J. Cryptology (1998) 11: 109–124

Journal of
CRYPTOLOGY

A Public-Key Cryptosystem Using Purely Cubic Fields

R. Scheidler
Department of Mathematical Sciences, University of Delaware,
Newark, DE 19716, U.S.A.
scheidle@math.udel.edu

Communicated by Andrew M. Odlyzko

Received 8 July 1994 and revised 22 February 1997

Abstract. This paper presents an RSA-like public-key cryptosystem that can only be broken by factoring its modulus. Messages are encoded as units in a purely cubic field, and the encryption exponent is a multiple of 3. Similar systems with encryption powers of the form $2e$ as well as $3e$ were designed by Rabin, Williams, and Loxton et al. Our scheme is more general than previously developed methods in that it allows a broader class of primes for its modulus, namely any pair of distinct primes $p, q \equiv 1 \pmod 3$ rather than $p \equiv 4 \pmod 9$ and $q \equiv 7 \pmod 9$. The system employs several number theoretic techniques in the cyclotomic field $\mathbf{Q}(\sqrt{-3})$, including Euclidean division, rapid evaluation of cubic residuacity characters, and the computation of prime divisors of rational primes.

Key words. Public-key cryptosystem, Purely cubic field, Cubic residuacity character, Euclidean division.

1. Introduction

While RSA [12] is undoubtedly the most well-known and widely used public-key cryptosystem, the question of whether knowledge of the factorization of the modulus R is required in order to break RSA remains open. This problem has led to the development of a variety of public-key systems whose security is *equivalent* to the difficulty of factoring the modulus, i.e., for which it is necessary to factor the modulus in order to retrieve plaintext from ciphertext without using the secret key. The basic idea underlying all these systems is to replace the public RSA encryption exponent e by λe, where λ is a small prime (usually, $\lambda = 2$ or 3, but larger values of λ are possible). Upon raising a ciphertext to the secret exponent d, the decrypter obtains not the original message, but its λth power. As a result, the encrypter needs to provide a clue indicating which of the λth roots $\pmod R$ of this power is the correct message.

Rabin was the first to make use of this idea (with $\lambda = 2$) in his well-known signature scheme [11]. Two quadratic cryptosystems as well as a cubic scheme were developed by Williams [16], [17], [18] (see also [13] in connection with [17]). A different cubic

scheme is due to Loxton et al. [10]. All these methods utilize arithmetic in some quadratic number field, with the exception of [16] which, like RSA, uses modular arithmetic in the rational integers. Recently, Scheidler and Williams extended the ideas of [18] to cyclotomic fields of degree higher than 2 and designed a cryptosystem with exponent $5e$ [15], [14].

All the above schemes were shown to be as difficult to break as it is to factor their moduli. Since the proof of this result is of a constructive nature and can thus be converted into a chosen ciphertext attack, care must be taken when using these systems. While the overall asymptotic complexity of these methods is the same as that of RSA, the algorithms tend to be more involved, both mathematically and computationally. Furthermore, all the above techniques, with the exception of [17], impose restrictions on the primes used in the modulus. Hence, there is a price to pay for the additional information regarding the security of these methods compared with that of RSA.

This paper presents an RSA-like public-key cryptosystem with exponent $3e$, (i.e., $\lambda = 3$), that is based on arithmetic in a purely cubic field. The ideas are loosely based on Williams's quadratic scheme [17]. The modulus R is the product of two distinct primes $p, q \equiv 1 \pmod 3$. This means that our method allows a wider class of primes than the cubic techniques [18], [10] which are restricted to $p \equiv 4 \pmod 9$ and $q \equiv 7 \pmod 9$ (the scheme in [14] allows $p, q \equiv 4 \text{ or } 7 \pmod 9$). Like previous designs, our method's security is equivalent to the difficulty of factoring R in the above sense. The blocksize is twice as large as that of previous schemes, though no message expansion occurs. The public key is essentially the same size as an RSA key, and the complexity of encryption is the same as that of RSA for large encryption exponents, but worse by a factor that is linear in the size of the modulus for small encryption exponents. The secret key tends to be twice as large as an RSA key, thereby making decryption roughly twice as expensive as RSA decryption. Other drawbacks of our system are similar to those of comparable techniques, in particular, its vulnerability to a chosen ciphertext attack and its rather involved mathematical machinery. Consequently, the scheme loses some of its practicality over RSA, but the underlying number theoretic principles and methods, such as Euclidean division and rapid computation of cubic residuacity symbols, are of mathematical interest.

The paper is organized as follows. The next section outlines the mathematical basis for our cryptosystem. Section 3 discusses modular arithmetic in purely cubic fields and Section 4 presents the scheme itself. Section 5 analyzes the method's security. In Section 6 we give the underlying algorithms in more detail. Specifically, we present techniques for Euclidean division, evaluating cubic residuacity characters without factoring, and computing prime divisors of rational primes in the cyclotomic field of degree 2.

2. Notation and Preliminaries

For a brief summary on purely cubic fields, see, for example, p. 198 of [4]. Let:

D be a cube-free rational integer,
δ be the unique real cube root of D, so $\delta = \sqrt[3]{D}$,
$\mathbf{K} = \mathbf{Q}(\delta)$ the purely cubic field generated by δ, $(\mathbf{K} : \mathbf{Q}) = 3$,
ζ a nontrivial cube root of unity, $\zeta = (-1 \pm \sqrt{-3})/2$,

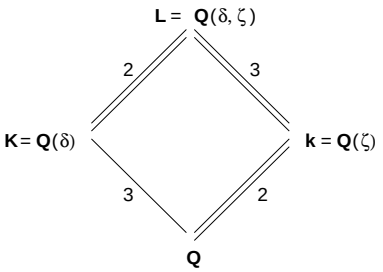

Fig. 1. Lattice diagram of field extensions.

$\mathbf{k} = \mathbf{Q}(\zeta)$ the cyclotomic field generated by ζ, $(\mathbf{k} : \mathbf{Q}) = 2$,
$\mathbf{L} = \mathbf{K}(\zeta) = \mathbf{k}(\delta) = \mathbf{Q}(\delta, \zeta)$ the Galois closure of $\mathbf{K}$, $(\mathbf{L} : \mathbf{Q}) = 6$.

Here, $(\mathbf{F} : \mathbf{Q})$ denotes the degree of a field $\mathbf{F}$ over $\mathbf{Q}$. A diagram of these field extensions is displayed in Fig. 1. Double lines indicate normal extensions and the numbers next to the lines give the relative degree of the extension.

For a field $\mathbf{F}$ ($\mathbf{F} = \mathbf{k}, \mathbf{K}$, or $\mathbf{L}$), denote the ring of integers in $\mathbf{F}$ by $\mathbf{O_F}$. Clearly, $\mathbf{O_k} = \mathbf{Z}[\zeta] = \mathbf{Z} \oplus \mathbf{Z}\zeta$, $\mathbf{O_K} \supseteq \mathbf{Z}[\delta] = \mathbf{Z} \oplus \mathbf{Z}\delta \oplus \mathbf{Z}\delta^2$, and $\mathbf{O_L} \supseteq \mathbf{Z}[\zeta][\delta] = \mathbf{Z}[\zeta] \oplus \mathbf{Z}[\zeta]\delta \oplus \mathbf{Z}[\zeta]\delta^2$. Equality is not necessarily satisfied for the latter two inclusions (see pp. 136ff. of [2]), but in our cryptoscheme, we only consider algebraic integers of the form $a_0 + a_1\delta + a_2\delta^2$ where $a_0, a_1, a_2 \in \mathbf{Z}[\zeta]$.

The Galois group G of $\mathbf{L}$ over $\mathbf{Q}$ has two generators σ, τ defined by

$$\zeta^\tau = \zeta, \qquad \zeta^\sigma = \zeta^2, \qquad \delta^\tau = \zeta\delta, \qquad \delta^\sigma = \delta.$$

Here, σ is the restriction of the complex conjugation to $\mathbf{L}$. G is isomorphic to the symmetric group S_3; the generators of G satisfy

$$\sigma^2 = \tau^3 = (\sigma\tau)^2 = 1.$$

For $\theta \in \mathbf{L}$, we write in short $\theta^\sigma = \overline{\theta}$, $\theta^\tau = \theta'$, $\theta^{\tau^2} = \theta''$.

