z^*_{p_1q_1}$ and each of which has the same cardinality. Suppose that $Z^*_{p_1q_1}$ is a uniform distribution and $x \in_R Z^*_{p_1q_1}$. Then, the

probability of $x \in Z_{i,j}(p_1q_1)$ are equal for each $0 \le i,\ j \le 2$. Therefore, corresponding to the quadratic residuosity intractability assumption given in [42,43], we can analogize the intractability assumption to cubic residuosity as follows.

**Assumption 5.1.** The Cubic Residuosity Intractability Assumption (CRA) *Let $P(l)$ denote the set of primes of size $l$ bits. Define $C' = \{\mathrm{N}|\mathrm{N} = p \times q,\ p = 4p_1+1,\ q = 4q_1+1,\ p_1 \equiv q_1 \equiv 1 \bmod 3$ and $p_1, q_1 \in P(l)\}$. Suppose that $p_1$ and $q_1$ are unknown. Then, for any $\mathrm{N} \in C'$, the ensembles $Z_{i,j}(p_1q_1)$, $0 \le i,\ j \le 2$, are polynomial-time indistinguishable.*

Let $r_0 = \langle e_1^0, e_2^0\rangle \in Z_{0,0}(p_1q_1)$, $r_1 = \langle e_1^0, e_2^1\rangle \in Z_{0,1}(p_1q_1)$, $r_2 = \langle e_1^1, e_2^0\rangle \in Z_{1,0}(p_1q_1)$, $r_3 = \langle e_1^1, e_2^1\rangle \in Z_{1,1}(p_1q_1)$, $r_4 = \langle e_1^1, e_2^2\rangle \in Z_{1,2}(p_1q_1)$, $r_5 = \langle e_1^2, e_2^1\rangle \in Z_{2,1}(p_1q_1)$, $r_6 = \langle e_1^2, e_2^2\rangle \in Z_{2,2}(p_1q_1)$, $r_7 = \langle e_1^2, e_2^0\rangle \in Z_{2,0}(p_1q_1)$, $r_8 = \langle e_1^0, e_2^2\rangle \in Z_{0,2}(p_1q_1)$. Since $r_i^3 = \langle 1, 1\rangle$, $0 \le i \le 8$, we have the following remark.

**Remark 5.1.** *Let $n = p_1q_1$. If $a$ is a cubic residue mod $n$ and $x \in Z_n^*$ is a cubic root of $a \bmod n$ (i.e., $x^3 \equiv a \bmod n$), then $y = r_i x \bmod n$, $0 \le i \le 8$, are the nine distinct incongruent roots of the equation $x^3 \equiv a \bmod n$.*

**Lemma 5.1.** *Let $n = p_1q_1$. Given $x, y \in Z_n^*$ such that $x^3 \equiv y^3 \bmod n$ and $x \ne y$ then there is $\frac{1}{2}$ chance of factoring $n$.*

**Proof:** Note first that $x,\ y \in Z_n^*$, $x^3 \equiv y^3 \bmod n$ and $x \ne y$ mean that $x$ and $y$ are two distinct incongruent cubic root of a common cubic residue mod $n$. Thus, by Remark 5.1, we have $y = r_i x$ for $1 \le i \le 8$. Note further that $x^3 \equiv y^3 \bmod n$ implies $(x-y)(x^2+xy+y^2) \equiv (x-y)x^2(1+r_i+r_i^2) \equiv 0 \bmod n, 1 \le i \le 8$, or $(x-y)(1+r_i+r_i^2) \equiv 0 \bmod n$, $1 \le i \le 8$, because$x \in Z_n^*$. Therefore, we see that $\gcd((x-y) \bmod n, n) = p_1$or $q_1$ if $(1 + r_i + r_i^2) \not\equiv 0 \bmod n$. Next, by direct computation of CRT, we have $(1 + r_i + r_i^2) \not\equiv 0 \bmod n$ for $i = 1, 2, 7, 8$ and $(1 + r_i + r_i^2) \equiv 0 \bmod n$, for $i = 3, 4, 5, 6$. Thus, there is $\frac{1}{2}$ chance of factoring $n$ by means of $\gcd((x - y) \bmod n, n)$.

