New Number-Theoretic Cryptographic Primitives

Éric Brier\(^1\), Houda Ferradi\(^2\), Marc Joye\(^3\), and David Naccache\(^4\)

\(^1\) Ingenico
9 Avenue de la Gare, 26300 Alixan, France
eric.brier@ingenico.com

\(^2\) NTT Secure Platform Laboratories
3–9–11 Midori-cho, Musashino-shi, Tokyo 180–8585, Japan
houda.ferradi@ens.fr

\(^3\) OneSpan
Romeinsesteenweg 564 C, 1853 Grimbergen, Belgium
marc.joye@onespan.com

\(^4\) DIENS, École normale supérieure, CNRS, PSL University
45 rue d’Ulm, 75230, Paris Cedex 05, France
david.naccache@ens.fr

Abstract. This paper introduces new \(p^rq\)-based one-way functions and companion signature schemes. The new signature schemes are interesting because they do not belong to the two common design blueprints, which are the inversion of a trapdoor permutation and the Fiat–Shamir transform. In the basic signature scheme, the signer generates multiple RSA-like moduli \(n_i = p_i^2q_i\) and keeps their factors secret. The signature is a bounded-size prime whose Jacobi symbols with respect to the \(n_i\)’s match the message digest. The generalized signature schemes replace the Jacobi symbol with higher-power residue symbols.

Given their very unique design the proposed signature schemes seem to be overlooked “missing species” in the corpus of known signature algorithms.

Keywords: \(r\)th-power residue symbol · \(r\)th-order imprint · \(p^rq\) moduli · Number theory · One-way functions · Digital signatures · Cryptographic primitives

1 Introduction

One-Way Functions. A fundamental building block for constructing secure signature schemes or public-key cryptosystems is one-way functions [15, Chapter 2]. Informally, a one-way function (OWF) is a function \(f\) that is easy to compute in polynomial time (by definition) on every input, but hard to invert given the image of a random input.

Basically, there exist three families of OWFs: (i) one-way permutations which are bijective OWFs, (ii) trapdoor OWFs which are one-way unless some extra information is given, and (iii) collision-free or collision-resistant hash functions. Almost all known OWFs have been based on intractable problems from number theory or some related mathematical fields like coding theory.

Digital Signatures. Diffie and Hellman in their seminal work [11] first pointed out the notion of digital signatures. Since then, there have been many signature proposals built from trapdoor one-way permutations based on different algebraic assumptions. The most well-known being the one devised by Rivest, Shamir and Adleman from the so-called RSA assumption [36].

Concurrently to the above, another popular approach to construct signature schemes is by using the Fiat–Shamir tranform [13]. It consists in turning a public-coin proof of knowledge into a signature scheme, which has yielded many efficient signature schemes like the Schnorr signature [42].
Cryptography Modulo $p'q$. Moduli of the form $p'q$ have found a few applications in cryptography since the mid 1980s, the most notable of which are probably the ESIGN signature scheme and its variants using $p^2q$ [33,14,31,18,43], Okamoto–Uchiyama’s cryptosystem [32,41], Schmidt-Samoa’s cryptosystem [40] or constructions such as [44] and [38].

There are four main approaches of factorization algorithms for the structure $p^r q$: The Elliptic Curve Method (ECM) [27] which was improved by Peralta and Okamoto [35], the Number Field Sieve (NFS) [23], the Lattice Factoring Method (LFM) [4] and factoring using Jacobi symbols. Note that the special structure of $p^r q$ is not threatened by NFS beyond regular RSA moduli are threatened by that same attack. Actually, it turns out that using $p^2 q$ moduli does not seem to render factoring significantly easier. Boneh, Durfee and Howgrave-Graham [4] showed that $n = p^r q$ can be factored in polynomial time when $r$ is large (i.e., $r \approx \log p$). Consequently, as stated in [30], this LLL-based approach [24] does not apply to the setting considered in this paper where $r$ is rather small. See also [29,28].

Organization. The rest of this paper is organized as follows. In the next section, we introduce some useful notation and review the definitions of the Jacobi symbol and of a signature scheme. Section 3 proposes a new OWF, building on the concept of Jacobi imprint. We then present in Section 4 a first signature scheme relying on this new OWF and prove its security. In Section 5, we generalize our basic design to higher-order residue symbols and introduce the corresponding signature schemes. As an illustration, we implement Quartapus in Section 6, a signature scheme based on the quartic residue symbol. Finally, we conclude the paper in Section 7.

2 Notation and Basic Definitions

If $D$ is a finite domain, we let $x \overset{\mathcal{R}}{\leftarrow} D$ denote picking an element of $D$ uniformly at random and assigning it to $x$. A boldface variable $x$ is used to denote a vector of elements identified by that variable; i.e., $x = (x_0, \ldots, x_{k-1})$. The symbol $\mathbb{P}$ stands for the set of (rational) primes. Given a vector $n = (n_0, \ldots, n_{k-1})$ of pairwise co-prime integers $n_j$ ($0 \leq j \leq k-1$) and a vector $x = (x_0, \ldots, x_{k-1})$ of integers, we use $\text{CRT}(x, n)$ for the Chinese-remainder function, returning the smallest non-negative integer $y$ such that $y \equiv x_j \pmod{n_j}$ for $0 \leq j \leq k-1$ [12, Chapter 2].