$\mathbf{L}$ is a normal extension of degree 3 over $\mathbf{k}$ whose Galois group is generated by τ. For $\theta \in \mathbf{L}$, the relative norm of θ is $N_{\mathbf{L}|\mathbf{k}}(\theta) = \theta\theta'\theta'' \in \mathbf{k}$. If $\theta \in \mathbf{K}$, then $N_{\mathbf{L}|\mathbf{k}}(\theta) = N_{\mathbf{K}|\mathbf{Q}}(\theta) \in \mathbf{Q}$. Write $N(\theta)$ for $N_{\mathbf{L}|\mathbf{k}}(\theta)$.

Let p be a rational prime such that p does not divide D and $p \equiv 1 \pmod 3$. Since $\mathbf{k} = \mathbf{Q}(\sqrt{-3})$ and the Legendre symbol $(-3/p) = 1$, p splits into two primes in $\mathbf{Z}[\zeta]$, i.e., $p = \pi\overline{\pi}$ where π is a prime in $\mathbf{Z}[\zeta]$.

For any $\theta \in \mathbf{Z}[\zeta]$, we have $\theta^p \equiv \theta \pmod\pi$, hence if θ is not a multiple of π, there is a unique $k \in \{0, 1, 2\}$ such that $\theta^{(p-1)/3} \equiv \zeta^k \pmod\pi$. The *cubic residuacity character* $[\theta/\pi]$ is defined to be ζ^k. For distinct primes $\pi, \psi \in \mathbf{Z}[\zeta]$, we set $[\theta/\pi\psi] = [\theta/\pi][\theta/\psi]$. It is well known that for $\theta, \eta, \xi \in \mathbf{Z}[\zeta]$ relatively prime, $[\theta\eta/\xi] = [\theta/\xi][\eta/\xi]$ and $[\theta/\xi] = [\eta/\xi]$ if $\theta \equiv \eta \pmod\xi$, i.e., ξ divides $\theta - \eta$ in $\mathbf{Z}[\zeta]$ (see p. 112 of [6]).

Any prime divisor π of p in $\mathbf{Z}[\zeta]$ splits into three distinct prime ideals P, $P' = P^\tau$, $P'' = P^{\tau^2}$ in $\mathbf{O_L}$ if $[D/\pi] = 1$, i.e., if D is a cubic residue (mod p). π is inert in $\mathbf{O_L}$ if $[D/\pi] \neq 1$ (see [5]). In the latter case, $\pi^\tau = \pi$, and the map $\tau \pmod\pi$ on $\mathbf{O_L}$

is the *Frobenius automorphism*, given by exponentiation by p, so $\theta^p \equiv \theta' \pmod{\pi}$ or $\theta^p \equiv \theta'' \pmod{\pi}$ for all $\theta \in \mathbf{O_L}$. Hence $N(\theta) \equiv \theta^{p^2+p+1} \pmod{\pi}$ in $\mathbf{O_L}$. In the special case where $N(\theta) \equiv 1 \pmod{\pi}$, it follows from the inertness of π in $\mathbf{O_L}$ that

$$\theta^{(p^2+p+1)/3} \equiv \zeta^k \pmod{\pi}$$

for some $k \in \{0, 1, 2\}$.

Let $\alpha \in \mathbf{O_L}$, $\pi \nmid \alpha$, $N = N(\alpha) \in \mathbf{Z}[\zeta]$, and set $\beta = \alpha/\alpha' = \alpha^2\alpha''/N$. Then $N(\beta) = 1$, hence $\beta^{(p^2+p+1)/3} \equiv \zeta^k \pmod{\pi}$ for some $k \in \{0, 1, 2\}$. In this case, k is given as follows. If $\alpha^p \equiv \alpha' \pmod{\pi}$, then $\beta \equiv \alpha^{1-p} \pmod{\pi}$ and $\beta^{(p^2+p+1)/3} \equiv (\alpha^{p^2+p+1})^{(1-p)/3} \equiv N^{(1-p)/3} \equiv [N/\pi]^{-1} \pmod{\pi}$. Similarly, if $\alpha^p \equiv \alpha'' \pmod{\pi}$, then $\beta \equiv \alpha^{1-p^2} \pmod{\pi}$ and $\beta^{(p^2+p+1)/3} \equiv (N^{p+1})^{(1-p)/3} \equiv N^{2((1-p)/3)} \equiv [N/\pi] \pmod{\pi}$. This result gives rise to the following theorem, which is the basis of our cryptosystem.

Theorem 2.1. *Let p, q be distinct rational primes such that $p, q \equiv 1 \pmod 3$, and let π, ψ be prime divisors of p and q, respectively, in $\mathbf{k}$. Set $\rho = \pi\psi$, $R = pq = \rho\overline{\rho}$, and $f = ((p^2 + p + 1)(q^2 + q + 1))/9$. Let $D \in \mathbf{Z}$ satisfy $[D/\pi] = [D/\psi]^{-1} \neq 1$. Let $\alpha \in \mathbf{Z}[\delta]$ be such that $[N(\alpha)/\rho] = 1$, and set $\beta = \alpha/\alpha'$. Then $\beta^f \equiv \zeta^k \pmod{\rho}$ for some $k \in \{0, 1, 2\}$.*

Proof. Without loss of generality, assume that $[D/\pi] = \zeta$, $[D/\psi] = \zeta^2$. We have $\delta^{p-1} \equiv D^{(p-1)/3} \equiv [D/\pi] \equiv \zeta \pmod{\pi}$ and, similarly, $\delta^{q-1} \equiv \zeta^2 \pmod{\psi}$. Hence $\delta^p \equiv \delta' \pmod{\pi}$ and $\delta^q \equiv \delta'' \pmod{\psi}$. If $\alpha = a_0 + a_1\delta + a_2\delta^2$, $a_0, a_1, a_2 \in \mathbf{Z}$, then, by Fermat's Little Theorem,

$$\alpha^p \equiv a_0^p + a_1^p\delta^p + a_2^p\delta^{2p} \equiv a_0 + a_1\delta' + a_2\delta'^2 \equiv \alpha' \pmod{\pi},$$

similarly $\alpha^q \equiv \alpha'' \pmod{\psi}$. If $\beta = \alpha/\alpha'$, then $\beta \equiv \alpha^{1-p} \pmod{\pi}$, $\beta \equiv \alpha^{1-q^2} \pmod{\psi}$, hence by our previous observation, $\beta^{(p^2+p+1)/3} \equiv [N/\pi]^{-1} \equiv [N/\psi] \pmod{\pi}$, $\beta^{(q^2+q+1)/3} \equiv [N/\psi] \pmod{\psi}$, where $N = N(\alpha)$. Since $(p^2 + p + 1)/3 \equiv (q^2 + q + 1)/3 \equiv 1 \pmod 3$, it follows that $\beta^f \equiv [N/\psi]^{(q^2+q+1)/3} \equiv [N/\psi] \pmod{\pi}$ and $\beta^f \equiv [N/\psi]^{(p^2+p+1)/3} \equiv [N/\psi] \pmod{\psi}$, so if $[N/\psi] = \zeta^k$, $0 \leq k \leq 2$, then $\beta^f \equiv \zeta^k \pmod{\rho}$. □

Corollary 2.2. *Let $e, d \in \mathbf{Z}$ satisfy $3ed \equiv 1 \pmod f$. Then $\beta^{3ed} \equiv \zeta^l\beta \pmod{\rho}$ for some $l \in \{0, 1, 2\}$.*

Proof. Let $3ed = 1 + xf$, $x \in \mathbf{Z}$, and set $l \equiv kx \pmod 3$, $0 \leq l \leq 2$, where k is as in Theorem 2.1. Then, by the theorem,

$$\beta^{3ed} \equiv \beta^{1+xf} \equiv (\beta^f)^x\beta \equiv \zeta^{kx}\beta \equiv \zeta^l\beta \pmod{\rho}.$$ □

The basic idea for our cryptosystem is to encode a message as a unit $\beta = \alpha/\alpha'$ as above and encrypt it as $\beta^{3e} \pmod{\rho}$. To decrypt, we compute $(\beta^{3e})^d \equiv \zeta^l\beta \pmod{\rho}$ by

Corollary 2.2. If the decrypter knows l, then he or she can obtain β, and, finally, the original message.

Note that there are $2(p-1)/3$ cubic nonresidues (mod p), so there are $(4(p-1)(q-1))/9$ values of D (mod R) such that $[D/\pi] \neq 1$ and $[D/\psi] \neq 1$. If we select such a value of D and replace ψ by $\overline{\psi}$ if $[D/\pi] = [D/\psi]$, then D is as desired, and approximately 44% (four-ninths) of all integers satisfy that property. The following lemma shows that we can always find a small value of D that is suitable.