From Lemma 5.1, we immediately have the following theorem.

**Theorem 5.1.** *Let $n = p_1q_1$, where $p_1$ and $q_1$ are unknown. Suppose that $a$ is a cubic residue* mod $n$. *If there exists an algorithm which can determine, in a polynomial time, two distinct cubic roots $\{w_1, w_2\}$ of $a \bmod n$ and $w_2 = r_i w_1$ for some $i \in \{1, 2, 7, 8\}$, then $n$ can be factored into the product of $p_1$ and $q_1$, in a polynomial time.*

Now, suppose an adversary intends to forge a valid signature of a message $m$ from the verification equation

$$r^3x^3 + ct^3s^3 \equiv H\left(m, r^2\right)^3 \bmod p_1q_1 \tag{1}$$

of our scheme.

Then, in order to find a suitable set $(r, c, t, s)$ that satisfy Equation (1), he may try to perform the three following steps: (a) Determine $r$, $t$ and compute $M = H(m, r^2)$. (b) By setting $X = rx$, $Y = ts$, Equation (1) can be rewritten as

$$X^3 + cY^3 \equiv M^3 \bmod p_1q_1 \ \text{ or } \ Y^3 \equiv c^{-1}(M^3 - X^3) \bmod p_1q_1. \tag{2}$$

(c) Either (i) determine $c$, $X$ and solve for $Y$ by finding a cubic root of $c^{-1}(M^3-X^3) \bmod p_1q_1$, or (ii) determine $c$ and solve for $(X, Y)$ by using Pollard -Schnorr's method [24]. However, we claim that he can not succeed in both cases.

**Case 1**: Determine $c$, $X$ and solve $Y$ by finding a cubic root of $c^{-1}(M^3-X^3) \bmod p_1q_1$ Obviously, Equation (2) is solvable if and only if $c^{-1}(M^3-X^3)$ is a cubic residue mod $p_1q_1$; i.e., if and only if $(M^3 - X^3) \bmod p_1q_1$ and $c$ are in the same class $Z_{i,j}(p_1q_1)$, $0 \le i,\ j \le 2$. However, by the Cubic Residuosity Intractability Assumption, adjusting $(M^3 - X^3) \bmod p_1q_1$ such that it belongs in the same class $Z_{i,j}(p_1q_1)$ as $c$ is an intractability problem.

Assume even if the adversary has a magic box (MB) that can adjust $c$ and $(M^3, X^3)$ such that $c^{-1}(M^3 - X^3)$ is a cubic residue $\bmod p_1q_1$. He still need to compute a cubic root of $c^{-1}(M^3 - X^3) \bmod p_1q_1$. Assume further that the MB can also solve $Y^3 \equiv c^{-1}(M^3 - X^3) \bmod p_1q_1$with probability $\varepsilon$ in polynomial time. Then, by inputting $c^{-1}(M^3 - X^3)$ into MB repeatedly, if MB outputs two different cubic roots of $\{w_1, w_2\}$. $c^{-1}(M^3 - X^3)$ and $w_2 = r_i w_1 \bmod p_1q_1$ for some $i = 1, 2, 7, 8$, the adversary has $\frac{1}{2}\varepsilon$ chance of factoring $n$ in polynomial time. This is rather unlikely because the factoring problem is known to be computationally infeasible at present.

**Case 2**: Determine $c$ and solve for $(X, Y)$ by using Pollard-Schnorr's method [24]. Although in [24], Pollard and Schnorr also extended the algorithm for solving the equation $X^2 + kY^2 \equiv m \bmod n$ to give an efficient method to find the integer solutions for the equation $x^3 + ky^3 + k^2z^3 - 3kxyz \equiv m \bmod n$, where $k$, $m$ are relatively prime to $n$, their solutions did not contain those of the form $(x, y, 0)$ with $xy \not\equiv 0 \bmod n$. Therefore, Equation (2) cannot be solved by Pollard-Schnorr's method.

As far as our knowledge is concerned, currently there are no efficient algorithms to solve the equation $X^3 + cY^3 \equiv M^3 \bmod p_1q_1$ even if $k$, $m$ are relatively prime to $n = p_1q_1$. Accordingly, our signature scheme is secure against Pollard-Schnorr's attack.

