Designs, Codes and Cryptography, 6, 117–131 (1995)


# A Public-Key Cryptosystem Utilizing Cyclotomic Fields

RENATE SCHEIDLER scheidle@math.udel.edu
*Department of Mathematical Sciences, University of Delaware, Newark, DE 19716*

HUGH C. WILLIAMS hugh_williams@csmail.cs.umanitoba.ca
*Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2*

**Communicated by:** R. Mullin

*Received January 14, 1994*

**Abstract.** While it is well-known that the RSA public-key cryptosystem can be broken if its modulus $N$ can be factored, it is not known whether there are other ways of breaking RSA. This paper presents a public-key scheme which necessarily requires knowledge of the factorization of its modulus in order to be broken. Rabin introduced the first system whose security is equivalent to the difficulty of factoring the modulus. His scheme is based on squaring (cubing) for encryption and extracting square (cube) roots for decryption. This introduces a 1:4 (1:9) ambiguity in the decryption. Various schemes which overcome this problem have been introduced for both the quadratic and cubic case. We generalize the ideas of Williams' cubic system to larger prime exponents. The cases of higher prime order introduce a number of problems not encountered in the quadratic and cubic cases, namely the existence of fundamental units in the underlying cyclotomic field, the evaluation of higher power residue symbols, and the increased difficulty of Euclidean division in the field.

**Keywords:** Public-key cryptosystem, cyclotomic field, residue symbol, Euclidean division

## 1. Introduction

It is well-known that the RSA public-key cryptosystem can be broken if its modulus $N$ can be factored. However, it is not known if the opposite is true, i.e. whether there are other methods of breaking RSA. It is therefore of interest to develop cryptographic schemes whose security is equivalent to the difficulty of factoring the modulus, i.e. for which knowledge of the factorization of the modulus is necessary in order to retrieve plaintext from ciphertext without the use of the decryption key. Rabin [12] introduced the first such system, in which encryption is essentially squaring the message modulo $N$, and decryption is extracting square roots modulo the factors $p$ and $q$ of $N$. The main problem with this method is a 1:4 ambiguity in the decryption. Rabin pointed out that the same technique could be used when cubing the message for encryption and would result in a 1:9 ambiguity in the decrypted text. In order to distinguish the correct root for decryption, the required information needs to be either included in the encryption/decryption algorithms or transmitted together with the encrypted message. The former approach was taken by Williams [15] in the quadratic case and recently by Loxton, Khoo, Bird and Seberry [9] in the cubic case. The latter idea was used by Williams [16] who presented a cubic scheme based on arithmetic in the complex quadratic field generated by a primitive cube root of unity.

In this paper, we present an RSA-like cryptosystem which can be used with higher prime exponents as well. The scheme itself is a generalization of Williams' system [16] to Euclidean cyclotomic fields of higher prime order. It solves Rabin's ambiguity problem and its security is equivalent to the difficulty of factoring the modulus. Key generation and encryption employ some interesting number theoretic concepts and algorithms which do not occur in the simpler quadratic and cubic cases. We present an algorithm for Euclidean division in cyclotomic fields. We also make use of higher power residue symbols—generalizations of the Jacobi and Legendre symbols—and give a method for computing them without factoring the denominator. Finally, we address the problem of evaluating these symbols for units, i.e. for nontrivial divisors of 1 in the field.

It should be noted that for any system of this kind, there is a price to pay for the additional information regarding its security. Certain restrictions need to be placed on the primes $p$, $q$ (and thus on the modulus $N = pq$). The mechanisms for key generation as well as encryption and decryption are more complex than those for RSA and require more computation. The public key is larger than an RSA key. Finally, since the proof of the equivalence of breaking the scheme to the difficulty of factoring its modulus is constructive, the system could be vulnerable to a chosen ciphertext attack (see [15]).

The paper is organized as follows. The following section presents the mathematical concepts used in our cryptosystem. The scheme itself is introduced in Section 3 and its security is analyzed in Section 4. Section 5 discusses the underlying algorithms in more detail. The paper concludes with an explicit description and computational results for the quintic case in Section 6.

## 2. Mathematical Preliminaries

Let $\lambda$ be a prime and $\zeta$ be a primitive $\lambda$-th root of unity, i.e. $\zeta \neq 1$ and $\zeta^\lambda = 1$. By adjoining $\zeta$ to the field $\mathbf{Q}$ of rationals, we obtain an algebraic number field $\mathbf{F} = \mathbf{Q}(\zeta)$ of degree $\lambda - 1$ over $\mathbf{Q}$, *the cyclotomic field of order* $\lambda$. Every $\alpha \in \mathbf{F}$ has a unique representation $\alpha = a_1\zeta + a_2\zeta^2 + \cdots + a_{\lambda-1}\zeta^{\lambda-1}$ where $a_1, \ldots, a_{\lambda-1} \in \mathbf{Q}$.

Denote by $\mathbf{R} = \mathbf{Z}[\zeta] = \mathbf{Z}\zeta + \cdots + \mathbf{Z}\zeta^{\lambda-1}$ the *ring of algebraic integers* in $\mathbf{F}$, where $\mathbf{Z}$ is the set of rational integers. We define the $\lambda - 1$ *conjugate mappings* $\sigma_i : \mathbf{F} \to \mathbf{F}$ by $\sigma_i(\zeta) = \zeta^i$ for $1 \leq i \leq \lambda - 1$. The two rational numbers $N(\alpha) = \prod_{i=1}^{\lambda-1} \sigma_i(\alpha) \in \mathbf{Q}^{\geq 0}$ and $\mathrm{Tr}(\alpha) = \sum_{i=1}^{\lambda-1} \sigma_i(\alpha) \in \mathbf{Q}$ are called the *norm* and *trace* of $\alpha \in \mathbf{F}$, respectively. Then $N(\mathbf{R}), \mathrm{Tr}(\mathbf{R}) \subseteq \mathbf{Z}$ and $N(\alpha\beta) = N(\alpha)N(\beta)$, $\mathrm{Tr}(a\alpha + b\beta) = a\,\mathrm{Tr}(\alpha) + b\,\mathrm{Tr}(\beta)$ for any $\alpha, \beta \in \mathbf{F}, a, b \in \mathbf{Q}$.

A *unit* in $\mathbf{F}$ is a divisor (in $\mathbf{R}$) of 1, or equivalently, an element in $\mathbf{R}$ of norm 1. Two elements $\alpha, \beta \in \mathbf{R}$ are said to be *associates* if there exists a unit $\varepsilon$ such that $\alpha = \varepsilon\beta$.

A *prime* $\pi$ in $\mathbf{R}$ is an element in $\mathbf{R}$ such that for any $\alpha, \beta \in \mathbf{R}$, if $\pi \mid \alpha\beta$ in $\mathbf{R}$, then $\pi \mid \alpha$ or $\pi \mid \beta$ in $\mathbf{R}$. $\omega = -2\zeta - \zeta^2 - \zeta^3 - \cdots - \zeta^{\lambda-1} = 1 - \zeta$ is a prime in $\mathbf{R}$ and $N(\omega) = \lambda$. If $\pi \neq \omega$ is a prime in $\mathbf{R}$, then $N(\pi) = p^k$ where $p$ is a prime in $\mathbf{Z}$ and $k$ is the order of $p$ modulo $\lambda$, hence $N(\pi) \equiv 1 (\mathrm{mod}\, \lambda)$.

Let $\alpha \in \mathbf{R}$, $\alpha \neq 0$, and let $\pi \in \mathbf{R}$ be a prime which does not divide $\alpha$. Since $\alpha^{N(\pi)-1} \equiv 1 (\mathrm{mod}\, \pi)$, we can define the *$\lambda$-th residue symbol* as

$$\left[\frac{\alpha}{\pi}\right] = \zeta^k$$

where $k$ is such that $\alpha^{\frac{N(\pi)-1}{\lambda}} \equiv \zeta^k (\mathrm{mod}\, \pi)$ and $0 \leq k \leq \lambda - 1$.