Lemma 2.3. *Under the assumption of the Extended Riemann Hypothesis* (*ERH*), *there exists a value* D *such that* $[D/\pi] \neq 1$, $[D/\psi] \neq 1$, *and* $D \leq 4(\log R)^4$.

Proof. Since the set of values of $D \pmod R$ with $[D/\pi] = 1$ is a proper subgroup of $(\mathbf{Z}/R\mathbf{Z})^*$ the smallest D value outside this set satisfies $D \leq 2(\log R)^2$ by a theorem due to Bach [1] (assuming ERH). An analogous result holds for ψ. Let $D_1 \pmod R$ be the smallest cubic nonresidue (mod p) and let $D_2 \pmod R$ be the smallest nonresidue (mod q), so $D_1, D_2 \leq 2(\log R)^2$. If D_1 is also a nonresidue (mod q) or D_2 is also a nonresidue (mod p), then the result of the lemma holds with $D = D_1$ (in the former case) or $D = D_2$ (in the latter case). If $[D_1/\psi] = [D_2/\pi] = 1$, then $D = D_1 D_2$ satisfies the lemma. □

For our scheme, we need an efficient method to perform arithmetic modulo $\rho = \pi\psi$.

3. Arithmetic (mod ρ)

Arithmetic (mod ρ) *in* $\mathbf{k}$. Let $\rho = r_0 + r_1\zeta$, $r_0, r_1 \in \mathbf{Z}$, so $R = \rho\overline{\rho} = r_0^2 - r_0 r_1 + r_1^2$. Then $\gcd(r_0, R) = \gcd(r_1, R) = 1$. Set $r \equiv -r_0 r_1^{-1} \pmod R$, $0 < r < R$. Then $r \equiv \zeta \pmod\rho$, and any algebraic integer $x_0 + x_1\zeta \in \mathbf{Z}[\zeta]$ satisfies $x_0 + x_1\zeta \equiv x \pmod\rho$ where $x \in \mathbf{Z}$ and $x \equiv x_0 + x_1 r \pmod R$, $0 \leq x < R$. Hence, arithmetic (mod ρ) in $\mathbf{k}$ reduces to rational integer arithmetic (mod R).

Arithmetic (mod ρ) *in* $\mathbf{L}$. By the above remark, any integer in $\mathbf{Z}[\zeta][\delta]$ is congruent (mod ρ) to an integer in $\mathbf{Z}[\delta]$. The cryptosystem in particular requires us to compute $\beta \pmod\rho$, where $\beta = \alpha/\alpha'$ and $\alpha \in \mathbf{Z}[\delta]$. Write $\beta = (1/N)\alpha^2\alpha''$ where $N = N(\alpha) \in \mathbf{Z}$. We will always have $\gcd(N, R) = 1$, so $N^{-1} \pmod R$ exists. Now $\alpha^2\alpha'' \equiv a_0 + a_1\delta + a_2\delta^2 \pmod\rho$ for some $a_0, a_1, a_2 \in \mathbf{Z}$. Then $\beta \equiv b_0 + b_1\delta + b_2\delta^2 \pmod\rho$ where $\beta_i \equiv N^{-1}a_i \pmod R$ and $0 \leq b_i < R$ for $i = 0, 1, 2$. Hence, $\beta \pmod\rho$ is associated with a triple of rational integers (b_0, b_1, b_2), where all three integers are between 0 inclusive and R exclusive.

Modular exponentiation in $\mathbf{O_L}$. Let $\beta \equiv b_0 + b_1\delta + b_2\delta^2 \pmod\rho$, $b_0, b_1, b_2 \in \mathbf{Z}$, and let $n \in \mathbf{Z}_+$. Then $\beta^n \pmod\rho$ can be computed using a well-known exponentiation technique (see p. 441f. of [7]).

Algorithm 3.1.

Input: $\beta = b_0 + b_1\delta + b_2\delta^2$, $b_0, b_1, b_2 \in \mathbf{Z}$, $0 \leq b_0, b_1, b_2 < R$.
Output: $\theta \equiv \beta^n \pmod\rho$, $\theta = t_0 + t_1\delta + t_2\delta^2$, $t_0, t_1, t_2 \in \mathbf{Z}$, $0 \leq t_0, t_1, t_2 < R$.

Algorithm:

1. Set $\theta \leftarrow 1$, $\eta \leftarrow \beta$.
2. Set $b \leftarrow n \pmod 2$, $(b = 0 \text{ or } 1)$, $n \leftarrow \lfloor n/2 \rfloor$.
3. If $b = 1$, then
   Set $\theta \leftarrow \theta\beta \pmod \rho$,
   If $n = 0$, then output θ and stop.
4. Set $\eta \leftarrow \eta^2 \pmod \rho$. Goto Step 2.

Here, every product of the form $\xi\varphi \equiv z_0 + z_1\delta + z_2\delta^2 \pmod\rho$ where $\xi \equiv x_0 + x_1\delta + x_2\delta^2 \pmod\rho$ and $\varphi \equiv y_0 + y_1\delta + y_2\delta^2 \pmod\rho$ is computed using the formulas

$$\begin{aligned} z_0 &\equiv x_0y_0 + x_1y_2D + x_2y_1D \pmod R, \\ z_1 &\equiv x_0y_1 + x_1y_0 + x_2y_2D \pmod R, \\ z_2 &\equiv x_0y_2 + x_1y_1 + x_2y_0 \pmod R. \end{aligned}$$

Clearly, this method requires $O(\log n(\log R)^2)$ bit operations assuming standard integer arithmetic implementation, and $O(\log n \log R \log\log R \log\log\log R)$ bit operations under fast (e.g., FFT-based) implementation of integer arithmetic.

4. The Cryptosystem

Let p, q, R, π, ψ, ρ, D, e, and d be as in Theorem 2.1 and Corollary 2.2 (an algorithm for computing π and ψ is given in Section 6).

Generally, in RSA-related cryptosystems, messages are assumed to be rational integers M between 0 and R and relatively prime to R. Note that the case $\gcd(M, R) \neq 1$ reveals the factorization of R, an extremely unlikely event if both p and q are large. In fact, the probability that an arbitrary rational integer between 0 and R is not relatively prime to R is so small that we henceforth ignore this case.

In our scheme we encode messages as *pairs* of rational integers (m_0, m_1) such that $0 < m_0, m_1 < R$ and $\gcd(m_0m_1, R) = 1$. This results in a blocksize that is twice as large as that of RSA. Mathematically, we associate with the message (m_0, m_1) the algebraic integer $\mu = m_0 + m_1\delta + \delta^2 \in \mathbf{Z}[\delta]$. The unit μ/μ' uniquely determines the pair (m_0, m_1):

Lemma 4.1. *Let $\alpha, \gamma \in \mathbf{Z}[\zeta][\delta]$ satisfy $\alpha\gamma' = \gamma\alpha'$. Then there exist $a, c \in \mathbf{Z}[\zeta]$ such that $a\gamma = c\alpha$.*

Proof. Let $\alpha = a_0 + a_1\delta + a_2\delta^2$, $\gamma = c_0 + c_1\delta + c_2\delta^2$, $(a_0, a_1, a_2, c_0, c_1, c_2 \in \mathbf{Z}[\zeta])$, $\alpha\gamma' = \gamma\alpha'$. Multiplying and comparing the coefficients of 1, δ, and δ^2 yields

$$\begin{aligned} D\zeta(\zeta - 1)(a_1c_2 - a_2c_1) &= 0, \\ (\zeta - 1)(a_1c_0 - a_0c_1) &= 0, \\ (\zeta - 1)(\zeta + 1)(a_0c_2 - a_2c_0) &= 0, \end{aligned}$$

whence follows $a_0c_2 = c_0a_2$, $a_1c_2 = c_1a_2$, so $a_2\gamma = c_2\alpha$. □

Corollary 4.2. *Let* $\alpha, \gamma \in \mathbf{Z}[\delta]$ *satisfy* $\alpha\gamma' \equiv \gamma\alpha' \pmod{\rho}$. *Then* α *and* $\gamma \pmod{\rho}$ *differ only by a factor in* $\mathbf{Z}/R\mathbf{Z}$.

It follows that normalizing $\mu = m_0 + m_1\delta + \delta^2$ such that the coefficient of δ^2 is 1 guarantees that μ/μ' uniquely determines the coefficients m_0 and m_1.

Next, we need to ensure that $\gcd(N(\mu), R) = 1$.

Lemma 4.3. *If* $a_0, a_1, a_2 \in \mathbf{Z}$, $\gcd(a_0, R) = 1$, *then* $\gcd(N, R) = 1$, *where* $N = N(a_0 + a_1\delta + a_2\delta^2)$.