5.2. **Security against no-message attacks.** In the so called no-message attack, the attacker only knows the public key of the signer (this is mentioned in Section 2.1). The proof of the proposed scheme being secure against existential forgery using the no-message attack discussed in this section is adopted from [31,33,44], in which the attacker is simulated by a probabilistic polynomial time Turing machine $A$ that generates probabilistic inputs by reading bits from a random tape and outputs from a random oracle.

5.2.1. *Unforgeability.* Signature schemes often use a hash function $H$, therefore, the function $H$ has to be free of collision. A hash function is an important ingredient of a signature scheme security. Bellare and Rogaway [34] and Fiat and Shamir [45] all considered that $H$ is actually a random function. This suggestion about $H$ being a random function originated from the corresponding model, called the "random oracle model", in which the hash function can be seen as an oracle that produces a random value for each new query. However, identical answers are obtained if the same query is asked twice.

Now, assume that the hash function $H$ outputs a $k$-bit string, where $2^{k-1} < p_1q_1 \leq 2^k$ as defined in Definition 4.2. Then, we will consider a signature scheme which, on the input message $m$ and a random number $\sigma_1$ takes its value from an appropriately large set; produce a triplet $(\sigma_1, h, \sigma_2)$ as the signature. In the triplet $(\sigma_1, h, \sigma_2)$, $h$ is the output hash value of $(m, \sigma_1)$ and $\sigma_2$ only depends on$\sigma_1$, the message $m$ and $h$.

We will state a well-known lemma given by Pointcheval and Stern [35]. The Forking Lemma, and which will be repeatedly used below. This lemma uses the "oracle replay attack", by a polynomial replay of an attack with the same random tape and a different oracle, to obtain two signatures of a specific form. By directly applying the Forking Lemma technique of Pointcheval and Stern [33], we can obtain the following generic result. Accordingly, we will now illustrate the Forking Lemma suitable for the current No-Message Attack scenario.

**Lemma 5.2** (The Forking Lemma, Theorem 1 [35])**.** *Let the forger $A$ be a Probabilistic Polynomial time Turing machine (PPT) whose input only consists of public data. We denote the number of queries that $A$ can ask to the random oracle by $Q$. Assume that, within a time bound $T$, $A$ produces a valid signature $(m, \sigma_1, h, \sigma_2)$ with probability $\varepsilon \geq \frac{7Q}{2^k}$, then there is another machine which has control over $A$ and produces two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$, such that $h \neq h'$ in expected time $T' \leq \frac{84480TQ}{\varepsilon}$.*

We will now apply this lemma to our scheme in order to prove its security against no-message attacks.

**Theorem 5.2** (Security against no-message attacks)**.** *Assume that within a time bound $T_1$, an attacker A (PPT) performs an existential forgery of our scheme under a no-message attack. If it has a non-negligible probability $\varepsilon$ of success, then the discrete logarithm problem with a $\beta$-RSA modulus can be solved with the probability of $\varepsilon'' = \frac{\varepsilon}{18}$, in expected time less than $\bar{c} \cdot \left(\frac{84480QT_1}{\varepsilon} + T_2 + T_3\right)$ for some constant $\bar{c} \geq 1$.*

Notice that $T_2$ and $T_3$ represent the average computing times of finding the greatest common divisor via Euclidean algorithm and solving the cubic residue $x^3 \equiv a \bmod p_1q_1$ respectively.

**Proof**: Suppose that an attacker can break our signature scheme of probability $\varepsilon$ within a bound time $T_1$. Then, he continuously replays the same input $(m, \sigma)$ to different machines. By using the Forking Lemma, he can obtain two valid signatures $(m, \sigma, h_1, \sigma_1)$ and $(m, \sigma, h_2, \sigma_2)$ in expected time $T_1' \leq \frac{84480QT_1}{\varepsilon}$, such that hash function values $h_1 \neq h_2$, where $h_1 = H_1(m, r_1^2)$, $h_2 = H_2(m, r_2^2)$. Here $\sigma = (m, r^2)$ is the input; $\sigma_1 = (c_1, r_1, s_1)$ and $\sigma_2 = (c_2, r_2, s_2)$ are the outputs.