Assume now that $\mathbf{R}$ is a *Unique Factorization Domain* (UFD)—this restricts our scheme to the fields where $\lambda \leq 19$ (see Masley & Montgomery [10]). Then we can define

$$\left[\frac{\alpha}{\beta}\right] = \prod_{i=1}^{r} \left[\frac{\alpha}{\pi_i}\right]^{e_i},$$

where $\beta \in \mathbf{R}$, $\beta \neq 0$, and $\beta = \prod_{i=1}^{r} \pi_i^{e_i}$ is the unique prime factorization (up to order and unit factors) of $\beta$ in $\mathbf{R}$.[1] (This is well-defined since for any unit $\varepsilon$, $\left[\frac{\alpha}{\varepsilon}\right] = \left[\frac{\alpha}{\pi_1}\right]\left[\frac{\alpha}{\pi_2}\right]^{-1} = 1$, where $\pi_1 = \varepsilon\pi_2$.) It is easy to see that $\left[\frac{\alpha\gamma}{\beta}\right] = \left[\frac{\alpha}{\beta}\right]\left[\frac{\gamma}{\beta}\right]$ and $\left[\frac{\alpha}{\beta}\right] = \left[\frac{\gamma}{\beta}\right]$ if $\alpha \equiv \gamma (\mathrm{mod}\, \beta)$ for any $\alpha, \beta, \gamma \in \mathbf{R}$, $\beta \neq 0$.

## 3. The Cryptosystem

Henceforth, let $p, q \in \mathbf{Z}$ be primes such that $p \equiv q \equiv 1 (\mathrm{mod}\, \lambda)$ and $p, q \not\equiv 1 (\mathrm{mod}\, \lambda^2)$. Set $N = pq$ and $f = \frac{\phi(N)}{\lambda^2}$, where $\phi$ denotes Euler's totient function, i.e. $\phi(N) = (p-1)(q-1)$. Then $\lambda^2 \mid \phi(N)$ and $\lambda \nmid f$. Let $e, d \in \mathbf{Z}$ be such that $\lambda ed \equiv 1 (\mathrm{mod}\, f)$. Finally, define primes $\pi, \psi \in \mathbf{R}$ such that $N(\pi) = p$, $N(\psi) = q$, and $r \in \mathbf{Z}$ such that $gcd(r-1, N) = 1$, $r^\lambda \equiv 1 (\mathrm{mod}\, N)$, and $\left[\frac{r}{\pi\psi}\right] = 1$. The basis for our scheme is the following theorem.

THEOREM 3.1 *Let $X \in \mathbf{Z}$ be such that $gcd(X, N) = 1$ and $\left[\frac{X}{\pi\psi}\right] = 1$. Then $X^f \equiv r^k (\mathrm{mod}\, N)$ for some $k \in \{0, \ldots, \lambda - 1\}$.*

*Proof.* Let $\left[\frac{X}{\pi}\right] = \zeta^i$, $\left[\frac{r}{\pi}\right] = \zeta^j$, $0 \leq i, j \leq \lambda - 1$. Since $\left[\frac{X}{\pi\psi}\right] = \left[\frac{r}{\pi\psi}\right] = 1$, we have $\left[\frac{X}{\psi}\right] = \zeta^{\lambda - i}$, $\left[\frac{r}{\psi}\right] = \zeta^{\lambda - j}$. Then $r^\lambda \equiv \left[\frac{r}{\pi}\right] \equiv \zeta^j (\mathrm{mod}\, \pi)$ and $r^{\frac{q-1}{\lambda}} \equiv \left[\frac{r}{\psi}\right] \equiv \zeta^{-j} (\mathrm{mod}\, \psi)$. Since $gcd(r-1, N) = 1$, we have $r \not\equiv 1 (\mathrm{mod}\, p)$, hence $r \equiv \zeta^l (\mathrm{mod}\, \pi)$ for some $l \neq 0$, and $\zeta^j \equiv \left[\frac{r}{\pi}\right] \equiv r^{\frac{p-1}{\lambda}} \equiv \zeta^{\frac{p-1}{\lambda} l} \not\equiv 1 (\mathrm{mod}\, \pi)$ implies $j \neq 0$. Define $k$ such that $kj \equiv fi (\mathrm{mod}\, \lambda)$ and $0 \leq k \leq \lambda - 1$. Then $\zeta^{fi} \equiv \zeta^{jk} \equiv r^{\frac{p-1}{\lambda} k} (\mathrm{mod}\, \pi)$, so $\zeta^{\frac{q-1}{\lambda} i} \equiv r^k (\mathrm{mod}\, \pi)$; similarly $\zeta^{-\frac{p-1}{\lambda} i} \equiv r^k (\mathrm{mod}\, \psi)$. It follows that $X^f \equiv \left[\frac{X}{\pi}\right]^{\frac{q-1}{\lambda}} \equiv \zeta^{\frac{q-1}{\lambda} i} \equiv r^k (\mathrm{mod}\, \pi)$ and $X^f \equiv \left[\frac{X}{\psi}\right]^{\frac{p-1}{\lambda}} \equiv \zeta^{-\frac{p-1}{\lambda} i} \equiv r^k (\mathrm{mod}\, \psi)$. Since $X, r \in \mathbf{Z}$, we have $X^f \equiv r^k (\mathrm{mod}\, N)$. ∎

COROLLARY *If $Z \equiv X^{\lambda e} (\mathrm{mod}\, N)$, then $Z^d \equiv r^k X (\mathrm{mod}\, N)$ for some $k \in \{0, \ldots, \lambda - 1\}$.*

We are now prepared to present our scheme.

*Key Generation*:

1. Choose two large primes $p, q$ where $p, q \equiv 1 (\mathrm{mod}\, \lambda)$, $p, q \not\equiv 1 (\mathrm{mod}\, \lambda^2)$, and a large positive integer $e$ such that $0 < e < (p-1)(q-1)$ and $gcd(e, (p-1)(q-1)) = 1$.
2. Compute $N, f, d, \pi, \psi, r$ as above.
3. Calculate $\pi\psi = c_1\zeta + c_2\zeta^2 + \cdots + c_{\lambda-1}\zeta^{\lambda-1}$ where $c_1, \ldots, c_{\lambda-1} \in \mathbf{Z}$.
4. Find $S \in \mathbf{Z}$ such that $0 < S < N$ and $\left[\frac{S}{\pi\psi}\right] = \zeta^{\lambda-1}$.
5. Publicize $K = \{r, S, c_1, \ldots, c_{\lambda-1}, e\}$ and keep $d$ secret.

For step 4, we merely require $\left[\frac{S}{\pi\psi}\right] \neq 1$; the specification $\left[\frac{S}{\pi\psi}\right] = \zeta^{\lambda-1}$ serves to simplify our arithmetic. In order to find $S$, generate a random integer $T$ relatively prime to $N$ and compute $\left[\frac{T}{\pi\psi}\right] = \zeta^k, 0 \leq k \leq \lambda - 1$. If $k = 0$, try another $T$, otherwise set $S \equiv T^l (\mathrm{mod}\, N), 0 < S < N$, where $kl \equiv \lambda - 1 (\mathrm{mod}\, \lambda)$. Then $\left[\frac{S}{\pi\psi}\right] = \left[\frac{T}{\pi\psi}\right]^l = \zeta^{kl} = \zeta^{\lambda-1}$.

Note that $N = N(\pi\psi)$ is easily computed. Algorithms for finding $r$, $\pi$ and $\psi$ from $p$ and $q$ as well as evaluating residue symbols in the cases $\lambda = 2, 3, 5$ are given in Section 5.

As in RSA, messages are considered to be encoded as integer blocks $M$ such that $0 < M < N$. Note that any non-trivial common divisor of $M$ and $N$ is either $p$ or $q$, so it is extremely unlikely that a message is not relatively prime to $N$. Hence we may assume that $\gcd(M, N) = 1$ for any message $M$.

*Encryption*: Let $M \in \mathbf{Z}$ be a message, $0 < M < N$, $\gcd(M, N) = 1$. Encrypt $M$ as follows:

1. Determine $\left[\frac{M}{\pi\psi}\right] = \zeta^m, 0 \leq m \leq \lambda - 1$.
2. Compute $M_0 \equiv MS^m$, $M_i \equiv r^i M_0 (\mathrm{mod}\, N)$ such that $0 < M_i < N$ $(0 \leq i \leq \lambda - 1)$
3. Sort the $M_i$ in ascending order to obtain $\hat{M}_0 < \cdots < \hat{M}_{\lambda-1}$ where $\{\hat{M}_0, \ldots, \hat{M}_{\lambda-1}\} = \{M_0, \ldots, M_{\lambda-1}\}$. (Note that all $M_i$ are pairwise distinct.) Find $n$ such that $0 \leq n \leq \lambda - 1$ and $M_0 = \hat{M}_n$.
4. Compute $C \equiv M_0^{\lambda e} (\mathrm{mod}\, N), 0 < C < N$.
5. Transmit $\{C, m, n\}$.