2.1 The Jacobi Symbol

Given a positive integer $n$, an integer $a$ with $\gcd(a, n) = 1$ is called a quadratic residue modulo $n$ if and only if $x^2 \equiv a \pmod{n}$ is solvable. If $a$ is not a quadratic residue then it is called a quadratic non-residue modulo $n$.

Let $a$ be an integer and let $p \in \mathbb{P}$, $p \neq 2$. The Legendre symbol $\left( \frac{a}{p} \right)$ is defined as:

$$\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p, \\
-1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\
0 & \text{if } \gcd(a, p) \neq 1.
\end{cases}$$

The Legendre symbol satisfies Euler’s criterion, namely $\left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

The Jacobi symbol is a natural generalization of the Legendre symbol.

**Definition 1.** Let $n$ be an odd positive integer with prime factorization $n = \prod_j p_j^{e_j}$. Then, for an integer $a$, the Jacobi symbol $\left( \frac{a}{n} \right)$ is given by

$$\left( \frac{a}{n} \right) = \prod_j \left( \frac{a}{p_j} \right)^{e_j}$$

with the convention $\left( \frac{a}{1} \right) = 1$ for all integers $a$. 

2
Interestingly, the prime factorization of \( n \) is not required for evaluating \( \left( \frac{a}{n} \right) \). It can be efficiently computed with \( O((\log_2 a)(\log_2 n)) \) bit operations [1, § 5.9]. We point out that the Legendre and Jacobi symbols are indistinguishable when \( n \) is an odd prime. Also, we note that the Legendre symbol allows to determine whether an integer is a quadratic residue or not, whereas the Jacobi symbol does not allow checking this property.

### 2.2 Digital Signatures

A signature scheme [20] is a tuple, \( \Sigma = (\text{KeyGen}, \text{Sign}, \text{Verify}) \), of probabilistic polynomial-time algorithms satisfying:

- **KeyGen\((1^\kappa)\)** On input security parameter \( 1^\kappa \), key generation algorithm KeyGen produces a pair \((pk, sk)\) of matching public and private keys.
- **Sign\((sk, m)\)** Given a private key \( sk \) and a message \( m \) in a set \( M \) of messages, signing algorithm Sign produces a signature \( \sigma \).
- **Verify\((pk, m, \sigma)\)** Given a public key \( pk \), a message \( m \in M \), and a signature \( \sigma \), the verifying algorithm Verify checks whether \( \sigma \) is a valid signature on \( m \) with respect to \( pk \).

The classical security notion for signature schemes is **existential unforgeability against chosen-message attacks** (in short, EUF-CMA) [16]. Basically, it requires that an adversary having access to a signing oracle returning the signature on messages of its choice is unable to produce a valid signature on a message not previously submitted to the signing oracle. In the **random oracle model** [2], the adversary has in addition access to a hash oracle viewed as a random oracle. More formally:

**Definition 2.** A signature scheme \( \Sigma \) is **EUF-CMA secure** if, for every probabilistic polynomial-time adversary \( A \), the success probability, \( \text{Adv}_{\mathcal{A}, \Sigma}^{\text{EUF}}(\kappa) := \text{Pr}[\text{EUF}_A^\Sigma(\kappa) = 1] \), is negligible against the security game defined in Figure 1.

![EUF-CMA experiment for digital signature schemes.](https://example.com/fig1.png)

### 3 A Candidate One-Way Function

If \( p \) is an odd prime then half of the integers in the sequence \( 1, 2, \ldots, p - 1 \) are quadratic residues modulo \( p \), and half are not. The problem of counting the number of occurrences of \( k \) distinct integers \( (a_0, a_1, \ldots, a_{k-1}) \) modulo \( p \) obeying a given pattern \( (\epsilon_0, \epsilon_1, \ldots, \epsilon_{k-1}) \) with \( \epsilon_j = \left( \frac{a_j}{p} \right) \in \{-1, 1\} \) and variations thereof has been studied in a number of papers, including [9,10,7,34,17,37]. In particular, the results of Peralta in [34] indicate that the probability of

\[
\left( \left( \frac{a_0}{p} \right), \left( \frac{a_1}{p} \right), \ldots, \left( \frac{a_{k-1}}{p} \right) \right)
\]

matching any particular sequence \( (\epsilon_0, \epsilon_1, \ldots, \epsilon_{k-1}) \in \{-1, 1\}^k \) is in the range \( \frac{1}{p} \pm O(kp^{-1/2}) \).
This section considers a related problem. It relies on a new notion that we call *Jacobi imprint*. In essence, the imprint is an integer formed of bits representing the sequence of Jacobi symbols where −1’s are replaced by 1’s and 1’s by 0’s.

**Definition 3 (Jacobi Imprint).** For an integer $a$ and $n = (n_0, \ldots, n_{k-1}) \in \mathbb{N}^k$ such that $\gcd(a, n_j) = 1$ for $0 \leq j \leq k - 1$, the Jacobi imprint $I(a)$ is given by

$$I(a) = \left\{ \left( \frac{a}{n_j} \right) \right\} 2^j \quad \text{where} \quad \left( \frac{a}{n_j} \right) = \frac{1 - \left( \frac{a}{n_j} \right)}{2}.$$  

(At times we will interchangeably use $I(a)$ to denote the integer $I_n(a)$ or its binary representation.)