Since $r_1^2 \equiv r_2^2 \equiv r^2 \pmod{p_1q_1}$ and $r_1 \neq \pm r_2 \pmod{p_1q_1}$ with probability $\frac{1}{2}$, we are able to get a factor of $p_1q_1$ via $\gcd(r_1 - r_2, p_1q_1)$. Thus, the $\beta$-RSA modulus N can be factored in expected time $T_2$ with a non-negligible probability $\varepsilon' = \frac{\varepsilon}{2}$.

Moreover, under the assumption $r_1 \neq \pm r_2 \pmod{p_1q_1}$, if the attacker gets two valid signatures $(m, c_1, r_1, s_1)$ and $(m, c_2, r_2, s_2)$, consider the two congruence equations

$$\begin{cases} y^{r_1^3} r_1^{c_1 s_1^3} \equiv g^{h_1^3} \pmod{\mathrm{N}} & (3) \\ y^{r_2^3} r_2^{c_2 s_2^3} \equiv g^{h_2^3} \pmod{\mathrm{N}} & (4) \end{cases}$$

Hence, $y^{c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3} \equiv g^{c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3} \pmod{\mathrm{N}}$ or

$$x^3(c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3) \equiv (c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3) \pmod{p_1q_1} \quad (5)$$

Since $H_1$ and $H_2$ came from the "Oracle replay", we may further assume that $c_2 h_1^3 s_2^3 \neq c_1 h_2^3 s_1^3 \pmod{p_1q_1}$. Let $d = \gcd(c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3, p_1q_1)$. Considering the following three cases for the congruence Equation (5), we have

**Case 1:** If $d = 1$, then Equation (5) can be solved $x^3 \equiv (c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3)^{-1}[c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3] \pmod{p_1q_1}$.

**Cbse 2:** If $d = p_1$ or $q_1$, so $c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3 = \ell_1 p_1$ (or $\ell_2 q_1$) for some $\ell_1$ (or $\ell_2$), then $x^3 \equiv (\ell_1 p_1)^{-1}[c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3] \pmod{q_1}$ or $x^3 \equiv (\ell_2 q_1)^{-1}[c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3] \pmod{p_1}$.

**Ccse 3:** If $d = p_1q_1$, then $c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3 = 0 \pmod{p_1q_1}$. This implies $c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3 = 0 \pmod{p_1q_1}$ which contradicts our assumption.

Finally, let $\lambda = (c_2 r_1^3 s_2^3 - c_1 r_2^3 s_1^3)^{-1}(c_2 h_1^3 s_2^3 - c_1 h_2^3 s_1^3)$. Then, $x^3 \equiv \lambda \pmod{p_1q_1}$ is solvable if and only if $\lambda$ is a cubic residue $\bmod p_1q_1$. By Section 2, we already know that $\lambda \in Z_{0,0}(p_1q_1)$ with a probability of about $\frac{1}{9}$. Therefore, by using the oracle replay and Theorem 4.2, we obtain at least one solution $x$ with the probability of $\varepsilon'' = \frac{\varepsilon'}{9}$ in expected time $T_3$.

Additionally, let N be a $\beta$-RSA modulus and $g$, $G$, $p_1q_1$ be defined as above. Let $a \in G$ and the attacker attempts to find $b$, $1 \leq b \leq p_1q_1$, such that $a \equiv g^b \bmod \mathrm{N}$. Through trial and error, he can choose an integer $\ell \in C = \{c_{i,j} \,|0 \leq i, j \leq 2\}$ such that $y = a^\ell = g^{b\ell}$ is regarded as a public key. From the results above, the attacker inserts $a^\ell$, $g$, N, $p_1q_1$ as the inputs of the efficient oracle replay to obtain $O(y, g, \mathrm{N}, p_1q_1) = x$. By setting $b \equiv \ell^{-1}x^3 \bmod p_1q_1$, the attacker can check whether the equation $a \equiv g^b \bmod \mathrm{N}$ holds or not, since the probability that $\ell b$ is a cubic residue $\bmod p_1q_1$ is approximately $\frac{1}{9}$. Thus,

there exists such a $x \in Z^*_{p_1q_1}$ that is regarded as a secret key and satisfies $\ell b \equiv x^3 \bmod p_1q_1$, where the discrete logarithm problem with a $\beta$-RSA modulus can be solved in polynomial time with a non-negligible probability.