*Decryption*: On receiving $\{C, m, n\}$:

1. Compute $L_0 \equiv C^d$, $L_i \equiv r^i L_0 (\mathrm{mod}\, N)$ such that $0 < L_i < N (0 \leq i \leq \lambda - 1)$.
2. Sort the $L_i$ in ascending order to obtain $\hat{L}_0 < \cdots < \hat{L}_{\lambda-1}$ where $\{\hat{L}_0, \ldots, \hat{L}_{\lambda-1}\} = \{L_0, \ldots, L_{\lambda-1}\}$. Find $j$ such that $0 \leq j \leq \lambda - 1$ and $L_j = \hat{L}_n$.

3. Compute $S^{-1} (\mathrm{mod}\, N)$. (This need only be done once for each key $K$).

4. Compute $M \equiv S^{-m} L_j (\mathrm{mod}\, N)$ such that $0 < M < N$.

We have $\left[\frac{M_i}{\pi\psi}\right] = \left[\frac{r}{\pi\psi}\right]^i \left[\frac{M}{\pi\psi}\right]\left[\frac{S}{\pi\psi}\right]^m = \zeta^m \zeta^{(\lambda-1)m} = 1$ for $0 \leq i \leq \lambda - 1$, so all $M_i$ satisfy Theorem 3.1. Furthermore, $\hat{M}_i = \hat{L}_i$ for $0 \leq i \leq \lambda - 1$, so the decrypter is in fact able to identify the correct root $M_0$ of $C^d (\mathrm{mod}\, N)$.

## 4. Security

In order to prove that breaking our scheme is as difficult as factoring $N$, we first require three lemmas which are generalizations of results in [16].

LEMMA 4.1 *Let $Y \in \mathbf{Z}$. Then there exists for any $i \in \{0, \ldots, \lambda - 1\}$ an integer $X_i$ such that $X_i^\lambda \equiv Y^\lambda (\mathrm{mod}\, N)$ and $\left[\frac{X_i}{\pi\psi}\right] = \zeta^i \left[\frac{Y}{\pi\psi}\right]$.*

*Proof.* Let $i \in \{0, \ldots, \lambda - 1\}$ and let $j \in \{1, \ldots, \lambda - 1\}$ be such that $\left[\frac{r}{\pi}\right] = \zeta^j$. Let $k_i \in \mathbf{Z}$ be such that $jk_i \equiv i (\mathrm{mod}\, \lambda)$. By the Chinese Remainder Theorem, there exists $X_i \in \mathbf{Z}$ such that $X_i \equiv r^{k_i} Y (\mathrm{mod}\, p)$ and $X_i \equiv Y (\mathrm{mod}\, q)$. Then $X_i^\lambda \equiv Y^\lambda (\mathrm{mod}\, N)$ and $\left[\frac{X_i}{\pi\psi}\right] = \left[\frac{X_i}{\pi}\right]\left[\frac{X_i}{\psi}\right] = \left[\frac{r}{\pi}\right]^{k_i}\left[\frac{Y}{\pi}\right]\left[\frac{Y}{\psi}\right] = \zeta^{jk_i}\left[\frac{Y}{\pi\psi}\right] = \zeta^i \left[\frac{Y}{\pi\psi}\right]$. ∎

LEMMA 4.2 *Let $Y \in \mathbf{Z}$ be such that $\gcd(Y, N) = 1$ and let $m, n \in \{0, \ldots, \lambda - 1\}$. If $C \equiv Y^\lambda (\mathrm{mod}\, N)$ and $0 < C < N$, then there exists a unique $M \in \mathbf{Z}$, $0 < M < N$, such that encrypting $M$ under key $K = \{r, S, c_1, \ldots, c_{\lambda-1}, e\}$ yields $\{C, m, n\}$.*

*Proof.* Let $g \in \mathbf{Z}$ be such that $ge \equiv 1 (\mathrm{mod}\, \phi(N))$. By the previous Lemma, there exists $X \in \mathbf{Z}$ such that $X^\lambda \equiv (Y^g)^\lambda (\mathrm{mod}\, N)$ and $\left[\frac{X}{\pi\psi}\right] = 1$. For $0 \leq i \leq \lambda - 1$, define $X_i \equiv r^i X (\mathrm{mod}\, N)$, $0 < X_i < N$. Sort the $X_i$ in ascending order, obtaining $\hat{X}_0 < \cdots < \hat{X}_{\lambda-1}$, where $\{X_0, \ldots, X_{\lambda-1}\} = \{\hat{X}_0, \ldots, \hat{X}_{\lambda-1}\}$ and let $k$ be such that $X_k = \hat{X}_n$. Set $M \equiv S^{-m} X_k (\mathrm{mod}\, N)$, $0 < M < N$. We need to prove that encrypting $M$ under $K$ gives $\{C, m, n\}$.

Step 1: $\left[\frac{M}{\pi\psi}\right] = \left[\frac{S}{\pi\psi}\right]^{-m}\left[\frac{r}{\pi\psi}\right]^k \left[\frac{X}{\pi\psi}\right] = \zeta^{-(\lambda-1)m} = \zeta^m$.

Step 2: $M_i \equiv M S^m r^i \equiv X_k r^i (\mathrm{mod}\, N), 0 < M_i < N, (0 \leq i \leq \lambda - 1)$, so $\{M_0, \ldots, M_{\lambda-1}\} = \{X_0, \ldots, X_{\lambda-1}\}$.

Step 3: After sorting, we have $\hat{M}_i = \hat{X}_i (0 \leq i \leq \lambda - 1)$ and $M_0 \equiv X_k \equiv \hat{X}_n \equiv \hat{M}_n$.

Step 4: $M_0^{\lambda e} \equiv X_k^{\lambda e} \equiv X^{\lambda e} \equiv Y^{\lambda g e} \equiv Y^\lambda \equiv C (\mathrm{mod}\, N)$.

Now since decrypting $\{C, m, n\}$ under $K$ yields $M$, $M$ must also be unique. ∎

LEMMA 4.3 *If* $X, Y \in \mathbf{Z}$, $X^\lambda \equiv Y^\lambda \pmod N$, *and* $\left[\frac{X}{\pi\psi}\right] \neq \left[\frac{Y}{\pi\psi}\right]$, *then* $\gcd(X - r^i Y, N) = p$ *for some* $i \in \{0, \ldots, \lambda - 1\}$.

*Proof.* We have $X^\lambda - Y^\lambda \equiv (X - Y)(X - rY)\cdots(X - r^{\lambda-1}Y) \equiv 0 \pmod N$. Assume that $X - r^i Y \equiv 0 \pmod N$ for some $i \in \{0, \ldots, \lambda - 1\}$. Then $\left[\frac{X}{\pi\psi}\right] = \left[\frac{r}{\pi\psi}\right]^i \left[\frac{Y}{\pi\psi}\right] = \left[\frac{Y}{\pi\psi}\right]$ which contradicts our assumption. So there must be $i \in \{0, \ldots, \lambda - 1\}$ such that $X - r^i Y \equiv 0 \pmod p$ and $X - r^i Y \not\equiv 0 \pmod q$. But then $\gcd(X - r^i Y, N) = p$. ∎

THEOREM 4.4 *If A is an algorithm which, given any key K and cipher* $\{C, m, n\}$ *will find the corresponding plaintext M, then the following algorithm will factor N:*

1. *Find* $Y \in \mathbf{Z}$ *such that* $0 < Y < N$ *and* $\left[\frac{Y}{\pi\psi}\right] \neq 1$ *(note that S is a possible choice for Y).*
2. *Put* $C \equiv Y^\lambda \pmod N$, $0 < C < N$, *and select any* $m, n \in \{0, \ldots, \lambda - 1\}$.
3. *Use A to decrypt* $\{C, m, n\}$ *under K, obtaining M.*
4. *Put* $M_0 \equiv MS^m$, $X \equiv M_0^e \pmod N$.
5. *For* $0 \leq i \leq \lambda - 1$, *compute* $\gcd(X - r^i Y, N)$ *until a nontrivial factor is found.*

*Proof.* $M$ in step 2 is unique by Lemma 4.2. Since $1 = \left[\frac{X}{\pi\psi}\right] \neq \left[\frac{Y}{\pi\psi}\right]$ and $X^\lambda \equiv C \equiv Y^\lambda \pmod N$, by Lemma 4.3 we must have $\gcd(X - r^i Y, N) = p$ for some $i$. ∎

It should be noted that revealing $r$ does not seem to compromise the security of the system. By Lemma 4.3, we could factor $N$ if we found a $\lambda$-th root of unity $X \pmod N$ such that $\left[\frac{X}{\pi\psi}\right] \neq 1$. But this corresponds to the case $C = 1$ in Theorem 4.4, so, unless the number 1 represents a special case, the problem of finding $X$ is equivalent in difficulty to factoring $N$.