Proof. Suppose $p \mid N$, i.e., p divides N. Then $\pi \mid \alpha\alpha'\alpha''$ in $\mathbf{O_L}$, where $\alpha = a_0 + a_1\delta + a_2\delta^2$. The inertness of π in $\mathbf{O_L}$ implies $\pi \mid \alpha^{\tau^i}$ in $\mathbf{O_L}$ for some $i \in \{0, 1, 2\}$. Since $\pi = \pi'$, it follows that $\pi \mid \alpha^{\tau^i}$ for all $i \in \{0, 1, 2\}$, hence $\pi \mid \alpha + \alpha' + \alpha'' = 3a_0$ in $\mathbf{O_L}$. Thus $p = \pi\overline{\pi} \mid 9a_0^2$ in $\mathbf{O_L}$ and hence in $\mathbf{Z}$, contradicting $\gcd(a_0, R) = 1$. □

Since μ does not necessarily satisfy $[N(\mu)/\rho] = 1$ as required by Theorem 2.1, the designer needs to find a suitable factor $\eta \in \mathbf{Z}[\delta]$ such that $[N(\mu\eta)/\rho] = 1$. Set $\mathcal{S} = \{(s_0, s_1, s_2) \in \mathbf{Z}^3 \mid 0 \le s_i < R$ and $s_i = 0$ or $\gcd(s_i, R) = 1$ for $i = 0, 1, 2$, $[N(s_0 + s_1\delta + s_2\delta^2)/\rho] \ne 1\}$. The following lemma shows that there are almost $\frac{2}{3}R^3$ elements in $\mathcal{S}$.

Lemma 4.4. *For* $i = 0, 1, 2$, *set* $\mathcal{S}_i(p) = \{(x, y, z) \in \mathbf{Z}^3 \mid 0 \le x, y, z \le p - 1$, $(x, y, z) \ne (0, 0, 0)$, $[N(x + y\delta + z\delta^2)/\pi] = \zeta^i\}$. *Then* $|\mathcal{S}_i(p)| = (p^3 - 1)/3$ *for* $i = 0, 1, 2$.

Proof. Since π is inert in $\mathbf{O_L}$, the residue field $\mathbf{F} = \mathbf{O_L}/\pi\mathbf{O_L}$ is a finite field of p^3 elements. Let w be a generator of the cyclic multiplicative group $\mathbf{F}^* = \mathbf{F}\backslash 0$. Then for any $\omega \in \mathbf{O_L}$ such that $\omega \equiv w \pmod{\pi}$, we have $[N(\omega)/\pi] = \zeta^k$ for some k, where $k \not\equiv 0 \pmod 3$, as w is a cube in $\mathbf{F}$ otherwise. Let $\alpha \in \mathbf{Z}[\delta]$, then $\alpha \equiv \omega^{3l+n} \pmod{\pi}$ for some $l, n \in \mathbf{Z}$ such that $0 \le l \le (p^3 - 4)/3$ and $0 \le n \le 2$, so $[N(\alpha)/\pi] = [N(\omega)/\pi]^n = \zeta^{kn}$. So $\alpha \in \mathcal{S}_i(p)$ if and only if $i \equiv kn \pmod 3$, and the three distinct values $0, 1, 2$ of n correspond to the three distinct values $0, k, 2k \pmod 3$ of i. Since there are exactly $(p^3 - 1)/3$ values $\alpha \equiv \omega^{3l+n} \pmod{\pi}$ $(0 \le l \le (p^3 - 4)/3)$, the result follows. □

Suppose now that $[N(\mu)/\rho] = \zeta^m$, $m \in \{0, 1, 2\}$, for a message μ. Choose $\varphi \in \mathcal{S}$ such that $[N(\varphi)/\rho] = \zeta^\varepsilon$ where $\varepsilon = 1$ or 2. Then

$$\left[\frac{N(\mu\varphi^{2\varepsilon m})}{\rho}\right] = \left[\frac{N(\mu)}{\rho}\right]\left[\frac{N(\varphi)}{\rho}\right]^{2\varepsilon m} = \zeta^{m+2\varepsilon^2 m} = 1$$

as $\varepsilon^2 \equiv 1 \pmod 3$. φ will be part of the public key. In practice, we would wish to choose $\varphi = s_0 + s_1\delta + s_2\delta^2$ so that the s_i $(i = 0, 1, 2)$ are small. In fact, it is easy to find φ so that $s_1 = 1$ and $s_2 = 0$, i.e., $\varphi = s + \delta$ where $0 < s < R$ and $\gcd(s, R) = 1$:

Lemma 4.5. *For $i = 0, 1, 2$, set $\mathcal{T}_i(p) = \{x \in \mathbf{Z} \mid 1 \le x \le p-1, [(x^3+D)/\pi] = \zeta^i\}$. Then*

$$\left| |\mathcal{T}_i(p)| - \frac{p-1}{3} \right| \le \tfrac{4}{3}\sqrt{p}.$$

Proof. For $i \in \{0, 1, 2\}$ and $x \in \{1, 2, \ldots, p-1\}$, set

$$h_i(x) = \left(\left[\frac{x^3+D}{\pi} \right] - \zeta^{i+1} \right) \left(\left[\frac{x^3+D}{\pi} \right] - \zeta^{i-1} \right),$$

then $h_i(x) = 0$ if and only if $[(x^3+D)/\pi] \ne \zeta^i$, and $h_i(x) = (\zeta^i - \zeta^{i+1})(\zeta^i - \zeta^{i-1}) = 3\zeta^{2i}$ otherwise. So, since $\zeta^{i+1} + \zeta^{i-1} = -\zeta^i$:

$$\begin{aligned} |\mathcal{T}_i(p)| &= \frac{1}{3\zeta^{2i}} \sum_{x=1}^{p-1} h_i(x) \\ &= \frac{1}{3\zeta^{2i}} \left(\left[\frac{x^3+D}{\pi} \right]^2 + \zeta^i \left[\frac{x^3+D}{\pi} \right] \right) + \frac{p-1}{3}. \end{aligned}$$

By Theorem 5.41 on p. 225 of [9], we have for any nontrivial cubic character $\chi \pmod p$:

$$\left| \sum_{x=1}^{p-1} \chi(x^3+D) \right| \le 2\sqrt{p}.$$

Since both the residuacity symbol and its square are cubic characters (mod p), it follows that

$$\begin{aligned} \left| |\mathcal{T}_i(p)| - \frac{p-1}{3} \right| &\le \frac{1}{3} \left| \sum_{x=1}^{p-1} \left[\frac{x^3+D}{\pi} \right]^2 \right| + \frac{1}{3} \left| \sum_{x=1}^{p-1} \left[\frac{x^3+D}{\pi} \right] \right| \\ &\le \tfrac{4}{3}\sqrt{p}. \end{aligned}$$

□

Note that the bound of $\frac{4}{3}\sqrt{p}$ can be improved to $(2\sqrt{p}+7)/3$ using results from [3], but the proof is somewhat longer, and, for our purposes, the constant $\frac{4}{3}$ is more than sufficient.

The above lemma implies that about two thirds of all $s \in \mathbf{Z}, 0 < s < R, \gcd(s, R) = 1$, satisfy $[N(\varphi)/\pi] \ne 1$, where $\varphi = s + \delta$. We would hope to find a suitable value of s that is small.

We are now ready to present our scheme.

Key Generation:

1. Choose two distinct large rational primes p, q such that $p, q \equiv 1 \pmod 3$. Set $R = pq$ and $f = ((p^2+p+1)(q^2+q+1))/9$.
2. Find prime divisors π, ψ in $\mathbf{Z}[\zeta]$ of p and q, respectively. Compute $\rho = \pi\psi = r_0 + r_1\zeta; r_0, r_1 \in \mathbf{Z}$.

3. Find $D \in \mathbf{Z}$ such that $0 < D < R$, $\gcd(D, R) = 1$, and $[D/\pi] = [D/\psi]^{-1} \neq 1$.
4. Choose $e \in \mathbf{Z}$, $0 < e < R$ and solve $3ed \equiv 1 \pmod{f}$ for d, $0 < d < f$.
5. Find $\varphi = s + \delta \in \mathbf{Z}[\delta]$ such that $0 < s < R$, $\gcd(s, R) = 1$, and $[N(\varphi)/\rho] \neq 1$.
6. Set the public key to $K_p = (D, s, r_0, r_1, e)$ and the secret key to $K_s = \{d\}$. Discard p, q, f, π, and ψ.

Clearly, the factorization of R enables a cryptanalyst to compute m and solve the congruence in Step 4, thereby retrieving the secret key d.