5.3. **Security against adaptively chosen-message attacks.** Next, we aim to prove that the proposed signature scheme is secure against adaptively chosen-message attacks. In the adaptively chosen message case, where the attacker can ask the signer to sign any message that he wants if he has knowledge of the public key of the signer, he can then adapt his queries according to previous message-signature pairs. The attacker views the signer as a kind of oracle. The signer can be simulated by a simulator $S$ that cannot know the secret key, since the attacker did not interact with the real signer. Therefore, to prove the unforgeability property of a given signature scheme against adaptively chosen message attacks is the same as proving the existence of a simulator. The simulator creates an output distribution using a no-message attack that is indistinguishable from that of the adaptively chosen message attack.

We will state the "Forking Lemma" suitable for adaptively chosen-message attacks which was proved by Pointcheval and Stern [33] as follows.

**Lemma 5.3** (The Forking Lemma, Theorem 3 [35]). *Let $A$ be a probabilistic polynomial time Turing machine whose input only consists of public data. We denote respectively by $Q$ and $R$ the number of queries that $A$ can ask to the random oracle and the number of queries that $A$ can ask to the signer. Assume that, within a bound time $T_1$, $A$ produces, with probability $\varepsilon \geq \frac{10(R+1)(R+Q)}{2^k}$, a valid signature $(m, \sigma_1, h, \sigma_2)$. If the triplet $(\sigma_1, h, \sigma_2)$ can be simulated without knowing the secret key, with an indistinguishable distribution probability, then there is another machine which has control over the machine obtained from $A$, replacing interaction with the signer by simulation and produces two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma'_2)$ such that $h \neq h'$ in expected time $T' \leq \frac{120686T_1Q}{\varepsilon}$.*

**Lemma 5.4.** *For the discrete logarithm problem with a $\beta$-RSA modulus, the signer can be simulated with an indistinguishable distribution.*

**Proof:** The proof shares the same logic as in [36] directly. Under the random oracle model, using the two parameters $v$, $e$ for forgery, the attacker can obtain an indistinguishable simulation. First, he assumes that the output set $\Lambda$ of random oracles is $\{0, 1, 2, 3, \ldots, 2^k - 1\}$ and $2^k \geq p_1q_1 \geq 2^{k-1}$. He then randomly chooses $e \in Z^*_{p_1q_1}$, $\nu \in Z^*_{p_1q_1}$ and $c \in C = \{c_{i,j} \,|0 \leq i, j \leq 2\}$. Finally, by letting $r = g^{c^{-1}e^3}y^{c^{-1}\nu^3} \bmod \mathrm{N}$, $s = -rv^{-1} \bmod p_1q_1$ and $h = -erv^{-1} \bmod p_1q_1$, he can easily check that

$$\begin{aligned} y^{r^3}r^{cs^3} &\equiv g^{r^3x^3} \cdot g^{cs^3(c^{-1}e^3+c^{-1}x^3\nu^3)}(\mathrm{mod N}) \\ &\equiv g^{r^3x^3+c(c^{-1}e^3+c^{-1}x^3\nu^3)(-r^3\nu^{-3})}(\mathrm{mod N}) \\ &\equiv g^{r^3x^3-r^3e^3\nu^{-3}-r^3x^3}(\mathrm{mod}) \\ &\equiv g^{-r^3e^3\nu^{-3}}(\mathrm{mod N}) \equiv g^{h^3}(\mathrm{mod N}). \end{aligned}$$

It follows that the quadruple $(c, r, s, h)$ is a valid signature of a message $m$ as soon as $h = H(m, r^2)$.

Let $(c, r, s, h) \in C \times Z_{\mathrm{N}} \times Z_{p_1q_1} \times \Lambda$. Trying to output this signature through our simulation yields the following system of equations

$$\begin{cases} h^3v^3 + r^3e^3 \equiv 0 \bmod p_1q_1 \\ x^3v^3 + e^3 \equiv c \log_g r \bmod p_1q_1. \end{cases}$$

Consider the determinant $\Delta = \begin{vmatrix} h^3 & r^3 \\ x^3 & 1 \end{vmatrix} = h^3 - x^3r^3 \bmod p_1q_1$.