It is clear that this algorithm can be used to mount a chosen ciphertext attack if an attacker (who generates $Y$) is able to convince his opponent to decrypt the triple $\{C, m, n\}$ and is somehow able to obtain the corresponding plaintext $M$ and hence $X$.

If $A$ is such that it can only decrypt a fraction $\frac{1}{k}$ of all messages, then we expect to be able to find $M$ and proceed as above after $k$ trials at a value of $Y$.

## 5. Algorithms

For the implementation of our scheme, we need efficient methods to find $r$, $\pi$, and $\psi$ from $p$ and $q$ as well as an algorithm which does not require factoring for evaluating residue symbols.

We let the time complexity of an algorithm refer to the number of arithmetic integer operations (addition, subtraction, multiplication, division with remainder, and comparison of two rational integers) it performs; we do not consider the computation time each such operation requires. The space complexity of an algorithm is the number of bits in the binary representation of its largest input. All inputs are rational integers; integers $\alpha = a_1\zeta + \cdots + a_{\lambda-1}\zeta^{\lambda-1} \in \mathbf{R}$ are represented by their coordinate vectors $(a_1, \ldots, a_{\lambda-1})$.

In order to find a primitive $\lambda$-th root $r(\mathrm{mod}\, N)$ such that $\gcd(r-1, N) = 1$, and $\left[\frac{r}{\pi\psi}\right] = 1$, we need to find non-residues $v(\mathrm{mod}\, p)$ and $w(\mathrm{mod}\, q)$, i.e. $v^{\frac{p-1}{\lambda}} \not\equiv 1(\mathrm{mod}\, p)$ and $w^{\frac{q-1}{\lambda}} \not\equiv 1(\mathrm{mod}\, q)$. Then $\left[\frac{v}{\pi}\right] = \zeta^i, \left[\frac{w}{\psi}\right] = \zeta^j$ for some $i, j \in \{1, \ldots, \lambda - 1\}$. Let $k \in Z$ be such that $\frac{p-1}{\lambda}ik + \frac{q-1}{\lambda}j \equiv 0(\mathrm{mod}\, \lambda)$ and $1 \leq k \leq \lambda - 1$. Define $a \equiv v^{\frac{p-1}{\lambda}k}(\mathrm{mod}\, p), b \equiv w^{\frac{q-1}{\lambda}}(\mathrm{mod}\, q)$. Then $a \equiv \left[\frac{v}{\pi}\right]^k \equiv \zeta^{ik} \not\equiv 1(\mathrm{mod}\, \pi)$, since $i, k \not\equiv 0(\mathrm{mod}\, \lambda)$, so $a \not\equiv 1(\mathrm{mod}\, p), b \not\equiv 1(\mathrm{mod}\, q)$, and $a^\lambda \equiv 1(\mathrm{mod}\, p), b^\lambda \equiv 1(\mathrm{mod}\, q)$. Use the Chinese Remainder Theorem to compute $r$ such that $r \equiv a(\mathrm{mod}\, p)$ and $r \equiv b(\mathrm{mod}\, q)$. Then $r \not\equiv 1(\mathrm{mod}\, p)$ and $r \not\equiv 1(\mathrm{mod}\, q)$, so $\gcd(r-1, N) = 1$. Furthermore $r^\lambda \equiv 1(\mathrm{mod}\, p), r^\lambda \equiv 1(\mathrm{mod}\, q)$, so $r^\lambda \equiv 1(\mathrm{mod}\, N)$. Finally,

$$\left[\frac{r}{\pi\psi}\right] = \left[\frac{a}{\pi}\right]\left[\frac{b}{\psi}\right] = \left[\frac{v}{\pi}\right]^{\frac{p-1}{\lambda}k}\left[\frac{w}{\psi}\right]^{\frac{q-1}{\lambda}} = \zeta^{\frac{p-1}{\lambda}ki + \frac{q-1}{\lambda}j} = 1.$$

By a theorem of Bach [1], the least positive $\lambda$-th nonresidue $v(\mathrm{mod}\, p)$ satisfies $v < 2(\log p)^2$, assuming the truth of the Extended Riemann Hypothesis (ERH), thus, according to this we can find a value of $v$ after at most $O((\log p)^2)$ steps, although we expect to find one much faster by trial as the probability of a successful guess is $\frac{(p-1)(\lambda-1)}{\lambda}$. Since calculating $a$ from $v$ requires $O(\log p)$ arithmetic operations on inputs of at most $O(\log p)$ bits of storage, computing $r$ requires $O((\log N)^3)$ arithmetic operations at the very worst (assuming ERH) and $O(\log N)$ operations in practice, as well as space $O(\log N)$.

A method for finding $\pi$ such that $N(\pi) = p$ is given in Buchmann & Williams [3] and Buchmann & Williams [4]. The algorithm is based on the reduction theory for ideals in $\mathbf{R}$. It is easy to show that $\pi$ is a generator of the principal ideal $\mathbf{p}$ whose $\mathbf{Z}$-basis is $p, \zeta - r, (\zeta - r)^2, \ldots, (\zeta - r)^{\lambda-2}$. To find $\pi$, we first precompute generators for all reduced (principal) ideals in the UFD $\mathbf{R}$, using the technique of [2]. Then the reduction method of [3] and [4] is applied to the ideal $\mathbf{p}$ to find a reduced ideal $\mathbf{a}$ and an integer $\beta$ such that $\mathbf{p} = \beta\mathbf{a}$. Finally, the list of generators is searched for a generator $\alpha$ of $\mathbf{a}$, and we set $\pi = \beta\alpha$. For fixed $\lambda$, this algorithm can be shown to require a total of $O(l + \log p)$ arithmetic operations and $O(l + \log p)$ bits of storage, where $l$ is the number of reduced ideals in $\mathbf{R}$. Computations show that $l = 1$ for $\lambda \leq 7$ (see [3], [4]).

There is an alternative way to compute $\pi$ if $\mathbf{F}$ is Euclidean. In general, an algebraic number field $\mathbf{F}$ (or its ring of integers $\mathbf{R}$) is said to be *Euclidean* for the norm if for every $a, b \in \mathbf{R}, b \neq 0$, there exist $q, r \in \mathbf{R}$ such that $a = qb + r$ and $|N(r)| < |N(b)|$, or equivalently, for every $x \in \mathbf{F}$ there exists $y \in \mathbf{R}$ such that $|N(x - y)| < 1$. The process of finding $q$ and $r$ is called *Euclidean division*. If $\mathbf{F}$ is Euclidean and we define for any $a, b \in \mathbf{R}$ the *greatest common divisor* $d \in \mathbf{R}$ of $a$ and $b$ to be a divisor of both $a$ and $b$ in $\mathbf{R}$ such that each divisor $d'$ of both $a$ and $b$ is also a divisor of $d$ in $\mathbf{R}$, then $d$ is unique up

to multiplication by a unit and can be found using the *Euclidean Algorithm*

$$\begin{aligned} a &= q_0 b + r_1, & |N(r_1)| &< |N(b)|, \\ b &= q_1 r_1 + r_2, & |N(r_2)| &< |N(r_1)|, \\ r_1 &= q_1 r_2 + r_3, & |N(r_3)| &< |N(r_2)| \\ &\vdots \end{aligned}$$

until $r_{n-1} = q_n r_n + r_{n+1}$ such that $N(r_{n+1}) = 0$, i.e. $r_{n+1} = 0$. Then $r_n = \gcd(a, b)$ and $n = O(\log \max\{N(a), N(b)\})$. It can be shown that $\pi = \gcd(p, \zeta - r)$, and since $N(\zeta - r) < \lambda p^{\lambda-1}$, this method requires $O(\lambda \log p)$ Euclidean division steps.

An efficient algorithm for computing the residue symbol for $\lambda$ is crucial for our scheme. The techniques used will be analogous to those for evaluating the Jacobi symbol in $\mathbf{Z}$ without factoring the "denominator" by making use of Kummer's law of reciprocity plus complementaries as well as Euclidean division.

If $\mathbf{F}$ is a cyclotomic field of degree $\lambda - 1$ over $Q$, then Lenstra [8] proved that $\mathbf{F}$ is Euclidean for $\lambda \leq 11$. McKenzie [11] showed the same for $\lambda = 13$; his results may be extendable to the cases $\lambda = 17$ and 19, but the technique requires an extensive search and is thus not suitable as a practical Euclidean division method. It is known that $\mathbf{F}$ is not Euclidean (in fact, $\mathbf{R}$ is not even a UFD) for $\lambda \geq 23$.