Note that $R = r_0^2 - r_0 r_1 + r_1^2 \geq r_0^2 - |r_0 r_1| + r_1^2 = (|r_0| - |r_1|)^2 + |r_0 r_1| \geq |r_0 r_1|$. Hence, if a user manages to find a small value of s, the public key requires only marginally more storage than a public RSA key. Since d can be as large as f, the secret key may require up to $2 \log R$ bits of memory, i.e., twice as much as a secret RSA key.

Precomputation (need only be done once per key):

1. Compute $r \equiv r_0 r_1^{-1} \pmod{R}$, $0 < r < R$.
2. Compute $N_\varphi = N(\varphi) = s^3 + D$ and $[N_\varphi/\rho] = \zeta^\varepsilon$, $\varepsilon = 1$ or 2.
3. Compute $N_\varphi^* \equiv N_\varphi^{-1} \pmod{R}$, $0 < N_\varphi^* < R$.

Encryption: Encrypt a message (m_0, m_1), $0 < m_0, m_1 < R$, $\gcd(m_0 m_1, R) = 1$ as follows:

1. Set $\mu = m_0 + m_1\delta + \delta^2$, $N_\mu = N(\mu) = m_0^3 + m_1^3 D + D^2 - 3m_0 m_1 D$.
2. Compute $[N_\mu/\rho] = \zeta^m$, $m \in \{0, 1, 2\}$, and $N_\mu^* \equiv N_\mu^{-1} \pmod{R}$, $0 < N_\mu^* < R$.
3. Set $\alpha \equiv \mu\varphi^{2\varepsilon m} \pmod{\rho}$ and $\beta = \alpha/\alpha' \equiv (N_\varphi^*)^{2\varepsilon m} N_\mu^* \alpha^2 \alpha'' \equiv b_0 + b_1\delta + b_2\delta^2 \pmod{\rho}$, $0 \leq b_0, b_1, b_2 < R$.
4. For $i = 0, 1, 2$, compute $r^i\beta \pmod{\rho}$. Sort the triples $(r^i b_0, r^i b_1, r^i b_2) \pmod{R}$ in lexicographical order, obtaining a corresponding ordering of the values $r^i\beta$, $i = 0, 1, 2$; say, $\beta_0 < \beta_1 < \beta_2$. Identify $n \in \{0, 1, 2\}$ such that $\beta = \beta_n$.
5. Compute $\beta^e \equiv b_0^{(e)} + b_1^{(e)}\delta + b_2^{(e)}\delta^2 \pmod{\rho}$, $0 \leq b_i^{(e)} < R$ for $i = 0, 1, 2$.
6. Find $l = \min\{i \mid b_i^{(e)} \not\equiv 0 \pmod{R}\} \in \{0, 1, 2\}$.
   Compute $b^* \equiv (b_l^{(e)})^{-1} \pmod{R}$, $0 < b^* < R$.
   Set $E_1 \equiv b^* b_{(l+1) \pmod 3}^{(e)} \pmod{R}$, $E_2 \equiv b^* b_{(l+2) \pmod 3}^{(e)} \pmod{R}$, $0 \leq E_1, E_2 < R$, where all subscripts are taken to be between 0 and 2.
7. Transmit $C = (E_1, E_2, l, m, n)$.

Step 7 shows that ciphertexts in our scheme are pairs of integers between 0 and R, just like plaintexts. Note that we will almost always have $l = 0$, so $E_1 \equiv (b_0^{(e)})^{-1} b_1^{(e)} \pmod{R}$, $E_2 \equiv (b_0^{(e)})^{-1} b_2^{(e)} \pmod{R}$.

A rapid method for computing residuacity symbols $[N/\rho]$ is given in Section 6. For $N \in \mathbf{Z}$, computing $[N/\rho]$ and $N^{-1} \pmod{R}$ can be combined into a single algorithm.

Decryption: Upon receiving $C = (E_1, E_2, l, m, n)$:

1. If $l = 0$, then set $\xi = 1 + E_1\delta + E_2\delta^2$.
   If $l = 1$, then set $\xi = E_2 + \delta + E_1\delta^2$.
   If $l = 2$, then set $\xi = E_1 + E_2\delta + \delta^2$.
   Compute $N(\xi)$.

2. Compute $N_\xi^* \equiv N(\xi)^{-1} \pmod R$, $0 < N_\xi^* < R$. Then compute $\theta \equiv (N_\xi^* \xi^3)^d \equiv t_0 + t_1\delta + t_2\delta^2 \pmod\rho$, $0 \le t_0, t_1, t_2 < R$.
3. For $i = 0, 1, 2$, compute $r^i\theta \pmod\rho$. Sort the triples $(r^i t_0, r^i t_1, r^i t_2) \pmod R$ in lexicographical order, obtaining a corresponding ordering of the values $r^i\theta$ $(i = 0, 1, 2)$; say, $\theta_0 < \theta_1 < \theta_2$. Identify θ_n.
4. Compute $\eta = \theta_n(\varphi'/\varphi)^{2\varepsilon m} \equiv \theta_n((\varphi')^2\varphi'' N_\varphi^*)^{2\varepsilon m} \equiv e_0 + e_1\delta + e_2\delta^2 \pmod R$, $0 \le e_0, e_1, e_2 < R$.
5. Define the matrix

$$\mathcal{M} = \begin{pmatrix} e_0 - 1 & e_2 D - r & e_1 D r^2 \\ e_1 & e_0 r - 1 & e_2 D r^2 \\ e_2 & e_1 r & e_0 r^2 - 1 \end{pmatrix}$$

and solve the system of linear congruences given by

$$\mathcal{M}\begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv 0 \pmod R$$

for x, y, x. Set $\widehat{m}_0 \equiv xz^{-1} \pmod R$, $\widehat{m}_1 \equiv yz^{-1} \pmod R$, $0 < m_0, m_1 < R$.

Theorem 4.6. *Encryption and decryption as given above are well-defined operations. Furthermore,* $(\widehat{m}_0, \widehat{m}_1) = (m_0, m_1)$.

Proof. Consider first the encryption algorithm. We have $[N(\alpha)/\rho] = 1$, so by Corollary 2.2, $\beta^{3ed} \equiv \zeta^k\beta \pmod\rho$ for some $k \in \{0, 1, 2\}$. It is easy to see that the triples $(r^i b_0, r^i b_1, r^i b_2) \pmod R$ in Step 4 are all distinct, so n is well defined. Furthermore, one of the $b_i^{(e)}$ in Step 6 must be nonzero, so l, b^*, E_1, and E_2 are also well defined.

Now consider the decryption algorithm. Step 1 yields $\xi \equiv b^*\beta^e \pmod\rho$, hence $N(\xi) \equiv (b^*)^3 \pmod R$ and N_ξ^* in Step 2 exists. Furthermore, $(N_\xi^*\xi^3)^d \equiv (N_\xi^*(b^*)^3\beta^{3e})^d \equiv \beta^{3ed} \equiv \zeta^k\beta \pmod\rho$ for some $k \in \{0, 1, 2\}$ by Corollary 2.2. So the ordered sequence $(\theta_0, \theta_1, \theta_2)$ is the same as the sequence $(\beta_0, \beta_1, \beta_2)$ in Step 4 of the encryption routine. Therefore, $\theta_n = \beta_n = \beta = \alpha/\alpha' = \mu\varphi^{2\varepsilon m}/\mu'(\varphi')^{2\varepsilon m}$ and $\eta = \mu/\mu'$. By Corollary 4.2, m_0 and m_1 are uniquely determined and are computed as follows. The congruence $x + y\delta + z\delta^2 \equiv (e_0 + e_1\delta + e_2\delta^2)(x + yr\delta + zr^2\delta^2) \pmod\rho$ is equivalent to the system of congruences given by

$$\mathcal{M}\begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv 0 \pmod R$$

which is obtained by multiplying and comparing coefficients of 1, δ, and δ^2 (note that $\det(\mathcal{M}) \equiv N(\eta) - 1 \equiv 0 \pmod R$). Again by Corollary 4.2, $x + y\delta + z\delta^2 \equiv F\mu \equiv Fm_0 + Fm_1\delta + F\delta^2 \pmod\rho$ for some $F \in \mathbf{Z}$. Hence, $F \equiv z \pmod R$ and $m_0 \equiv xz^{-1} \equiv \widehat{m}_0 \pmod R$, $m_1 \equiv \widehat{m}_1 \pmod R$. Since $0 < m_0, m_1, \widehat{m}_0, \widehat{m}_1 < R$, it follows that $m_0 = \widehat{m}_0$ and $m_1 = \widehat{m}_1$. □

Clearly, this scheme can also be used for generating signatures, since Theorem 4.6 still holds if e and d are exchanged.