**Case 1:** $\Delta \neq 0$, then the system of equation has exactly one solution $(\nu^3, e^3)$, and therefore, 81 ways for simulator $S$ to generate such 81 different valid signatures.

**Cbse 2:** $\Delta = 0$, then $h^3 \equiv x^3 r^3 \bmod p_1 q_1$. $S$ can generate such signatures only if $r = h = s = 0 \bmod p_1 q_1$, $e^3 = -x^3 \nu^3 \bmod p_1 q_1$ and $v \in Z^*_{p_1 q_1}$. Thus, there are $\varphi(p_1 q_1)$ ways to generate at most $\left\lceil \frac{pq}{p_1 q_1} \right\rceil = 17$ different improper signatures. However, the probability of $\Delta = 0$ is bounded by $O\left(\frac{\mathrm{N}}{2^k \mathrm{N}^2}\right) = O\left(\frac{1}{2^k \mathrm{N}}\right) < O\left(\frac{1}{\mathrm{N}}\right)$, which is a negligible value.

Thus, even without the secret key, the probability of the simulator $S$ to successfully simulate a valid signature is overwhelming.

**Theorem 5.3** (Security against adaptively chosen-message attacks)**.** *Assume that $Q$, $R$ are the same as defined in Lemma 5.3 and $T_2$, $T_3$ are the same as described in Theorem 5.2. Let $A$ be an attacker which performs an existential forgery under an adaptively chosen-message attack against our scheme and has a non-negligible probability $\varepsilon$ of success within a bound time $T_1$. Assume that $\varepsilon \geq \frac{10(R+1)(R+Q)}{p_1 q_1}$, then the discrete logarithm problem with a $\beta$-*RSA *modulus can be solved with the probability of $\varepsilon' = \frac{\varepsilon}{18}$ in expected time less than $\bar{\bar{c}} \cdot \left(\frac{120686 Q T_1}{\varepsilon} + T_2 + T_3\right)$ for some constant $\bar{\bar{c}} \geq 1$.*

**Proof**: Let $A$(PPT) be an attacker which performs an existential forgery of our scheme under an adaptively chosen-message attack within a bound time $T_1$. If the attacker has a non-negligible probability $\varepsilon \geq \frac{10(R+1)(R+Q)}{p_1 q_1}$ of success, then by Lemma 5.4, the signer can be simulated by simulator $S$ which does not know the secret key with an indistinguishable distribution probability. Therefore, by Lemma 5.3 (the Forking Lemma), the collusion of the attacker $A$ and the simulator $S$ can gain two valid signatures, $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$, such that $h \neq h'$ in expected time $T' \leq \frac{120686 T_1 Q}{\varepsilon}$. Once this is done, using the same proof as in Theorem 5.2, we obtain the result of Theorem 5.3.

6. **Conclusions and Future Works.** In view of security flaws were discovered among many signature schemes suggested previously with exponential quadratic verification equation and with security based on discrete logarithm and integer factorization problems. In this paper, by taking advantage of the cubic residue theory, we have proposed a new signature scheme with an exponential cubic verification equation to prevent the attack from Pollard-Schnorr's congruence solutions. In addition, by using the random oracle modeling and the Forking Lemma, we have formally proved that the security of our proposed scheme is based on solving the discrete logarithm problem with a composite modulus. This has been proved by Bach in 1984 to be equivalent to solving both the integer factorization and the discrete logarithm with a prime modulus. Furthermore, we have shown that our scheme is secure against the two most frequently cited attack scenarios, the no-message attack and the adaptively chosen-message attack.

Since cubic residues are introduced into the proposed scheme, the computational cost is inevitably increased in comparison with those signature schemes having exponential quadratic verification equation. Nevertheless, in 1986, Williams [46] suggested an effective method to reduce the complexity of computing the cubic roots of a cubic residue modulo an RSA composite. Further, in 2009, Chang and Lai [47] proposed an effective method to speed up modular exponentiation operation. Perhaps Williams' method together with Chang and Lai's method can be applied to develop an effective method to reduce the computation complexity of our signature generation and verification. This remains to be our future research problem.