Assume now that $\lambda$ is an odd prime $\leq 11$. Recall that $\omega = 1 - \zeta$. A number $\alpha \in \mathbf{R}$ is defined to be *primary* (Kummer [5], p. 350, Smith [13], p. 118) if

i) $\alpha \not\equiv 0 (\mathrm{mod}\, \omega)$

ii) $\alpha \equiv B (\mathrm{mod}\, \omega^2)$

iii) $\alpha\bar{\alpha} \equiv B^2 (\mathrm{mod}\, \lambda)$

for some $B \in \mathbf{Z}$, where all congruences are taken in $\mathbf{R}$. If $\lambda = 2$, then $\alpha$ is said to be primary if $\alpha \equiv 1 (\mathrm{mod}\, 4)$. It can be shown that $B \equiv -\mathrm{Tr}(\alpha) (\mathrm{mod}\, \lambda)$. Conditions i) and ii) are equivalent, respectively, to $\mathrm{Tr}(\alpha) \not\equiv 0 (\mathrm{mod}\, \lambda)$ and $\mathrm{Tr}\left(\frac{d\alpha}{d\zeta}\right) \equiv 0 (\mathrm{mod}\, \lambda)$, where $\frac{d\alpha}{d\zeta}$ is the derivative of $\alpha$ as a function of $\zeta$.

If $\alpha, \beta \in \mathbf{R}$ are primary, then so is $\alpha\beta$, and every $\alpha \in \mathbf{R}$ such that $\mathrm{Tr}(\alpha) \not\equiv 0 (\mathrm{mod}\, \lambda)$ has a primary associate. In fact, condition ii) can always be achieved by multiplying $\alpha$ by a suitable power of $\zeta$; this has no bearing on conditions i) and iii). Furthermore, any two primary associates only differ by a factor of a $\lambda$-th power. Since 1 is primary, it follows that every primary unit is a $\lambda$-th power and thus has residue symbol 1.

Let $0 \neq \alpha \in \mathbf{R}$. We can write $\alpha = \varepsilon \omega^k \gamma$ where $k \geq 0$, $\varepsilon$ is a unit, and $\gamma$ is primary. Then for any $\beta \in \mathbf{R}$ relatively prime to $\alpha$ and primary, we have $\left[\frac{\alpha}{\beta}\right] = \left[\frac{\varepsilon}{\beta}\right]\left[\frac{\omega}{\beta}\right]^k \left[\frac{\gamma}{\beta}\right]$. Kummer's *Law of Reciprocity* ([5], pp. 345ff.; [13], pp. 120f.) states that $\left[\frac{\gamma}{\beta}\right] = \left[\frac{\beta}{\gamma}\right]$ for $\beta, \gamma \in \mathbf{R}$ primary and relatively prime. The values of $\left[\frac{\varepsilon}{\beta}\right]$ for units $\varepsilon$ and $\left[\frac{\omega}{\beta}\right]$ are given by the *complementaries* ([5], pp. 485ff.; [13], pp. 121ff.). To evaluate $\left[\frac{\alpha}{\beta}\right]$ for $\alpha, \beta \in \mathbf{R}$

relatively prime, we first obtain a primary associate $\beta'$ of $\beta$, then use Euclidean division to find $q, r \in \mathbf{R}$ such that $\alpha = q\beta' + r$ and $N(r) < N(\beta')$. Write $r = \varepsilon\omega^k\gamma$ where $k \geq 0$, $\varepsilon$ is a unit and $\gamma$ is primary. Using the law of reciprocity and the complementaries $\left[\frac{\varepsilon}{\beta'}\right] = \zeta^i, \left[\frac{\omega}{\beta'}\right] = \zeta^j, 0 \leq i, j \leq \lambda - 1$, we obtain $\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\beta'}\right] = \left[\frac{r}{\beta'}\right] = \zeta^{i+kj}\left[\frac{\beta'}{\gamma}\right]$, and we can repeat this process with $\left[\frac{\beta'}{\gamma}\right]$, until we obtain $N(\gamma) = 1$, at which point $\gamma$ is a primary unit, so $\left[\frac{\gamma}{\beta'}\right] = 1$.

Suppose we have $N(\gamma) = 1$ after $l$ iterations. If each individual step can be performed in constant time and $\omega$ divides $r$ $k_i$ times in iteration $i$, then the total number of operations required is $O(l + k_1 + \cdots + k_l)$. Let $B(\lambda) < 1$ be a bound on $N(r)/N(\beta')$ given by the Euclidean division algorithm. Then $N(\beta')$ is reduced by a factor of $\frac{B(\lambda)}{\lambda^{k_i}}$ in each iteration, so $l$ iterations reduce $N(\beta')$ by a factor of at least $\frac{\lambda^{k_1+\cdots+k_l}}{B(\lambda)^l}$. It follows that the overall complexity of the algorithm is $O\left(\frac{\log N(\beta)}{\log \min\{\lambda, B(\lambda)^{-1}\}}\right)$. Furthermore, the norms of all inputs are bounded by $\max \log\{N(\alpha), N(\beta)\}$.

Our Euclidean division algorithm is based on ideas of Lenstra [7] and is outlined as follows. Define the bilinear form $\mu$ on $\mathbf{F}$ by $\mu(x) = \mathrm{Tr}(x\bar{x}) = \sum_{i=1}^{\lambda-1} |\sigma_i(x)|^2$ for $x \in \mathbf{F}$. The *fundamental domain* $\mathbf{D}$ with respect to $\mathbf{R}$ is $\mathbf{D} = \{z \in \mathbf{F} \mid \mu(z) \leq \mu(z - u)$ for all $u \in \mathbf{R}\}$. Then it can be shown that $\mathbf{F} = \mathbf{D} + \mathbf{R}$. Lenstra proves in [7] that $\mu(z) \leq \frac{\lambda^2-1}{12}$ for all $z \in \mathbf{D}$. The arithmetic-geometric mean inequality implies $N(x)^2 \leq \left(\frac{\mu(x)}{\lambda-1}\right)^{\lambda-1}$ for $x \in \mathbf{F}$. Hence if for any $x \in \mathbf{F}$ we can find a representation $x = z + y$ where $z \in \mathbf{D}$ and $y \in \mathbf{R}$, then $N(x - y) \leq B(\lambda)$, where $B(\lambda) = \left(\frac{\lambda+1}{12}\right)^{\frac{\lambda-1}{2}}$. This gives the following bounds $B(\lambda)$ on $N(x - y)$:

| $\lambda$ | 2 | 3 | 5 | 7 | 11 |
|---|---|---|---|---|---|
| $B(\lambda)$ | $\frac{1}{2}$ | $\frac{1}{3}$ | $\frac{1}{4}$ | $\frac{8}{27}$ | 1 |

For comparison, a Euclidean division method due to Uspensky ([14], see also Landau [6], pp. 228–231) for $\lambda = 5$ gives a bound of $\left(\frac{79}{80}\right)^2$ on $N(x - y)$. Kummer's bound ([5], pp. 87–91, for details see Lenstra [8]) of $\left(\frac{77}{80}\right)^2$ is slightly better. Williams [16] gives a bound of $\frac{3}{4}$ for $\lambda = 3$, which can be improved to $\frac{19}{36}$ and $\frac{11}{24}$, using Uspensky's and Kummer's techniques, respectively. Moreover, none of the classical methods provide bounds for the cases $\lambda = 7$ and 11.

Unfortunately, this technique does not yield a tight bound ($B(\lambda) < 1$) for the case $\lambda = 11$. Note that $B(\lambda)^{-1} < \lambda$ for all $\lambda$, so this bound yields a running time proportional to $(\log N(\beta))\left(\frac{\lambda-1}{2}\log\frac{12}{\lambda+1}\right)^{-1}$ for the residue symbol algorithm, where the proportionality factor does not depend on $\lambda$.

Now let $x \in \mathbf{F}$. The above observations show that computing $y \in \mathbf{R}$ such that $x - y \in \mathbf{D}$ is sufficient for Euclidean division, since $N(x - y) \leq \left(\frac{\lambda+1}{12}\right)^{\frac{\lambda-1}{2}} < 1$ for $\lambda \leq 7$ (and $= 1$ for $\lambda = 11$). The following Lemma shows that in order to achieve $x - y \in \mathbf{D}$, it suffices to minimize $\mu(x - y)$.