5. Security

For the security analysis of our scheme, we require a number of lemmas.

Lemma 5.1. *Let* $\alpha = a_0 + a_1\delta + \delta^2$, $\gamma = c_0 + c_1\delta + \delta^2$, $a_0, a_1, c_0, c_1 \in \mathbf{Z}$, $\gcd(a_0a_1c_0c_1, R) = 1$. *If* $\alpha^3(\gamma')^3 = \gamma^3(\alpha')^3$, *then* $\alpha = \alpha_i$ *for some* $i \in \{0, 1, 2\}$ *where* $\alpha_i = f_i^{-1}\gamma\delta^i$ *and*

$$f_i = \begin{cases} 1 & \text{if} \quad i = 0, \\ c_1 & \text{if} \quad i = 1, \\ c_0 & \text{if} \quad i = 2. \end{cases}$$

Hence, $\alpha_i = a_{i,0} + a_{i,1}\delta + \delta^2$ *where*

$$a_{i,0} = \begin{cases} c_0 & \text{if} \quad i = 0, \\ Dc_1^{-1} & \text{if} \quad i = 1, \\ Dc_1c_0^{-1} & \text{if} \quad i = 2, \end{cases} \qquad a_{i,1} = \begin{cases} c_1 & \text{if} \quad i = 0, \\ c_0c_1^{-1} & \text{if} \quad i = 1, \\ Dc_0^{-1} & \text{if} \quad i = 2. \end{cases}$$

Proof. If $(\alpha\gamma')^3 = (\gamma\alpha')^3$, then $(\alpha\gamma' - \gamma\alpha')(\alpha\gamma' - \zeta\gamma\alpha')(\alpha\gamma' - \zeta^2\gamma\alpha') = 0$, hence $\alpha\gamma' = \zeta^i\gamma\alpha'$ for some $i \in \{0, 1, 2\}$. Comparing coefficients of 1, δ, and δ^2 yields

$$\begin{aligned} a_0c_0 + a_1D\zeta^2 + c_1D\zeta &= a_0c_0\zeta^i + a_1D\zeta^{i+1} + c_1D\zeta^{i+2}, \\ a_0c_1\zeta + a_1c_0 + D\zeta^2 &= a_0c_1\zeta^i + a_1c_0\zeta^{i+1} + D\zeta^{i+2}, \\ a_0\zeta^2 + a_1c_1\zeta + c_0 &= a_0\zeta^i + a_1c_1\zeta^{i+1} + c_0\zeta^{i+2}. \end{aligned}$$

Solving for a_0 and a_1 for each $i \in \{0, 1, 2\}$ yields the result. □

Corollary 5.2. *Let* α, γ *be as in Lemma* 5.1. *If* $\alpha^3(\gamma')^3 \equiv \gamma^3(\alpha')^3 \pmod{\rho}$, *then* $\alpha \equiv \alpha_i \equiv f_i^{-1}\gamma\delta^i \pmod{\pi}$, $\alpha \equiv \alpha_j \equiv f_j^{-1}\gamma\delta^j \pmod{\psi}$ *for some* $i, j \in \{0, 1, 2\}$.

Lemma 5.3. *Let* α, γ *be as in Lemma* 5.1 *and let* $\alpha^3(\gamma')^3 \equiv \gamma^3(\alpha')^3 \pmod{\rho}$. *Then there exists* $i \in \{0, 1, 2\}$ *such that* $\alpha \equiv \alpha_i \equiv f_i^{-1}\gamma\delta^i \pmod{\rho}$ *if and only if* $[N(\alpha)/\rho] = [N(\gamma)/\rho]$.

Proof. By Corollary 5.2, $\alpha \equiv f_i^{-1}\gamma\delta^i \pmod{\pi}$, $\alpha \equiv f_j^{-1}\gamma\zeta^j \pmod{\psi}$ for some $i, j \in \{0, 1, 2\}$, so $N(\alpha) \equiv f_i^{-3}N(\gamma)D^i \pmod{p}$ and $N(\alpha) \equiv f_j^{-3}N(\gamma)D^j \pmod{q}$. Therefore $[N(\alpha)/\pi] = [N(\gamma)/\pi][D/\pi]^i$ and $[N(\alpha)/\psi] = [N(\gamma)/\psi][D/\psi]^j$. Since $[D/\psi] = [D/\pi]^{-1}$, it follows that $[N(\alpha)/\rho] = [N(\gamma)/\rho][D/\pi]^{i-j}$. Now $[D/\pi] \neq 1$, so $[N(\alpha)/\rho] = [N(\gamma)/\rho]$ if and only if $i = j$. □

Lemma 5.4. *Let* $\gamma = c_0 + c_1\delta + \delta^2$, $c_0, c_1 \in \mathbf{Z}$, $\gcd(c_0c_1, R) = 1$, $[N(\gamma)/\rho] \neq 1$. *Then there are exactly three solutions* $\alpha = a_0 + a_1\delta + \delta^2$ *to the congruence* $\alpha^3(\gamma')^3 \equiv \gamma^3(\alpha')^3 \pmod{\rho}$ *such that* $a_0, a_1 \in \mathbf{Z}$, $\gcd(a_0a_1, R) = 1$, *and* $[N(\alpha)/\rho] = 1$.

Proof. By Corollary 5.2, $\alpha \equiv \alpha_i \equiv f_i^{-1}\gamma\delta^i \pmod{\pi}$, $\alpha \equiv \alpha_i \equiv f_j^{-1}\gamma\delta^j \pmod{\psi}$ for some $i, j \in \{0, 1, 2\}$. From the proof of Lemma 5.3, $[N(\alpha)/\rho] = [N(\gamma)/\rho][D/\pi]^{i-j}$. We must have $i \neq j$ as otherwise $[N(\alpha)/\rho] = [N(\gamma)/\rho] \neq 1$. Since $[D/\pi] \neq 1$, there are exactly three pairs (i, j), $0 \leq i, j \leq 2$ such that $i \neq j$ and $[N(\gamma)/\rho][D/\pi]^{i-j} = 1$. □

Corollary 5.5. *Let $\alpha = a_0 + a_1\delta + \delta^2$, $\gamma = c_0 + c_1\delta + \delta^2$ be as in Lemma* 5.4. *For $k \in \{0, 1, 2\}$, let $\gamma_k = c_{k,0} + c_{k,1}\delta + \delta^2$ where*

$$c_{k,0} \equiv \begin{cases} c_0 \pmod{R} & \text{if} \quad k = 0, \\ Dc_1^{-1} \pmod{R} & \text{if} \quad k = 1, \\ Dc_1c_0^{-1} \pmod{R} & \text{if} \quad k = 2, \end{cases}$$

$$c_{k,1} \equiv \begin{cases} c_1 \pmod{R} & \text{if} \quad k = 0, \\ c_0c_1^{-1} \pmod{R} & \text{if} \quad k = 1, \\ Dc_0^{-1} \pmod{R} & \text{if} \quad k = 2. \end{cases}$$

Then $p = \gcd(a_0 - c_{i,0}, R)$ or $p = \gcd(a_1 - c_{i,1}, R)$ for some $i \in \{0, 1, 2\}$.

Proof. $\gamma_k \equiv f_k^{-1}\gamma\delta^k \pmod{\rho}$ where

$$f_k \equiv \begin{cases} 1 \pmod{R} & \text{if} \quad k = 0, \\ c_1 \pmod{R} & \text{if} \quad k = 1, \\ c_0 \pmod{R} & \text{if} \quad k = 2. \end{cases}$$

By Lemma 5.4, $\alpha \equiv \gamma_i \pmod{\pi}$, $\alpha \equiv \gamma_j \pmod{\psi}$ where $i, j \in \{0, 1, 2\}$ satisfy $[N(\gamma)/\rho][D/\pi]^{i-j} = 1$. In particular, $i \neq j$. It follows that

$$\begin{aligned} a_0 &\equiv c_{i,0} \pmod{p}, & a_1 &\equiv c_{i,1} \pmod{p}, \\ a_0 &\equiv c_{j,0} \pmod{q}, & a_1 &\equiv c_{j,1} \pmod{q}. \end{aligned}$$

If $c_{i,0} \not\equiv c_{j,0} \pmod{p}$, then $p \mid a_0 - c_{i,0}$, $q \nmid a_0 - c_{i,0}$, so $p = \gcd(a_0 - c_{i,0}, R)$. If $c_{i,0} \equiv c_{j,0} \pmod{p}$, then $c_{i,1} \not\equiv c_{j,1} \pmod{p}$ as otherwise $\alpha \equiv \gamma_j \pmod{\rho}$, i.e., $i = j$, contradicting Lemma 5.3. Hence by analogous reasoning, $p = \gcd(a_1 - c_{i,1}, R)$. □

Corollary 5.5 shows that knowledge of two algebraic integers α, γ satisfying the conditions of Lemma 5.4 yields the factorization of the modulus R.