### 3.1 Function $F_0$

Let $q = (q_0, \ldots, q_{k-1})$ be a set of $k$ distinct (odd) primes and let $Q = \prod_{j=0}^{k-1} q_j$. Consider the function $F_0$ given by

$$F_0: \mathcal{D} \subset \mathbb{Z}_Q^* \to \mathbb{N}, x \mapsto F_0(x) = I_q(x).$$

We argue that an appropriate selection for the domain of $F_0$ and the number of primes $q_j$’s turns $F_0$ into a one-way function.

Of course, $\mathcal{D}$ cannot be the whole group $\mathbb{Z}_Q^*$. Otherwise, given a challenge $\hat{y} = F_0(\hat{x})$, an attacker could execute Algorithm 1.

**Algorithm 1: Finding a (large) pre-image**

**Data:** $\hat{y} = \sum_{j=0}^{k-1} \hat{y}_j 2^j$ with $\hat{y}_j \in \{0, 1\}$ and $q = (q_0, \ldots, q_{k-1})$

**Result:** $x \in \mathbb{Z}_Q^*$ such that $F_0(x) = \hat{y}$

**for** $0 \leq j \leq k - 1$

**do**

$r_j \leftarrow \mathbb{Z}_{q_j}^*$ such that $\left\{ \frac{r_j}{q_j} \right\} = \hat{y}_j$

**end**

$x \leftarrow \text{CRT}(r, q)$ where $r = (r_0, \ldots, r_{k-1})$

return $x$

This algorithm yields outputs that are smaller than $Q = \prod_{j=0}^{k-1} q_j$. An obvious way to prevent an attacker to successfully run Algorithm 1 would be to restrict $\mathcal{D}$ to entries smaller than a given bound $B$.

But there is another way to tackle the problem of finding pre-images to $F_0$. Let $\mathcal{Z}$ be the set of $k$-bit integers in $\mathbb{N}$. Now if we regard an imprint in $\mathcal{Z}$ as an element of $(\mathbb{Z}_2)^k$ (that is, if we look at its binary representation), we see that $F_0$ induces a group homomorphism from $(\mathbb{Z}_Q^*, \cdot)$ to $(\mathbb{Z}, \oplus)$:

$$F_0(x_1 \cdot x_2 \mod Q) = F_0(x_1) \oplus F_0(x_2), \quad \forall x_1, x_2 \in \mathbb{Z}_Q^*.$$  

Therefore, an attacker could generate a set of $\ell$ “small” primes $p_i$’s (with $p_i \nmid Q$) and compute the corresponding imprint $z_i = F_0(p_i)$, for $1 \leq i \leq \ell$. It suffices then for the attacker to use linear algebra modulo 2 (i.e., Gaussian elimination) to find a subset of the $z_i$’s having the target imprint $\hat{y}$ as an xor:

$$\hat{y} = \varepsilon_1 z_1 \oplus \cdots \oplus \varepsilon_\ell z_\ell \quad \text{with} \quad \varepsilon_i \in \{0, 1\}.$$  

A pre-image is given by

$$x = \prod_{1 \leq i \leq \ell, \varepsilon_i = 1} p_i,$$

\(^5\) If a solution $\varepsilon_1, \ldots, \varepsilon_\ell$ does not exist, refresh the $p_i$’s as necessary.
which is valid provided that \( x < B \). This second attack is avoided by limiting \( \mathcal{D} \) to primes.

Furthermore, each prime \( q_j \) in \( q \) imposes a condition on the pre-image. The birthday paradox suggests to choose the number \( k \) of primes \( q_j \)'s to be at least \( 2\kappa \), where \( \kappa \) is the security parameter.

All in all, we recommend to select \( k = 2\kappa \) and \( \mathcal{D} = \{ x \in \mathbb{P} \mid x < B \text{ with } B \ll Q \text{ where } Q = \prod_{j=0}^{k-1} q_j \} \).

### 3.2 From \( \mathcal{F}_0 \) to \( \mathcal{F}_1 \)

We use function \( \mathcal{F}_0 \) as a starting point to define a (conjectured) trapdoor one-way function. The resulting function \( \mathcal{F}_1 \) has the extra property that it can be inverted when it is given a trapdoor as an additional input. To insert a trapdoor, we replace the primes \( q_j \)'s with RSA-like moduli of the form \( n_j = p_j^2q_j \). This does not affect the output value since \( \mathcal{I}_n(x) = \mathcal{I}_q(x) \) for all \( x \) such that \( \gcd(x,n_j) = 1 \) for \( 0 \leq j \leq k - 1 \). The trapdoor is \( q \).

We conjecture:

**Assumption 1.** Let \( \kappa \) denote a security parameter. Let also \( k = k(\kappa) \) and \( \ell = \ell(\kappa) \). Define \( \mathcal{D} = \{ x \in \mathbb{P} \mid x < 2^{k\ell} \} \) and

\[
\mathcal{F}_1 : \mathcal{D} \to \mathbb{N}, x \mapsto \mathcal{F}_1(x) = \mathcal{I}_n(x)
\]

where \( n = (n_0, \ldots, n_{k-1}) \) is a set of \( k \) pairwise co-prime moduli of the form \( n_j = p_j^2q_j \) for \( \ell \)-bit primes \( p_j \) and \( q_j \), \( 0 \leq j \leq k - 1 \). For every polynomial-time algorithm \( \mathcal{A} \), the success probability

\[
\Pr[\hat{x} \in \mathcal{D}; \mathcal{A}(\mathcal{F}_1(\hat{x})) = x \mid \mathcal{F}_1(x) = \mathcal{F}_1(\hat{x})]
\]

is negligible.