LEMMA 5.1 *Let $x \in \mathbf{F}$ and let $y \in \mathbf{R}$ such that $\mu(x-y)$ is minimal. Then $x - y \in \mathbf{D}$.*

*Proof.* We need to show that $\mu(x-y) \le \mu(x-y-u)$ for all $u \in \mathbf{R}$. Let $u \in \mathbf{R}$ and let $v = y+u \in \mathbf{R}$. Since $\mu(x-y)$ is minimal, we have $\mu(x-y) \le \mu(x-v) = \mu(x-y-u)$. ∎

For reasons of symmetry, we will represent field elements as linear combinations of all $\lambda$ roots of unity $1, \zeta, \ldots, \zeta^{\lambda-1}$ (note that this representation is not unique since $\sum_{i=0}^{\lambda-1} \zeta^i = 0$). Let $x \in \mathbf{F}$ and let $y \in \mathbf{R}$ be such that $\mu(x-y)$ is minimal. Let $z = x - y = \sum_{i=0}^{\lambda-1} z_i \zeta^{\mu i}$ where $z_0 \le \cdots \le z_{\lambda-1}$. Then it is easy to show that $z_{\lambda-1} - z_0 \le 1$. For if we assume that $z_{\lambda-1} - z_0 > 1$ and set $y' = y - \zeta^{\mu_0} + \zeta^{\mu_n} \in \mathbf{R}$, $z' = z + \zeta^{\mu_0} - \zeta^{\mu_n} = x - y'$ (i.e. we add 1 to the smallest coefficient and subtract 1 from the largest coefficient of $z$), then a short calculation shows $\mu(z) > \mu(z')$, contradicting the minimality of $\mu(z)$. Now we will show that there are only $\lambda$ possible candidates for $y$, all of which can be easily computed from $x$.

THEOREM 5.2 *Let $x = \sum_{i=0}^{\lambda-1} x_i \zeta^i \in \mathbf{F}$, $z_i' = x_i - \lfloor x_i \rfloor$ for $0 \le i \le \lambda - 1$.*[2] *Let $z_i = z'_{\mu_i}$ where $0 \le z_0 \le \cdots \le z_{\lambda-1} < 1$. Set $z^{(0)} = \sum_{i=0}^{\lambda-1} z_i' \zeta^i = \sum_{i=0}^{\lambda-1} z_i \zeta^{\mu_i}$, $z^{(j)} = z^{(j-1)} + \zeta^{\mu_j}$ for $1 \le j \le \lambda - 1$. If $y \in \mathbf{R}$ is such that $\mu(x-y)$ is minimal, then $x - y = z^{(k)}$ for some $k \in \{0, \ldots, \lambda - 1\}$.*

*Proof.* Let $y \in \mathbf{R}$ be such that $\mu(w)$ is minimal where $w = x - y$. Set $u = \sum_{i=0}^{\lambda-1} \lfloor x_i \rfloor \zeta^i \in \mathbf{R}$, then $x = u + z^{(0)} = y + w$, so $w - z^{(0)} \in \mathbf{R}$. Hence if $w = \sum_{i=0}^{\lambda-1} w_i \zeta^{\mu_i}$, then $w_i - z_i = n_i \in \mathbf{Z}$ for all $i \in \{0, \ldots, \lambda - 1\}$. If $z_i = z_j$ and $n_i < n_j$ for some $i < j$, then swap $i$ and $j$ to obtain $n_i \ge n_j$. This does not violate the order of the $z_\nu$ $(0 \le \nu \le \lambda - 1)$.

Let $0 \le i < j \le \lambda - 1$. Then $0 \le z_j - z_i < 1$, hence $w_i - w_j \le n_j - n_i < 1 + w_i - w_j$. Now since $\mu(w)$ is minimal, we must have $|w_i - w_j| \le 1$, so $-1 \le n_j - n_i < 2$ or $n_j - n_i \in \{-1, 0, 1\}$. Suppose $n_j > n_i$, then $n_j - n_i = 1$ and $z_i < z_j$ by our renumbering of the $z_\nu$, hence $w_j = n_j + z_j > n_i + 1 + z_i = w_i + 1$ in contradiction to $|w_i - w_j| \le 1$. Therefore $n_j \le n_i$. It follows that $n_j - n_i \in \{0, -1\}$ and $0 \ge n_1 - n_0 \ge \cdots \ge n_{\lambda-1} - n_0 \ge -1$. Define $k$ such that $n_i - n_0 = 0$ for $i < k$ and $n_i - n_0 = -1$ for $i \ge k$. Then $w_i = z_i + n_0$ for $i < k$ and $w_i = z_i + n_0 - 1$ for $i \ge k$. Hence

$$\begin{aligned} w &= \sum_{i=0}^{k-1} (z_i + n_0)\zeta^{\mu_i} + \sum_{i=k}^{\lambda-1} (z_i + n_0 - 1)\zeta^{\mu_i} = \sum_{i=0}^{k-1} (z_i + 1)\zeta^{\mu_i} + \sum_{i=k}^{\lambda-1} z_i \zeta^{\mu_i} \\ &\quad + (n_0 - 1) \sum_{i=0}^{\lambda-1} \zeta^{\mu_i} \\ &= z^{(0)} + \sum_{i=0}^{k-1} \zeta^{\mu_i} = z^{(k)}. \end{aligned}$$

COROLLARY $z^{(k)} \in \mathbf{D}$ *for some* $k$, $0 \le k \le \lambda - 1$. ∎

The previous theorem and its corollary give rise to the following Euclidean division algorithm.

*Algorithm 5.1.* Given $x = \sum_{i=0}^{\lambda-1} x_i \zeta^i \in \mathbf{F}$, find $y \in \mathbf{R}$ such that $x - y \in \mathbf{D}$.

1. For $0 \le i \le \lambda - 1$ set $y_i = \lfloor x_i \rfloor$ and $z_i' = x_i - y_i$. Set $z = \sum_{i=0}^{\lambda-1} z_i' \zeta^i$, $y = \sum_{i=0}^{\lambda-1} y_i \zeta^i$.
2. Sort the $z_i'$ in non-descending order, i.e. let $z_i = z'_{\mu_i}$ and $0 \le z_0 \le z_1 \le \cdots \le z_{\lambda-1}$.
3. *While* $\mu(z) > \frac{\lambda^2-1}{12}$ *do*

   Set $y \leftarrow y - \zeta^{\mu 0}$, $z \leftarrow z + \zeta^{\mu 0}$.

   Sort the $z_i$ in non-descending order, i.e. set

$$t = z_0, z_0 = z_1, \ldots, z_{\lambda-2} = z_{\lambda-1}, z_{\lambda-1} = t + 1.$$

Clearly $y \in \mathbf{R}$ in each step. By Theorem 5.2, the algorithm terminates after at most $\lambda$ iterations of step 3, after which we will have added $\sum_{i=0}^{\lambda-1} \zeta^i = 0$ to the value of $z$ in step 1. Hence this algorithm produces $y \in \mathbf{R}$ such that $N(x - y) < 1$ using $O(\lambda)$ arithmetic operations.

Now let $\alpha, \beta \in \mathbf{R}, \beta \neq 0$. Then we apply Algorithm 5.1 to $x = \frac{\alpha}{\beta} = \frac{\gamma}{N(\beta)}$, where $\gamma = \alpha\sigma_2(\beta)\cdots\sigma_{\lambda-1}(\beta) \in \mathbf{R}$. If $\gamma = \sum_{i=1}^{\lambda-1} c_i \zeta^i$, then the values $y_i$ and $z_i$ in Algorithm 5.1 are given by $c_i = y_i N(\beta) + r_i$, $0 \le y_i < N(\beta)$, and $z_i = \frac{r_i}{N(\beta)}$ $(1 \le i \le \lambda - 1)$. In each iteration, we subtract 1 from the coefficient $y_{\mu_0}$ of $\zeta^{\mu_0}$ in $y$ and add $N(\beta)$ to the coefficient $r_{\mu_0}$ of $\zeta^{\mu_0}$ in $\sum_{i=1}^{\lambda-1} r_i \zeta^i$ (initially, $y_0 = r_0 = 0$). Hence $0 \le r_i < 2N(\beta)$ $(1 \le i \le \lambda - 1)$ throughout the algorithm. The largest input is either bounded by $2N(\beta)$ or it is the largest coefficient in absolute value of $\gamma$.

For computing the residue symbol $\left[\frac{\alpha}{\beta}\right]$, recall that Euclidean division was used in each iteration to compute $q, r \in \mathbf{R}$ such that $\alpha = r\beta + r$, $N(r) < N(b)$. Then we wrote $r = \varepsilon\omega^k\gamma$, where $\varepsilon$ is a unit and $\gamma$ is primary. If the coefficients of $\varepsilon^{-1}$ and $\omega^{-k}$ are small (this is the case for $\lambda \le 5$), then our previous analysis shows that the space required in each iteration (except the very first one) of the residue symbol algorithm is no larger than $O(\lambda \log N(\beta))$.

For the cryptosystem, the overall time and space complexity is $O(\log N)$ for the modular exponentiation plus the complexity of computing $\left[\frac{M}{\pi\psi}\right]$.