## REFERENCES


[1] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. on Information Theory*, vol.22, pp.644-654, 1976.

[2] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signature and public-key cryptosystem, *Communications of the ACM*, vol.21, no.2, pp.120-126, 1978.

[3] M. O. Rabin, *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*, MIT/LCS/TR-212, MIT Lab. for Computer Science, Cambridge, Mass, 1979.

[4] H. Ong, C. Schnorr and A. Shamir, An efficient signature scheme based on quadratic equations, *Proc. of the 16th Symposium on the Theory of Computing*, Washington, pp.208-216, 1984.

[5] T. ElGamal, A public key cryptosystem and a signature scheme based on the discrete logarithm, *IEEE Trans. on Information Theory*, vol.31, no.4, pp.469-472, 1985.

[6] C. P. Schnorr, Efficient identification and signatures for smart cards, *Advances in Cryptology – Proc. of Eurocrypt'89, LNCS*, vol.434, pp.688-689, 1990.

[7] J. He and T. Kiesler, Enhancing the security of ElGamal's signature scheme, *Iet Software/iee Proceedings – Software*, vol.141, no.4, pp.249-252, 1994.

[8] L. Harn, Public-key cryptosystem design based on factoring and discrete logarithms, *IEE Proc. of Computers and Digital Techniques*, vol.141, no.3, pp.193-195, 1994.

[9] E. F. Brickell and K. S. McCurley, An interactive identification scheme based on discrete logarithms and factoring, *J. Cryptology*, vol.5, no.1, pp.29-40, 1992.

[10] C. S. Laih and W. C. Kuo, New signature schemes based on factoring and discrete logarithms, *IEICE Trans. Fundamentals*, vol.E80-A, no.1, pp.46-53, 1997.

[11] Z. Shao, Signature schemes based on factoring and discrete logarithms, *IEE Proc. of Computers and Digital Techniques*, vol.145, no.1, pp.33-36, 1998.

[12] W. H. He, Digital signature scheme based on factoring and discrete logarithms, *Electronics Letters*, vol.37, no.4, pp.220-222, 2001.

[13] K. C. McCurley, The discrete logarithm problem, *Proc. of Symposia in Applied Mathematics*, Providence, Rhode Island, vol.42, pp.49-74, 1990.

[14] N. Y. Lee and T. Hwang, Modified Harn signature scheme based on factoring and discrete logarithms, *IEE Proc. of Computers and Digital Techniques*, vol.143, no.3, pp.196-198, 1996.

[15] C. S. Laih and W. C. Kuo, New signature schemes based on factoring and discrete logarithms, *IEICE Trans. Fundamentals*, vol.E80-A, no.1, pp.46-53, 1997.

[16] J. Li and G. Xiao, Remarks on new signature scheme based on two hard problems, *Electronics Letters*, vol.34, no.25, pp.2401-2402, 1998.

[17] N. Y. Lee, Security of Shao's signature schemes based on factoring and discrete logarithms, *IEE Proceedings*, vol.146, no.2, pp.119-121, 1999.

[18] H. M. Sun, Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms, *NCS*, 2002.

[19] M. S. Hwang, C. C. Yang and S. F. Tzeng, Improved digital signature scheme based on factoring and discrete logarithms, *Journal of Discrete Mathematical Sciences and Cryptography*, vol.5, no.2, pp.151-155, 2002.

[20] L. Ding and C. S. Laih, *Comment: Digital Signature Scheme Based on Factoring and Discrete Logarithms*, 2002 (unpublished).

[21] Z. Shao, Comment on signature schemes based on factoring and discrete logarithms, *Electronics Letters*, vol.38, no.24, pp.1518-1519, 2002.

[22] S. F. Tzeng, C. Y. Yang and M. S Hwang, A new digital signature scheme based on factorings and discrete logarithms, *International Journal of Computer Mathematics*, vol.81, pp.9-14, 2004.

[23] Z. Shao, Security of meta-He digital signature scheme based on factoring and discrete logarithm, *Applied Mathematics and Computation*, vol.170, pp.976-984, 2005.