Note that finding a pre-image to \( \hat{y} = \mathcal{F}_1(\hat{x}) \) is easy given the trapdoor \( q = (q_0, \ldots, q_{k-1}) \):

1. Run Algorithm 1 and obtain \( x \) such that \( \mathcal{I}_q(x) = \hat{y} \);
2. Update \( x \) as \( x \leftarrow xu^2 \mod Q \) with \( u \in \mathbb{Z}_{q_j}^* \) until \( x \) is prime;
3. Return \( x \).

Clearly, the so-obtained \( x \) is a valid pre-image: \( x \in \mathcal{D} \) and \( \mathcal{F}_1(x) = \hat{y} \).

**Remark 1.** By definition, the Jacobi imprint \( \mathcal{I}_n(x) \) requires \( x \) to be co-prime with \( n_j \) for \( 0 \leq j \leq k - 1 \). Strictly speaking, the domain \( \mathcal{D} \) should therefore exclude the primes \( p_j \) and \( q_j \). However, since primes \( p_j \) and \( q_j \) are \( \ell \)-bit primes—where \( \ell = \ell(\kappa) \)—the probability to output an \( x \) such that \( \gcd(x,n_j) \neq 1 \) for some \( 0 \leq j \leq k - 1 \) is negligible when the prime factorization of the \( n_j \)'s is unknown.

### 4 Signatures Modulo \( p^2q \)

We are now ready to formally describe a first signature scheme. We prove that it meets the EUF-CMA security level in the random oracle model.

#### 4.1 Description

Our basic signature scheme is a tuple of algorithms \( \Sigma = (\text{KeyGen}, \text{Sign}, \text{Verify}) \), which we define as follows:

**Key generation** The key generation algorithm \( \text{KeyGen} \) takes as input a security parameter \( 1^k \) and defines parameters \( k \) and \( \ell \). It selects a collision-resistant hash function \( H : \{0,1\}^* \to \{0,1\}^k \). It also produces \( k \) pairs \( (p_j,q_j) \) of \( \ell \)-bit primes and forms the moduli \( n_j = p_j^2q_j \). The public parameters are \( \text{pp} = (k,\ell,H) \). The public key is \( \text{pk} = \{ n_j \}_{0 \leq j \leq k-1} \) while the private key is \( \text{sk} = \{ q_j \}_{0 \leq j \leq k-1} \). The outputs are \( \text{pk} \) and \( \text{sk} \) (and \( \text{pp} \)).
Signing  The signing algorithm $\text{Sign}$ takes as inputs a message $m \in \{0,1\}^*$ and the secret key $sk$. The signature on message $m$ proceeds as follows:

1. Compute $H(m) = \sum_{j=0}^{k-1} h_j 2^j$ with $h_j \in \{0,1\}$;
2. Pick at random $k$ $\ell$-bit integers $r_j$ such that
dsatisfies

\[
\left\{ \frac{r_j}{q_j} \right\} = h_j, \quad \text{for } 0 \leq j \leq k - 1;
\]

3. Compute

\[R = \text{CRT}(r, q)\]

with $r = (r_0, \ldots, r_{k-1})$ and $q = (q_0, \ldots, q_{k-1})$;
4. Set $Q = \prod_{j=0}^{k-1} q_j$ and choose at random an integer $u \in \mathbb{Z}_Q^*$ such that

\[
\sigma := Ru^2 \mod Q \in \mathbb{P};
\]
5. Return $\sigma$.

Verification  The verifying algorithm $\text{Verify}$ takes as inputs the public key $pk$, a message $m$, and a signature $\sigma$ on message $m$. It checks whether

- $(i)$ $\sigma \in \mathbb{P}$,
- $(ii)$ $\sigma < 2^{\ell k}$,
- $(iii)$ $\mathcal{J}_n(\sigma) = H(m)$

where $n = (n_0, \ldots, n_{k-1})$. $\text{Verify}$ returns 1 (i.e., the signature is accepted) if and only if the three conditions above are fulfilled. Otherwise, $\text{Verify}$ returns 0.

The next proposition shows that the signature scheme is correct: for $(pk, sk) \leftarrow \text{KeyGen}(1^\kappa)$ and any message $m \in \{0,1\}^*$, $\text{Verify}(pk, m, \text{Sign}(m, sk)) = 1$.

**Proposition 1 (Correctness).** Signature scheme $\Sigma$ is correct.

**Proof.** Let $\{(\{n_j\}, \{q_j\})\}$ and $\sigma$ be the respective outputs of $\text{KeyGen}$ and $\text{Sign}$, with message $m$ as input. By construction, $\sigma$ is prime and $\sigma = Ru^2 \mod Q < 2^{\ell k}$. Moreover, since $\sigma \equiv r_j u^2 \pmod{q_j}$ ($0 \leq j \leq k - 1$), it follows that

\[
\mathcal{J}_q(\sigma) = \sum_{j=0}^{k-1} \left\{ \frac{r_j u^2}{q_j} \right\} 2^j = \sum_{j=0}^{k-1} \left\{ \frac{r_j}{q_j} \right\} 2^j.
\]

Finally, since $n_j = p_j^2 q_j$, we have $\left\{ \frac{r_j}{q_j} \right\} = \left\{ \frac{r_j}{q_j} \right\}$, and so $\mathcal{J}_n(\sigma) = \mathcal{J}_q(\sigma) = H(m)$.