Since the set of all $T \in \mathbf{Z}$ such that $0 < T < N$, $\gcd(T, N) = 1$, and $\left[\frac{T}{\pi\psi}\right] = 1$ is a multiplicative subgroup of $(\mathbf{Z}/N\mathbf{Z})^*$, Bach's Theorem [1] implies that we can find a value of $S$ in the public key such that $0 < S < (2(\log N)^2)^{\lambda-1}$. Hence the number of bits in the public key is bounded by $(\lambda-1)\log C + 2\log N + (\lambda-1)O(\log\log N)$, where $C$ is an upper bound on the absolute value of the largest coefficient of $\pi\psi$. Alternatively, the key could be given as $\{r, S, N, e\}$, requiring space $3\log N + (\lambda - 1)O(\log\log N)$. In this case, the encrypter needs to precompute $\pi\psi$. This can be achieved by employing techniques similar to those used for generating $\pi$ and $\psi$, i.e. by either computing $\gcd(N, \zeta - r)$ or by finding a generator of the principal ideal given by the $\mathbf{Z}$-basis $N, \zeta - r, (\zeta - r)^2, \ldots, (\zeta - r)^{\lambda-2}$.

It should be noted here that it is not known whether there exists an efficient method for computing residue symbols without using Euclidean division, nor is it known whether we can evaluate residue symbols for ideal denominators.

## 6. The Cases $\lambda = 2, 3, 5$

In the case where $\lambda = 2$, we have $p \equiv q \equiv 3 (\mathrm{mod}\, 4)$, $\pi = p$, $\psi = q$, $r = N - 1$, and the public key is $K = \{S, N, e\}$. The residue symbol is the Legendre/Jacobi symbol and Euclidean division reduces to the well-known division with remainder in $\mathbf{Z}$.

As mentioned before, a slightly modified version of the case $\lambda = 3$ was discussed by Williams in [16]. Here $p, q \equiv 4, 7 (\mathrm{mod}\, 9)$, and if $\pi\psi = c_1\zeta + c_2\zeta^2$, then we can set $r \equiv -c_1c_2 (\mathrm{mod}\, N)$, as this implies $r \equiv \zeta (\mathrm{mod}\, \pi\psi)$. In this case, we can set the key to be $K = \{S, c_1, c_2, e\}$.

The case $\lambda = 5$ is the first case in which we have units other than the powers of $\zeta$, so we will illustrate the technique of evaluating residue symbols in more detail. Here $\mathbf{F}$ is a quartic field over $\mathbf{Q}$. If $\alpha = \sum_{i=1}^{4} a_i\zeta^i \in \mathbf{R}$ and we define

$$a = a(\alpha) = a_1 - a_2 - a_3 + a_4,$$

$$b = b(\alpha) = a_1 + a_2 + a_3 + a_4 = -\mathrm{Tr}(\alpha),$$

$$c = c(\alpha) = a_1 + 2a_2 + 3a_3 + 4a_4 = \mathrm{Tr}\left(\frac{d\alpha}{d\zeta}\right) + 5a_1,$$

$$d = d(\alpha) = a_1 - 2a_2 + 2a_3 - a_4,$$

then $a, b, c, d \in \mathbf{Z}$ and $\alpha$ is primary if and only if $b \not\equiv 0 (\mathrm{mod}\, 5)$ and $a \equiv c \equiv 0 (\mathrm{mod}\, 5)$, so this yields a practical test for a number to be primary.

The *fundamental unit* in $\mathbf{F}$ is $\eta = -(\zeta^2 + \zeta^3)$, i.e. every unit $\varepsilon \in \mathbf{F}$ can be written as $\pm\zeta^j\eta^k$ where $0 \le j \le 4$ and $k \in \mathbf{Z}$. If we choose $\zeta = \exp\left(\frac{2\pi i}{5}\right)$, then $\eta = \frac{1+\sqrt{5}}{2}$. In the quintic case, Kummer's law of reciprocity and complementaries (explicitly stated by Williams [17]) are as follows.

LEMMA 6.1 *Let $\pi, \psi$ be primary primes. Then*

$$\text{a)}\left[\frac{\pi}{\psi}\right] = \left[\frac{\psi}{\pi}\right], \quad \text{b)}\left[\frac{\pm 1}{\pi}\right] = 1, \quad \text{c)}\left[\frac{\zeta}{\pi}\right] = \zeta^{\frac{N(\pi)-1}{5}},$$

*Furthermore, if $\pi = \sum_{i=1}^{4} a_i\zeta^i$, $b = \sum_{i=1}^{4} a_i$, and $b^* \in \mathbf{Z}$ is such that $bb^* \equiv 1 (\mathrm{mod}\, 5)$, then*

$$\text{d)}\left[\frac{\eta}{\pi}\right] = \zeta^{4db^*}, \quad \text{e)}\left[\frac{\omega}{\pi}\right] = \zeta^{4b^*\frac{c}{5} + 3\frac{N(\pi)+4}{5}}.$$

All properties of this lemma can be shown to hold for composite primary denominators as well. It is easy to find primary associates as follows.

LEMMA 6.2 *Let $\alpha \in \mathbf{R}$ be such that $\mathrm{Tr}(\alpha) \not\equiv 0 (\mathrm{mod}\, 5)$. Then $\alpha$ has a primary associate of the form $\alpha' = \zeta^j\eta^k\alpha$ where $0 \le j, k \le 4$.*

*Proof.* Let $\alpha = \sum_{i=1}^{4} a_i\zeta^i$ and let $b = b(\alpha), c = c(\alpha)$. Then $b \not\equiv 0 (\mathrm{mod}\, 5)$. Now $\alpha = \sum_{i=1}^{4} a_i(1-\omega)^i \equiv \sum_{i=1}^{4} a_i(1 - i\omega) \equiv b - c\omega (\mathrm{mod}\, \omega^2)$, so $\alpha\zeta^j \equiv \alpha(1-\omega)^j \equiv \alpha(1 - j\omega) \equiv b - (c + jb)\omega (\mathrm{mod}\, \omega^2)$, hence $b(\alpha\zeta^j) \equiv b \not\equiv 0 (\mathrm{mod}\, 5)$ and $c(\alpha\zeta^j) \equiv$

$c + jb \pmod 5$ for $0 \leq j \leq 4$. Since one of $c + jb$ $(0 \leq j \leq 4)$ must be divisible by 5, we have found an associate $\alpha'$ of $\alpha$ such that $b(\alpha') \not\equiv 0 \pmod 5$ and $c(\alpha') \equiv 0 \pmod 5$.

Assume now $b \not\equiv 0 \pmod 5$ and $c \equiv 0 \pmod 5$. Let $\alpha_j = \alpha\eta^j (0 \leq j \leq 4)$. A straightforward calculation yields $\eta^2 = \eta + 1, \eta^3 = 2\eta + 1, \eta^4 = 3\eta + 2$, hence if we let $n = \frac{a-b}{2} = -(a_2 + a_3)$, we have $a(\alpha_0) = a, a(\alpha_1) = n, a(\alpha_2) = n + a, a(\alpha_3) = 2n + a, a(\alpha_4) = 3n + 2a$. Furthermore, since $\eta \equiv -2 \pmod{\omega^2}$, it follows that $b(\alpha_j) \equiv (-2)^j b \not\equiv 0 \pmod 5$, $c(\alpha_j) \equiv (-2)^j c \equiv 0 \pmod 5$.

We need to prove that one of the $\alpha_j$ is primary, i.e. that $a(\alpha_j) \equiv 0 \pmod 5$ for some $j, 0 \leq j \leq 4$. If $a \equiv 0 \pmod 5$, then $\alpha_0$ is primary and if $n \equiv 0 \pmod 5$, then $\alpha_1$ is primary. So suppose now that $an \not\equiv 0 \pmod 5$. Then if $a \equiv -n \pmod 5$, then $\alpha_2$ is primary, if $a \equiv -2n \pmod 5$, then $\alpha_3$ is primary, and if $a \equiv n \pmod 5$, then $\alpha_4$ is primary. The only remaining case is $a \equiv 2n \pmod 5$, in which case $0 \equiv a - 2n \equiv b \pmod 5$, a contradiction. Hence we have found the required primary associate of $\alpha$. ∎

We are now ready to present the full algorithm for computing quintic residue symbols.

*Algorithm 6.2.* For $\alpha, \beta \in \mathbf{R}$ primary, $\gcd(\alpha, \beta) = 1$, evaluate $\left[\frac{\alpha}{\beta}\right] = \zeta^s, 0 \leq s \leq 4$.