[24] J. Pollard and C. Schnorr, An efficient solution of the congruence $x^2 + ky^2 = m \bmod n$, *IEEE Trans. on Information Theory*, vol.33, pp.17-28, 1987.

[25] C. C. Chang, Y. F. Chang and W. C. Wu, An extendable-message-passing protocol with signatures based on two hard problems and its applications, *Proc. of the International Conference on Cyberworlds (CW'05)*, 2005.

[26] H. F. Lin, J. S. Liu and C. Y. Chen, Improved Shao's signature scheme, *Journal of Information Science and Engineering*, vol.23, pp.285-298, 2007.

[27] S. Wei, Digital signature scheme based on two hard problems, *International Journal of Computer Science and Network Security*, vol.7, no.12, 2007.

[28] J. Zheng, Z. Shao, S. Huang and T. Yu, Security of two signature schemes based on two hard problems, *Proc. of the 11th IEEE International Conference on Communication Technology*, pp.745-748, 2008.
[29] H. F. Lin, C. Y. Gun and C. Y. Chen, Comments on Wei's digital signature scheme based on two hard problems, *International Journal of Computer Science and Network Security*, vol.9, no.2, 2009.
[30] E. Bach, Discrete logarithms and factoring, *Technical Report UCB/CSD 84/186*, Computer Science Division (EECS), University of California, Berkeley, CA, USA, 1984.
[31] D. Pointcheval and J. Stern, Security proofs for signature schemes, *Advances in Cryptology – Eurocrypt'96, LNCS*, vol.1070, pp.387-398, 1996.
[32] A. W. Dent, Fundamental problems in provable security and cryptography, *Phil. Trans. R Soc. A*, vol.364, no.1849, pp.3215-3230, 2006.
[33] D. Pointcheval and J. Stern, Security arguments for digital signatures and blind signatures, *Journal of Cryptology*, vol.13, no.3, pp.361-396, 2000.
[34] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, *Proc. of the 1st ACM Conference on Computer and Communications Security*, pp.62-73, 1993.
[35] R. Canetti, O. Goldreich and S. Halevi, The random oracle methodology, *J. ACM*, vol.51, no.4, pp.557-594, 2004.
[36] J. Katz, Introduction to cryptography lecture 39, *CMSC456*, University of Maryland, 2004.
[37] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, Springer-Verlag, 1993.
[38] K. H. Rosen, *Elementary Number Theory and Its Applications*, 3rd Edition, Reading, Addison-Wesley, 1993.
[39] S. Goldwasser and S. Micali, Probabilistic encryption, *J. Com. Sys. Sci.*, vol.28, no.2, pp.270-299, 1984.
[40] A. C. Yao, Theory and applications of trapdoor functions, *Proc. of the 23th Symposium on the Foundation of Computer Science*, pp.80-91, 1982.
[41] M. Naor and M. Yung, Public-key cryptosystems provably secure against chosen ciphertext attacks, *Proc. of the 22nd ACM Symposium of Theory of Computing*, 1990.
[42] M. Blum, P. Feldam and S. Micali, Non-interactive zero-knowledge proof systems, *Proc. of the 20th Annual Symposium on the Theory of Computing*, Chicago, pp.103-112, 1988.
[43] A. de Santis, S. Micali and G. Persiano, Non-interactive zero-knowledge proof systems, *Proc. of Crypto'87*, 1987.
[44] E. Brickell, D. Pointcheval, S. Vaudenay and M. Yung, Design validations for discrete logarithm based signature schemes, *Practice and Theory in Public Key Cryptography, LNCS*, vol.1751, pp.276-292, 2000.
[45] A. Fiat and A. Shamir, How to prove yourself: Practical solutions of identification and signature problems, *Advances in Cryptology – Proc. of CRYPTO'86, LNCS*, vol.263, pp.186-194, 1987.
[46] H. C. Williams, An $M^3$ public-key encryption scheme, *Proc. of Cryptology – CRYPTO'85*, pp.358-368, 1986.
[47] C.-C. Chang and Y.-P. Lai, Modular square-and-multiply operation for quadratic residue bases, *International Journal of Innovative Computing, Information and Control*, vol.5, no.10(A), pp.3059-3069, 2009.