### 4.2 Security Proof

**Theorem 1.** Signature scheme $\Sigma$ is EUF-CMA secure assuming the hardness of inverting $\mathcal{F}_1$, in the random oracle model.

**Proof.** The security proof is by contradiction. Suppose we are given as a challenge an output $\hat{s}$ of the function $\mathcal{F}_1$. We assume that there exists a polynomial-time adversary $A$ that is able to produce an existential signature forgery with non-negligible success probability. Adversary $A$ is allowed to make $q_H$ queries to random oracle $H$ and $q_\sigma$ queries to signing oracle $\text{Sign}$. We then use $A$’s forgery to invert $\mathcal{F}_1$; i.e., to find a pre-image to $\hat{s}$.

Specifically, suppose that the received challenge is the $k$-bit integer

\[\hat{s} \leftarrow \mathcal{F}_1(x) = \mathcal{J}_n(x) \quad \text{with } n = (n_0, \ldots, n_{k-1})\]

for moduli $n_j$ of the form $n_j = p_j^2 q_j$ where $p_j$’s and $q_j$’s are $\ell$-bit primes; $0 \leq j \leq k - 1$. The simulator sets the public key to $pk = \{n_j\}_{0 \leq j \leq k-1}$. It also selects a collision-resistant hash function $H$ mapping to $\{0,1\}^k$.

The public key $pk$ as well as public parameters $pp = (k, \ell, H)$ are given to $A$.

The simulator needs to answer the oracle queries made by $A$. It maintains a history list of tuples $(m_i, b_i, \sigma_i), \text{Hist}[H]$, that keeps track of the hash queries; $\text{Hist}[H]$ is initialized to $\emptyset$. It also maintains a counter $i$ initialized to 0 and chooses at random an index $i^* \in [1, \ldots, q_H]$.  


Answering hash queries When \( A \) submits a message \( m \) to \( H \), the simulator checks whether \( m \) was already queried:

- If \( m \notin \text{Hist}[H] \) then \( i \) is incremented: \( i \leftarrow i + 1 \). Next, the simulator sets \( m_i \leftarrow m \) and depending on the value of \( i \):
  - if \( i = i^* \), it sets \( h_i \leftarrow \hat{s} \) and \( \sigma_i \leftarrow \perp \);
  - if \( i \neq i^* \), it generates a random \( k \)-bit prime \( \sigma_i \) and sets \( h_i \leftarrow \mathcal{J}_n(\sigma_i) \).

Tuple \((m_i, h_i, \sigma_i)\) is appended to \( \text{Hist}[H] \): \( \text{Hist}[H] \leftarrow \text{Hist}[H] \cup (m_i, h_i, \sigma_i) \).

- If \( m \in \text{Hist}[H] \), the simulator finds the index \( i \) such that \( m = m_i \) and recovers the corresponding value \( h_i \).

The simulator returns \( h_i \) as the hash value of input message \( m \).

Answering signature queries Without loss of generality, we assume that when \( A \) calls signing oracle \( \text{Sign} \) with a message \( m \), it has already submitted \( m \) to hash oracle \( H \) (observe that the simulator can always call internally \( H \)). Therefore, there exists an index \( i \) such that \( m = m_i \) in \( \text{Hist}[H] \). The simulator recovers the corresponding value for \( \sigma_i \). There are two cases:

- If \( \sigma_i \neq \perp \) then the simulator returns \( \sigma_i \) as a valid signature on input message \( m \);
- Otherwise the simulator fails and stops.

The number of queries to the hash oracle being polynomial, with non-negligible probability, the adversary will return a signature forgery on its \( i^* \)-th query to \( H \); i.e., on message \( m_{i^*} \). Letting \( \sigma_{i^*} \) the corresponding signature returned by \( A \), we see that \( \sigma_{i^*} \) is a solution to the challenge since \( \mathcal{J}_n(\sigma_{i^*}) = H(m_{i^*}) = \hat{s} \).

4.3 Toy Example \((k = 8)\)

Picking the secret primes

<table>
<thead>
<tr>
<th>( j )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p_j )</td>
<td>59069</td>
<td>54139</td>
<td>52639</td>
<td>53813</td>
<td>49871</td>
<td>41269</td>
<td>53653</td>
<td>40361</td>
</tr>
<tr>
<td>( q_j )</td>
<td>62989</td>
<td>32917</td>
<td>36583</td>
<td>48383</td>
<td>36653</td>
<td>34963</td>
<td>52517</td>
<td>38971</td>
</tr>
</tbody>
</table>

we have the public moduli

\[
\begin{align*}
 n_0 &= 219777865328629 \\
 n_1 &= 096480757993357 \\
 n_2 &= 101366529455143 \\
 n_3 &= 140109376837127 \\
 n_4 &= 091160286242573 \\
 n_5 &= 059546546811643 \\
 n_6 &= 15117768427453 \\
 n_7 &= 063484161219691 
\end{align*}
\]

and the value \( Q = \prod_{i=0}^{7} q_i = 9625354820834804430180854766785161 \).