1. Set $s = 0$ and compute $N(\beta)$.

   {Compute $\gamma \equiv \alpha \pmod \beta$, $0 < N(\gamma) < N(\beta)$}

2. Compute $x = \frac{\alpha}{\beta} = \frac{\alpha\sigma_2(\beta)\sigma_3(\beta)\sigma_4(\beta)}{N(\beta)} \in \mathbf{F}$.

3. Use Algorithm 5.1 to find $y \in \mathbf{R}$ such that $N(x - y) < 1/4$.

4. Set $\gamma = \beta(x - y)$, then $\alpha = \beta y + \gamma$ and $0 < N(\gamma) < (1/4)N(\beta)$.

   {Make $\gamma$ primary}

5. Compute $b \equiv b(\beta) \pmod 5$, $b^* \equiv b^{-1} \pmod 5$, $c \equiv c(\beta) \pmod{25}$, $d \equiv d(\beta) \pmod 5$.

6. {Factor out $\omega$} Set $i = 0$.

   *While* $b(\gamma) \equiv 0 \pmod 5$ *do*

   $$\text{Set } \gamma \leftarrow \frac{\gamma}{\omega}, \quad i \leftarrow i + 1.$$

7. {Factor out $\zeta$} Set $j \equiv -c(\gamma)b^*(\gamma) \pmod 5$, $0 \leq j \leq 4$. Set $\gamma \leftarrow \gamma\zeta^j$.

8. {Factor out $\eta$} Compute $a(\gamma) \pmod 5$. Set $k = 0$.

   *If* $a(\gamma) \not\equiv 0 \pmod 5$, *then*

   $$\text{compute } n(\gamma) \equiv \frac{a(\gamma) - b(\gamma)}{2} \equiv -a_2(\gamma) - a_3(\gamma) \pmod 5.$$

*If* $0 \equiv n(\gamma) (\mathrm{mod}\, 5)$, *then* set $k = 1$.

*If* $a(\gamma) \equiv -n(\gamma) (\mathrm{mod}\, 5)$, *then* set $k = 2$.

*If* $a(\gamma) \equiv -2n(\gamma) (\mathrm{mod}\, 5)$, *then* set $k = 3$.

*If* $a(\gamma) \equiv n(\gamma) (\mathrm{mod}\, 5)$, *then* set $k = 4$.

Set $\gamma \leftarrow \gamma \eta^k$.

9. Set $s \leftarrow s + i\left(4b^* \frac{c}{5} + 3\frac{N(\beta)+4}{5}\right) - j\frac{N(\beta)-1}{5} - 4kdb^* (\mathrm{mod}\, 5),\ 0 \le s \le 4.$

10. Compute $N(\gamma)$.

*If* $N(\gamma) > 1$, *then*

Set $\alpha \leftarrow \beta, \beta \leftarrow \gamma$. *Goto* step 2.

Recall that once we have $N(\gamma) = 1$, then $\left[\frac{\gamma}{\beta}\right] = 1$ as $\gamma$ is primary. For the computation of $s$ in step 9, note that $i$ is the power of $\omega$ contained in $\gamma$, whereas $j$ and $k$ are the powers of $\zeta$ and $\eta$, respectively, which $\gamma$ needs to be multiplied by to obtain $c(\gamma) \equiv 0 (\mathrm{mod}\, 5)$ and $a(\gamma) \equiv 0 (\mathrm{mod}\, 5)$. Hence we need to add the appropriate multiple of $i$ given by Lemma 6.1 to $s$ while subtracting the correct multiples of $j$ and $k$.

We implemented the case $\lambda = 5$ on a DECStation 5000. The program was written in the language C and employed multiprecise integer arithmetic. On using a 200 digit modulus $N$ and exponent $e$, our cryptosystem required roughly 22 seconds for key generation and yielded encryption/decryption rates of 23 chars/sec ($\approx$ 183 bits/sec) and 38 chars/sec ($\approx$ 307 bits/sec), respectively. Note that we expect decryption to be significantly faster than encryption, since the encrypter needs to evaluate the residue symbol for each cryptogram.

The computation of the residue symbol whose numerator and denominator had norms of approximately 200 digits required 1.1 to 1.2 seconds of CPU time for both our Euclidean division method and the classical algorithms. Finding a prime divisor of a 100 digit rational prime took 2.4 to 2.5 CPU seconds, again for all three Euclidean division methods. This proves that the performance of the classical algorithms is very similar to that of the algorithm given here despite the significantly worse bounds.

Our scheme is noticeably slower than commercial RSA applications. This is primarily due to the residue symbol computation required for encryption. Furthermore, our implementation was entirely done in software, whereas many commercial RSA packages use hardware for their modular exponentiation. Thus it appears that our cryptosystem, while making use of a number of mathematically interesting concepts and algorithms, pays the price of loosing some of its practicality in comparison to RSA and the quadratic schemes of Rabin and Williams.

## Acknowledgements

The authors wish to gratefully acknowledge the assistance given by H. W. Lenstra, Jr. In addition, we would like to thank the referee for his helpful comments and suggestions.

## Notes

1. In an algebraic number field, every integral *ideal* $\mathbf{a}$ in $\mathbf{O}$ has a unique factorization into powers of prime ideals. In general, we can define $\left[\frac{\alpha}{\mathbf{p}}\right] = \zeta^k$ where $\mathbf{p}$ is a prime ideal not containing $\alpha$ and $\alpha^{\frac{N(\mathbf{p})-1}{\lambda}} \equiv \zeta^k \pmod{\mathbf{p}}$, $0 \leq k \leq \lambda - 1$. Similarly, $\left[\frac{\alpha}{\mathbf{a}}\right] = \prod_{i=1}^{r} \left[\frac{\alpha}{\mathbf{p}_i}\right]^{e_i}$, where, $\mathbf{a} = \prod_{i=1}^{r} \mathbf{p}_i^{e_i}$.
2. For a real number $a$, $\lfloor a \rfloor$ denotes the floor of $a$, i.e. the integer $n$ such that $n \leq a < n + 1$.

## References

1. E. Bach, Explicit bounds for primality testing and related problems, *Math. Comp.*, Vol. 55, No. 191 (1990) pp. 355–380.
2. J. Buchmann, On the computation of units and class numbers by a generalization of Lagrange's algorithm, *J. Number Theory*, Vol. 26, No. 1 (1987) pp. 8–30.
3. J. Buchmann and H. C. Williams, On principal ideal testing in totally complex quartic fields and the determination of certain cyclotomic constants, *Math. Comp.*, Vol. 48, No. 177 (1987) pp. 55–66.
4. J. Buchmann and H. C. Williams, On principal ideal testing in algebraic number fields, *J. Symb. Comp.*, Vol. 4 (1987) pp. 11–19.
5. E. E. Kummer, *Collected Papers*, Vol. 1, Springer, Berlin (1975).
6. E. Landau, *Vorlesungen über Zahlentheorie*, Chelsea, New York (1969).
7. H. W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, *J. Lond. Math. Soc.* Vol. 2, No. 10 (1975) pp. 457–465.
8. H. W. Lenstra, Jr., Euclidean number fields I, *Math. Intelligencer*, Vol. 2 (1979/80) pp. 6–15.
9. J. Loxton, D. S. P. Khoo, G. J. Bird, and J. Seberry, A cubic residue code equivalent to factorization, *J. of Cryptology*, Vol. 5, No. 2 (1992) pp. 139–150.
10. J. M. Masley and H. L. Montgomery, Cyclotomic fields with unique factorization, *J. Reine Angew. Math.*, Vol. 286/287 (1976) pp. 248–256.
11. R. G. McKenzie, *The Ring of Cyclotomic Integers of Modulus Thirteen Is Norm-Euclidean*, Ph.D. Dissertation, Department of Mathematics, Michigan State University (1988).
12. M. O. Rabin, Digitized Signatures and Public-Key Functions as Intractable as Factorization, M.I.T. Lab for Computer Science, Tech. Rep. LCS/TR-212 (1979).
13. H. J. S. Smith, *Report on the Theory of Numbers*, Chelsea, New York (1965).
14. J. Uspensky, Note sur les nombres entiers dépendant d'une racine cinquième de l'unité, *Math. Ann.*, Vol. 66 (1909) pp. 109–112.
15. H. C. Williams, A modification of the RSA public-key encryption procedure, *IEEE Trans. Inf. Theory*, Vol. IT-26, No. 6 (1980) pp. 726–729.
16. H. C. Williams, An $M^3$ public-key encryption scheme, *Advances in Cryptology—CRYPTO '85 Proceedings*, Springer, Berlin (1986), pp. 358–368.
17. K. S. Williams, Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity, *J. Reine Angew. Math.*, Vol. 288 (1976) pp. 207–210.