Lemma 5.6. *Let $\gamma = c_0 + c_1\delta + \delta^2$, $c_0, c_1 \in \mathbf{Z}$, $\gcd(c_0c_1, R) = 1$, and $[N(\gamma)/\rho] \neq 1$. Let E_1, E_2, l, n be the quantities defined by applying Steps* 4–6 *of the encryption method to $\theta = \gamma/\gamma'$ in place of β. Then there exists $\alpha = a_0 + a_1\delta + \delta^2$ such that $a_0, a_1 \in \mathbf{Z}$, $\gcd(a_0a_1, R) = 1$, $[N(\alpha)/\rho] = 1$, $\alpha^3(\gamma')^3 \equiv \gamma^3(\alpha')^3 \pmod{\rho}$, and the ciphertext corresponding to the message (a_0, a_1) is $C = (E_1, E_2, l, 0, n)$.*

Proof. It suffices to show that one of the three solutions given by Lemma 5.4 corresponds to the desired ciphertext. Let α_0 be any one of the solutions, then all three solutions

are given by $\alpha_i \equiv g_i^{-1}\alpha_0\delta^i \pmod{\rho}$ for suitable $g_i \in \mathbf{Z}$, $i = 0, 1, 2$. Note that $m = 0$ in the ciphertexts corresponding to all three α_i. Let $\beta = \alpha_0/\alpha_0'$ and let $\beta_0, \beta_1, \beta_2$ be the values obtained in Step 4 of the encryption process. Since $\alpha_i/\alpha_i' \equiv (\alpha_0/\alpha_0')\zeta^{-i} \pmod{\rho}$ for $i = 0, 1, 2$, we see that $\{(\alpha_i/\alpha_i') \mid i = 0, 1, 2\} = \{\beta_0, \beta_1, \beta_2\}$. Identify α_i such that $\beta_n = \alpha_i/\alpha_i'$ and set $\alpha = \alpha_i$. Then α and γ have the same value of n in their respective ciphertext.

Now, by Corollary 5.2, $\alpha \equiv f_i^{-1}\gamma\delta^i \pmod{\pi}$, $\alpha \equiv f_j^{-1}\gamma\delta^j \pmod{\psi}$ for some $i, j \in \{0, 1, 2\}$ and suitable $f_i, f_j \in \mathbf{Z}$, so $\beta_n \equiv \theta\zeta^{-i} \pmod{\pi}$ and $\beta_n \equiv \theta\zeta^{-j} \pmod{\psi}$. Therefore, Step 6 of the encryption algorithm yields the same values of l, E_1, and E_2 for both β_n and θ. □

It is now possible to show that the problem of breaking our system is equivalent to the difficulty of factoring the modulus R in the following sense.

Theorem 5.7. *If $\mathcal{A}$ is an algorithm that decrypts any ciphertext $C = (E_1, E_2, l, m, n)$, then $\mathcal{A}$ can be used to factor R.*

Proof. Let $\gamma = c_0 + c_1\delta + \delta^2$ be such that $c_0, c_1 \in \mathbf{Z}$, $\gcd(c_0c_1, R) = 1$, and $[N(\gamma)/\rho] \neq 1$ (note that φ as defined in Step 5 of the key generation is a possible candidate for γ). Set $\theta = \gamma/\gamma'$ and $m = 0$ (a false value for m in the ciphertext corresponding to the "message" (c_0, c_1)). Apply Steps 4–6 of the encryption routine to θ, obtaining a ciphertext $C = (E_1, E_2, l, 0, n)$. Applying $\mathcal{A}$ to C yields a "message" (a_0, a_1) where $\alpha = a_0 + a_1\delta + \delta^2$ satisfies $[N(\alpha)/\rho] = 1$ by Lemma 5.6. For $k = 0, 1, 2$, compute $\gamma_k = c_{k,0} + c_{k,1}\delta + \delta^2$ where the γ_k are defined as in Corollary 5.5. Then by the same corollary, $p = \gcd(a_0 - c_{i,0}, R)$ or $p = \gcd(a_1 - c_{i,1}, R)$ for some $i \in \{0, 1, 2\}$. □

If $\mathcal{A}$ decrypts a fraction $1/k$ of all ciphertexts, we expect to be able to factor R using $\mathcal{A}$ after k trials at a value of γ.

Unfortunately, the method described in Theorem 5.7 can be used for a chosen ciphertext attack, if an adversary is able to convince a decrypter to decipher the ciphertext corresponding to an algebraic integer γ where $[N(\gamma)/\rho] \neq 1$ and reveal the corresponding plaintext.

6. Algorithms

In this section we give two algorithms required for implementing our cryptosystem. The first algorithm computes the residuacity character $[\kappa/\omega]$, $\kappa, \omega \in \mathbf{Z}[\zeta]$, without making use of the factorization of ω in $\mathbf{Z}[\zeta]$. Both the method and the underlying tools are analogous to those used for computing Jacobi symbols in $\mathbf{Z}$ (see [19], [18], and [14]). The second algorithm finds for a rational prime $p \equiv 1 \pmod{3}$ a prime divisor π in $\mathbf{Z}[\zeta]$ (see [14]).

An algebraic integer $\kappa = k_0 + k_1\zeta$, $k_0, k_1 \in \mathbf{Z}$, is said to be *primary* if $k_0 \equiv 0 \pmod{3}$ and $k_1 \equiv 2 \pmod{3}$. It is easy to see that, for any $\kappa \in \mathbf{Z}[\zeta]$, exactly one of $\pm\kappa$, $\pm\zeta\kappa$, and $\pm\zeta^2\kappa$ is primary. Primary integers $\kappa, \omega \in \mathbf{Z}[\zeta]$ that are relatively prime

satisfy the *cubic law of reciprocity* $[\kappa/\omega] = [\omega/\kappa]$. The *complementaries* give the values of the residuacity character $[\kappa/\omega]$ for certain special values of κ, namely $[\pm 1/\omega] = 1$, $[\zeta/\omega] = \zeta^{(1/3)(N(\omega)-1)}$, and $[(1-\zeta)/\omega] = \zeta^{(2/3)(w_0+1)}$ where $\omega = w_0 + w_1\zeta$ is primary (see pp. 113ff. of [6]). Note that $1-\zeta$ is the only prime divisor in $\mathbf{Z}[\zeta]$ of 3.

Computing residuacity characters. For $\kappa, \omega \in \mathbf{Z}[\zeta]$ relatively prime, we can now compute $[\kappa/\omega]$ as follows. First, we find the unique primary integer $\widetilde{\omega} = \pm\zeta^i\omega$, $i \in \{0, 1, 2\}$. Then we compute $\varphi, \lambda \in \mathbf{Z}[\zeta]$ such that $\kappa = \varphi\omega + \lambda$ and $\lambda\overline{\lambda} < \kappa\overline{\kappa}$. This process is called *Euclidean division* and is the analogue in $\mathbf{Z}[\zeta]$ to division with remainder in $\mathbf{Z}$. We describe below how to find φ and λ. Next, we extract powers of $1-\zeta$ from λ to obtain $\hat{\lambda}$ such that $\lambda = \hat{\lambda}(1-\zeta)^j$ for some $j \geq 0$ and $1-\zeta \nmid \hat{\lambda}$ in $\mathbf{Z}[\zeta]$ (or equivalently, $3 \nmid \hat{\lambda}\overline{\hat{\lambda}}$ in $\mathbf{Z}$). Finally, we determine the unique primary integer $\widetilde{\lambda} = \pm\zeta^k\hat{\lambda}$, $k \in \{0, 1, 2\}$, and apply the cubic law of reciprocity to $[\widetilde{\lambda}/\widetilde{\omega}]$. Then from the complementaries,

$$\begin{aligned}\left[\frac{\kappa}{\omega}\right] &= \left[\frac{\kappa}{\widetilde{\omega}}\right] = \left[\frac{\lambda}{\widetilde{\omega}}\right] = \left[\frac{\hat{\lambda}}{\widetilde{\omega}}\right]\left[\frac{1-\zeta}{\widetilde{\omega}}\right]^j = \left[\frac{\widetilde{\lambda}}{\widetilde{\omega}}\right]\left[\frac{\zeta}{\widetilde{\omega}}\right]^{-k}\left[\frac{1-\zeta}{\widetilde{\omega}}\right]^j \\ &= \left[\frac{\widetilde{\omega}}{\widetilde{\lambda}}\right]\zeta^{(1/3)(1-N(\omega))k+(2/3)(\tilde{w}_0+1)j},\end{aligned}$$

where $\widetilde{\omega} = \widetilde{w}_0 + \widetilde{w}_1\zeta$. We can now repeat the procedure with $[\widetilde{\omega}/\widetilde{\lambda}]$ in place of $[\kappa/\omega]$. Since $\kappa\overline{\kappa}$ is a positive rational integer which strictly decreases in each iteration, the algorithm must eventually terminate with a primary value of κ such that $\kappa\overline{\kappa} = 1$, i.e., $\kappa = -\zeta$, at which point $[\kappa/\omega]$ can be evaluated directly from the appropriate complementary. It can be shown that the total number of iterations is essentially the same as the number of division with remainder steps required to compute $\gcd(\kappa\overline{\kappa}, \omega\overline{\omega})$, i.e., $O(\log \omega\overline{\omega})$.