Consider a message whose digest is \( \mathbf{h} = (h_0, \ldots, h_7) \) and draw \( r_j \)'s as:

<table>
<thead>
<tr>
<th>( j )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>( h_j )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( r_j )</td>
<td>64863</td>
<td>58999</td>
<td>47120</td>
<td>50684</td>
<td>37458</td>
<td>57079</td>
<td>43135</td>
<td>56942</td>
</tr>
</tbody>
</table>

We get \( \text{CRT}(r, q) = 1395786251559231878789764535858641198 \).

By selecting \( u = 2152266820709866295140077504687803459 \), we obtain the signature

\[
\sigma = 1137542561586761230770585345256092841 \in \mathbb{P} .
\]

5 Generalized Signatures

The Legendre symbol tells whether an integer is a square modulo a prime \( p \). Given an integer \( a \) and an odd prime \( p \), if \( p \nmid a \), there exists a unique integer \( j \) modulo 2 such that \( a^{(p-1)/2} \equiv (-1)^j \pmod{p} \). To obtain the analogue to a higher power \( r \), the rational integers need to be extended so that they include an \( r \)-th root of unity, namely \( e^{2\pi i/r} \).
5.1 Cyclotomic Integers and Higher-Order Residuosity

We start by reviewing some classical results on cyclotomic fields. We refer the reader to [19] and [45] for further introductory background.

Fix \( \zeta := \zeta_r \) a primitive \( r \)th root of unity; i.e., \( \zeta \) is a root of \( X^r - 1 \) and \( X^s \neq 1 \) for \( 0 < s < r \). Adjoining \( \zeta \) to the field \( \mathbb{Q} \) of rationals defines the cyclotomic field \( \mathbb{Q}(\zeta) \). It is the splitting field of \( X^r - 1 \); its Galois group \( \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \) is isomorphic to \( \mathbb{Z}_r^* \), with \( k \) mod \( r \) corresponding to the map \( \sigma_k : \zeta \mapsto \zeta^k \); see [19, Proposition 13.2.1] or [45, Theorem 2.5]. The ring of integers of \( \mathbb{Q}(\zeta) \) is \( \mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(\Phi_r) \) where \( \Phi_r \) is the \( r \)th cyclotomic polynomial; see [45, Theorem 2.6].

The elements \( \alpha \) of \( \mathbb{Z}[\zeta] \) are written as
\[
\alpha = \sum_{0 \leq j < \varphi(r)} a_j \zeta^j \quad \text{with } a_j \in \mathbb{Z}
\]
where \( \varphi \) denotes Euler’s totient function. The norm of \( \alpha \in \mathbb{Z}[\zeta] \) is the rational integer given by \( N(\alpha) = \prod_{k \in \mathbb{Z}_r^*} \sigma_k(\alpha) \). We assume that \( \mathbb{Z}[\zeta] \) is norm-Euclidean.\(^6\)

The elements of norm \( \pm 1 \) in \( \mathbb{Z}[\zeta] \) are called units. Two elements \( \alpha, \beta \in \mathbb{Z}[\zeta] \) that are equal up to multiplication by a unit \( \nu \in \mathbb{Z}[\zeta] \) (i.e., \( \alpha = \nu \beta \)) are said to be associates; we write \( \alpha \sim \beta \). A non-unit element \( \pi \in \mathbb{Z}[\zeta] \) is a prime in \( \mathbb{Z}[\zeta] \) if, for any \( \alpha, \beta \in \mathbb{Z}[\zeta] \), \( \pi \mid \alpha \beta \) implies \( \pi \mid \alpha \) or \( \pi \mid \beta \). If \( r \) is a prime power (i.e., \( r = q^\ell \) for some rational prime \( q \) and \( \ell \geq 1 \)) then \( (1 - \zeta) \) is a prime in \( \mathbb{Z}[\zeta] \) and \( N(1 - \zeta) = q \); otherwise, \( (1 - \zeta) \) is a unit in \( \mathbb{Z}[\zeta] \).

Let \( \pi \) be a prime in \( \mathbb{Z}[\zeta] \), with \( \gcd(N(\pi), r) = 1 \). For every \( \alpha \in \mathbb{Z}[\zeta] \) such that \( \pi \nmid \alpha \), we have \( \alpha^{N(\pi) - 1} \equiv 1 \pmod{\pi} \). Further, \( \langle \zeta \rangle \) is a subgroup of order \( r \) of \( (\mathbb{Z}[\zeta]/(\pi))^* \), it follows that \( r \mid (N(\pi) - 1) \) and
\[
\alpha^{N(\pi) - 1}/r \equiv \zeta^j \pmod{\pi} \quad \text{for some } j \in \mathbb{Z}_r.
\]

This defines the \( r \)th-power residue symbol.

**Definition 4.** Fix \( \zeta \) a primitive \( r \)th root of unity. Let \( \alpha, \pi \in \mathbb{Z}[\zeta] \) with \( \pi \) prime and \( \gcd(N(\pi), r) = 1 \). The \( r \)th-power residue symbol is defined by
\[
\left[ \frac{\alpha}{\pi} \right]_r = \begin{cases} \alpha^{N(\pi) - 1}/r \mod \pi & \text{if } \pi \nmid \alpha, \\ 0 & \text{otherwise}. \end{cases}
\]

Let \( \alpha, \beta, \pi \in \mathbb{Z}[\zeta] \) with \( \pi \) prime and \( \gcd(N(\pi), r) = 1 \). It is easily verified from the definition that the following properties are satisfied:
\[
\left[ \frac{\alpha \beta}{\pi} \right]_r = \left[ \frac{\alpha}{\pi} \right]_r \left[ \frac{\beta}{\pi} \right]_r, \quad \left[ \frac{\alpha}{\pi} \right]_r = \left[ \frac{\alpha \mod \pi}{\pi} \right]_r.
\]

Furthermore, in a way similar to the Jacobi symbol for quadratic residuosity, the \( r \)th-power residue symbol naturally generalizes.

**Definition 5.** Fix \( \zeta \) a primitive \( r \)th root of unity. Let \( \alpha, \lambda \in \mathbb{Z}[\zeta] \) with \( \lambda \) non-unit and \( \gcd(N(\lambda), r) = 1 \). Then, writing \( \lambda = \prod_j \pi_j^{e_j} \) for primes \( \pi_j \) in \( \mathbb{Z}[\zeta] \), if \( \alpha \) and \( \lambda \) are co-prime, the symbol \( \left[ \frac{\alpha}{\lambda} \right]_r \) is defined by
\[
\left[ \frac{\alpha}{\lambda} \right]_r = \prod_j \left[ \frac{\alpha}{\pi_j} \right]_r^{e_j}.
\]

Moreover, \( \left[ \frac{\alpha}{\pi} \right]_r = 1 \) for every unit \( \nu \in \mathbb{Z}[\zeta] \).

---

\(^6\) A ring \( R \) is said norm-Euclidean or Euclidean with respect to the norm \( N \) if for every \( \alpha, \beta \in R \), \( \beta \neq 0 \), there exist \( \eta, \rho \in R \) such that \( \alpha = \beta \eta + \rho \) and \( N(\rho) < N(\beta) \).
The notion of Jacobi imprint generalizes to higher powers. To ease the notation, we extend the brace symbol as follows:

\[
\left\{ \frac{\alpha}{\lambda} \right\}_r = j \quad \text{with} \quad j \in \mathbb{Z}_r
\]

where \( \left\{ \frac{\alpha}{\lambda} \right\}_r = j \) if and only if \( \left\{ \frac{\alpha}{\lambda} \right\}_r = \zeta^j \). Note that Definition 3 corresponds to the case \( r = 2 \).

**Definition 6 (r-th-order Imprint).** For an integer \( \alpha \in \mathbb{Z}[\zeta] \) and a vector \( \lambda = (\lambda_0, \ldots, \lambda_{k-1}) \in \mathbb{Z}[\zeta]^k \), such that \( \alpha \) and \( \lambda_j \) (with \( 0 \leq j \leq k-1 \)) are co-prime, the \( r \)-th-order imprint of \( \alpha \) w.r.t. \( \lambda \) is the integer \( I_{\lambda}^{(r)}(\alpha) \in \mathbb{Z} \) given by

\[
I_{\lambda}^{(r)}(\alpha) = \sum_{j=0}^{k-1} \left\{ \frac{\alpha}{\lambda_j} \right\}_r r^j.
\]

### 5.2 Parameter Selection

As discussed in the introduction, the main threat for factoring-related cryptosystems comes from NFS and its variants. The next table lists different types of security level and the commonly-accepted corresponding size for the modulus. See e.g. [3].

<table>
<thead>
<tr>
<th>Type</th>
<th>Bit-security</th>
<th>Modulus (bit size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>80</td>
<td>1024</td>
</tr>
<tr>
<td>Basic</td>
<td>112</td>
<td>2048</td>
</tr>
<tr>
<td>Normal</td>
<td>128</td>
<td>3072</td>
</tr>
<tr>
<td>High</td>
<td>192</td>
<td>7680</td>
</tr>
<tr>
<td>Very high</td>
<td>256</td>
<td>15360</td>
</tr>
</tbody>
</table>

The current state of affairs teaches that moduli could be selected of the form \( p_j q_j \) with \( r \geq 2 \) chosen to have a balanced resistance against both NFS-type and ECM-type factoring algorithms. Given a modulus whose length is chosen according to Table 1, a bound for the number of factors that may be allowed is derived in [22, Section 4]. This suggests to select \( r \) in the range \([2, \ldots, 5]\), depending on the security level.

**Remark 2.** If \( \zeta_r \) is an \( r \)-th primitive root of unity, the ring \( \mathbb{Z}[\zeta_r] \) is not necessarily norm-Euclidean. But for \( r \in \{2, 3, 4, 5\} \), the rings \( \mathbb{Z}[\zeta_r] \) are known to be norm-Euclidean [21, §8]; see also [26].

Each possible value for \( r \) gives rise to a signature scheme. Of particular interest are the following new species in the signature zoo:

- **Quadratapus** \( r = 2 \) legacy security;
- **Cubapus-112** \( r = 3 \) basic security;
- **Cubapus-128** \( r = 3 \) normal security;
- **Quartapus** \( r = 4 \) high security;
- **Pentapus** \( r = 5 \) very high security.

\(^7\) Quadratapus is an endangered species.
6 Quartapus

The $p^2q$ signature scheme given in Section 4 extends to any value of $r > 2$ (provided that $\mathbb{Z}[\zeta_r]$ is norm-Euclidean). As an illustration, we detail the Quartapus signature scheme, which is an adaptation to the case $r = 4$.