Euclidean division in $\mathbf{Z}[\zeta]$. For $\kappa, \omega \in \mathbf{Z}[k]$, integers $\varphi, \lambda \in \mathbf{Z}[\zeta]$ such that $\kappa = \varphi\omega + \lambda$ and $\lambda\overline{\lambda} < \omega\overline{\omega}$ can be found as follows. Define $x_0, x_1 \in \mathbf{Q}$ by $\kappa/\omega = \kappa\overline{\omega}/\omega\overline{\omega} = x_0 + x_1\zeta$. Set $y_0 = \mathrm{Ne}(x_0)$, $y_1 = \mathrm{Ne}(x_1)$, where for $z \in \mathbf{Q}$, $\mathrm{Ne}(z)$ denotes the nearest rational integer to z, i.e., $|z - \mathrm{Ne}(z)| \leq \frac{1}{2}$. Set $\varphi = y_0 + y_1\zeta$ and $\lambda = \kappa - \varphi\omega$. Then $\varphi, \lambda \in \mathbf{Z}[\zeta]$, $\kappa = \varphi\omega + \lambda$, and

$$\frac{\lambda\overline{\lambda}}{\omega\overline{\omega}} = \left(\frac{\kappa}{\omega} - \varphi\right)\overline{\left(\frac{\kappa}{\omega} - \varphi\right)} = (x_0 - y_0)^2 - (x_0 - y_0)(x_1 - y_1) + (x_1 - y_1)^2 \leq \frac{3}{4},$$

so $\lambda\overline{\lambda} \leq \frac{3}{4}\omega\overline{\omega} < \omega\overline{\omega}$. We point out that a more general, but slightly more complicated technique due to Lenstra [8] yields $\lambda\overline{\lambda} \leq \frac{1}{3}\omega\overline{\omega}$.

If we set $M = \max\{\kappa\overline{\kappa}, \omega\overline{\omega}\}$, then Euclidean division requires $O((\log M)^2)$ bit operations using standard arithmetic and $O(\log M \log\log M \log\log\log M)$ bit operations using fast arithmetic. Hence in the cryptosystem, the value of $[N(\alpha)/\rho]$ can be computed in $O((\log R)^3)$ standard bit operations and in $O((\log R)^2 \log\log R \log\log\log R))$ fast bit operations.

Computing greatest common divisors and prime divisors. The Euclidean division technique can be used to compute greatest common divisors in $\mathbf{Z}[\zeta]$ in the same fashion as

division with remainder in $\mathbf{Z}$ generates rational gcd's. For $\kappa, \omega \in \mathbf{Z}[\zeta]$, simply perform Euclidean division repeatedly, until the curent remainder is zero, at which point the previous remainder yields the greatest common divisor of κ and ω (unique up to sign and factors ζ^k, $k \in \{0, 1, 2\}$). The gcd is found after $O(\log \max\{\kappa\overline{\kappa}, \omega\overline{\omega}\})$ Euclidean division steps.

In this way, a prime divisor π of a rational prime $p \equiv 1 \pmod 3$ can be found by computing $\pi = \gcd(p, \zeta - r)$ where r is defined as in Step 1 of the precomputation in Section 4. This requires $O(\log R)$ Euclidean divisions.

As is the case with the rational Euclidean algorithm, this gcd algorithm can be extended to yield a pair of integers $\xi, \eta \in \mathbf{Z}[\zeta]$ such that $\kappa\xi + \omega\eta = \gcd(\kappa, \omega)$. If we compute $[N/\rho]$ for a rational integer $N \pmod R$, we can compute $N^{-1} \pmod R$ at the same time. Simply keep track of the outputs of each Euclidean division and use them to compute a representation $N\xi + \rho\eta = \gcd(N, \rho) = \pm\zeta^k$ for some $k \in \{0, 1, 2\}$. Multiplying this equation by its complex conjugate yields $N^2\xi\overline{\xi} + N\xi\overline{\rho\eta} + N\overline{\xi}\rho\eta + R\eta\overline{\eta} = 1$, so the inverse of $N \pmod R$ is the rational integer $N\xi\overline{\xi} + \xi\overline{\rho\eta} + \overline{\xi}\rho\eta \pmod R$. This computation does not increase the overall asymptotic complexity of the residuacity symbol computation.

The above results show that the overall asymptotic bit complexity of encryption is $O((\log R)^3)$ using standard arithmetic and $O(\log R \log\log R \log\log\log R)$ using fast arithmetic, regardless of the size of the encryption exponent e. For large values of e, this is the same as RSA; however, if a small encryption exponent is used (as is commonly done with RSA), then this is worse than RSA by a factor of $\log R$. Since the decryption exponent is usually of size $2 \log R$ (rather than $\log R$ for an RSA exponent), decryption of our system requires slightly more than twice the effort of RSA decryption, although asymptotically their respective complexities are identical and equal to the bit complexity of encryption.

Acknowledgment

The author wishes to thank Mark Giesbrecht and Hugh Williams as well as the referee for their helpful suggestions.

References

[1] E. Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, Ph.D. Dissertation, MIT Press, Cambridge, Massachusetts, 1985.
[2] B. N. Delone and D. K. Fadeev, *The Theory of Irrationalities of the Third Degree*, American Mathematical Society, Providence, Rhode Island, 1964.
[3] L. E. Dickson, Cyclotomy, higher congruences, and Waring's problem, *Amer. J. Math.*, vol. 57 (1935), pp. 391–424.
[4] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1993.
[5] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Z.*, vol. 31 (1930), pp. 565–582.
[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Springer-Verlag, New York, 1990.
[7] D. E. Knuth, *The Art of Computer Programming*, vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, Massachusetts, 1981.

[8] H. W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, *J. London Math. Soc.* (2), vol. 10 (1975), pp. 457–465.
[9] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edtion, Cambridge University Press, Cambridge, 1997.
[10] J. Loxton, D. S. P. Khoo, G. J. Bird, and J. Seberry, A cubic RSA code equivalent to factorization, *J. Cryptology*, vol. 5, no. 2 (1992), pp. 139–150.
[11] M. O. Rabin, Digitized Signatures and Public-Key Functions as Intractable as Factorization, Tech. Report LCS/TR-212, M.I.T. Laboratory for Computer Science, Cambridge, Massachusetts, 1979.
[12] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, vol. 21, no. 2 (1978), pp. 120–126.
[13] A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, Berlin, 1990.
[14] R. Scheidler, Applications of Algebraic Number Theory to Cryptography, Ph.D. Dissertation, University of Manitoba, 1993.
[15] R. Scheidler and H. C. Williams, A public-key cryptosystem utilizing cyclotomic fields, *Designs, Codes and Cryptography*, vol. 6 (1995), pp. 117–131.
[16] H. C. Williams, A modification of the RSA public-key encryption procedure, *IEEE Trans. Inform. Theory*, vol. 26, no. 6 (1980), pp. 726–729.
[17] H. C. Williams, Some public-key crypto-function as intractable as factorization, *Cryptologia*, vol. 9, no. 3 (1985), pp. 223–237.
[18] H. C. Williams, An M^3 public-key encryption scheme, *Advances in Cryptology – CRYPTO* '85 *Proceedings*, Springer-Verlag, Berlin, 1986, pp. 358–368.
[19] H. C. Williams and R. Holte, Computation of the solution of $x^3 + Dy^3 = 1$, *Math. Comp.*, vol. 31, no. 139 (1977), pp. 778–785.