Throughout this section, we let $\zeta := \zeta_4 = i$ denote a primitive $4$th root of unity. The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ contains the two automorphisms $\sigma_k: \zeta \mapsto \zeta^k$ with $k \in \{1, 2\}$. For an element $\alpha \in \mathbb{Z}[\zeta]$, we write $\alpha_k = \sigma_k(\alpha)$. The norm of $\alpha$ is given by $N(\alpha) = \alpha_1\alpha_2$.

6.1 Description

The Quartapus signature scheme, $(\text{KeyGen}, \text{Sign}, \text{Verify})$, is defined as follows.

**Key generation** KeyGen takes as input a security parameter $1^k$ and defines parameters $k$ and $\ell$. It selects a collision-resistant hash function $H: \{0, 1\}^* \rightarrow (\mathbb{Z}_4)^k$. It also produces $k$ pairs $(\pi_j, \psi_j)$ of primes in $\mathbb{Z}[\zeta]$, where $N(\pi_j)$ and $N(\psi_j)$ are $\ell$-bit long, and forms the moduli $\nu_j = \pi_j^4\psi_j$. The outputs are $pk = (k, \ell, H)$, $pk = \{\nu_j\}_{0 \leq j \leq k-1}$, and $sk = \{\psi_j\}_{0 \leq j \leq k-1}$.

**Signing** On input a message $m \in \{0, 1\}^*$ and sk, Sign does the following:

1. Compute $H(m) = \sum_{j=0}^{k-1} h_j 4^j$ with $h_j \in \mathbb{Z}_4$;
2. Pick at random $k$ integers $\rho_j \in \mathbb{Z}[\zeta]$ of $\ell$-bit norm such that
   \[ \left\{ \frac{\rho_j}{\psi_j} \right\} = h_j, \quad \text{for} \; 0 \leq j \leq k - 1; \]
3. Compute
   \[ \varrho = \text{CRT}(\rho, \psi) \]
   with $\rho = (\rho_0, \ldots, \rho_{k-1})$ and $\psi = (\psi_0, \ldots, \psi_{k-1})$;
4. Set $\Psi = \prod_{j=0}^{k-1} \psi_j$ and choose at random an integer $\upsilon \in (\mathbb{Z}[\zeta]/(\Psi))^*$ such that
   \[ \sigma := \varrho \upsilon^4 \mod \Psi \text{ is prime in } \mathbb{Z}[\zeta]; \]
5. Return $\sigma$.

**Verification** On input $\sigma$, $m$ and $pk$, Verify checks whether

(i) $\sigma$ is prime, (ii) $N(\sigma) < 2^{\ell k}$, (iii) $H(\varphi)(\sigma) = H(m)$

and, if so, accepts the signature.

Remark 3. The primes $\pi_j$’s and $\psi_j$’s must be chosen of norm of $\ell$ bits for an $\ell$ sized for the factoring problem over the rational integers. Indeed, suppose an attacker is given as a challenge $\nu = \pi\psi$, a product of two primes in $\mathbb{Z}[\zeta]$. The goal of the attacker is to recover $\pi$ and $\psi$.

The norm of $\nu$ satisfies $N(\nu) = N(\pi)N(\psi) := pq$ for two $\ell$-bit rational primes $p, q \equiv 1 \pmod{4}$. If $\ell$ were chosen too small so that the problem of factoring the product of two rational $\ell$-bit primes becomes feasible, the attacker could factor $N(\nu)$ and recover $p$ and $q$. Once $p$ and $q$ are found, its remaining task is to find $\pi, \psi \in \mathbb{Z}[\zeta]$ with $N(\pi) = p$ and $N(\psi) = q$. This can be efficiently achieved by generalizing Cornacchia’s algorithm [6, Algorithm 1.5.2] to fourth roots, as done in [8, §1.2] for cubic roots. The first step is to solve for $r$ over $\mathbb{F}_p^*$ the equation $r^2 + 1 = 0 \pmod{p}$. Next, to consider the integer $p := r - \zeta \in \mathbb{Z}[\zeta]$, whose norm is a multiple of $p$. Hence, the computation of gcd$(\rho, p)$ yields $\pi \in \mathbb{Z}[\zeta]$—remember that $\mathbb{Z}[\zeta]$ is norm-Euclidean, and $p = \pi\pi_2$ where $\pi_2 = \sigma_2(\pi)$. And similarly for $q$. 

10
6.2 Evaluating Quartic Residue Symbols

Quartapus requires the evaluation of the $4$th-power residue symbol. We refer to [46,8] for efficient implementations.

A generic algorithm for computing the $r$th-power residue symbol for any prime $r \leq 11$ is described in [5, Section 7]. The case $r = 3$ is discussed in [47,8,39] and the case $r = 5$ in [39].

7 Concluding Remarks

In this paper, we have introduced a formal definition and construction of a new family of one-way functions and signature schemes. They are related to the hardness of factoring moduli of the form $n = p^r q$. Since our constructions rely on newly introduced assumptions, further cryptanalytic efforts are demanded in order to get more confidence about their exact security.

Acknowledgments  We are grateful to Dan Bernstein, Dan Boneh, and Antoine Joux for comments and discussions on the ECM factoring method.

References