The Rabin cryptosystem revisited

Michele Elia∗, Matteo Piva †, Davide Schipani ‡

April 28, 2013

Abstract

The Rabin public-key cryptosystem is revisited with a focus on the problem of identifying
the encrypted message unambiguously for any pair of primes. Both theoretical and practical
solutions are presented. The Rabin signature is also reconsidered and a deterministic padding
mechanism is proposed.

Keywords: Rabin cryptosystem, Jacobi symbols, Residue Rings, Dedekind sums.

Mathematics Subject Classification (2010): 94A60, 11T71, 14G50

1 Introduction

In 1979, Michael Rabin [11] suggested a variant of RSA with public-key exponent 2, which he
showed to be as secure as factoring. The encryption of a message \( m \in \mathbb{Z}_N^* \) is \( C = m^2 \mod N \),
where \( N = pq \) is a product of two prime numbers, and the decryption is performed by solving the equation
\[
x^2 = C \mod N ,
\]
which has four roots, thus for a complete decryption further information is needed to identify
\( m \) among these roots. More precisely, for a fully automatic (deterministic) decryption we need
at minimum two more bits (computed at the encryption stage) to identify \( m \) without ambiguity.
The advantages of using this exponent 2, with respect to larger exponents, are: i) a smaller com-
putational burden, and ii) solving (1) is equivalent to factor \( N \). The disadvantages are: iii) the
computation, at the encryption stage, of the information required to identify the right root, and
the delivery of this information to the decryption stage, and iv) a vulnerability to chosen-plaintext
attack [4, 9, 14, 15]. Several naive choice methods base the selection of the correct root on the
message semantics, that is, they retain the root that corresponds to a message that looks most
meaningful, or the root that contains a known string of bits. However, all these methods are ei-
ther unusable, for example when the message is a secret key, or are only probabilistic, in any case

∗Politecnico di Torino, Italy  †Università di Trento, Italy  ‡University of Zurich, Switzerland
they affect the equivalence between breaking the Rabin scheme and factoring. Nevertheless, for schemes using pairs of primes congruent 3 modulo 4 (Blum primes), Williams proposed a root identification scheme based on the computation of a Jacobi symbol, using an additional parameter in the public key, and two additional bits in the encrypted message.

The Rabin cryptosystem may also be used to create a signature by exploiting the inverse mapping: in order to sign \( m \) the equation \( x^2 = m \mod N \) is solved and any of the four roots, say \( S \), can be used to form the signed message \((m, S)\). However, if \( x^2 = m \mod N \) has no solution the signature cannot be directly generated; to overcome this issue, a random pad \( U \) is used until \( x^2 = mU \mod N \) is solvable, and the signature is the triple \((m, U, S)\). A verifier compares \( S^2 \) with \( mU \mod N \) and accepts the signature as valid when these two numbers are equal. For an application to electronic signature, an in-depth analysis on advantages/disadvantages can be found in [3].

In the next Section we collect preliminary results concerning the solutions of the equation (1) and the mathematics that we need. In Section 3, we describe in detail the Rabin scheme in the standard setting, where both prime factors of \( N \) are congruent 3 modulo 4, and also propose a new identification rule exploiting the Dedekind sums. In Section 4 we address the identification problem for any pair of primes. In Section 5 we describe a Rabin signature with deterministic padding. Lastly, in Section 6, we draw some conclusions.

## 2 Preliminaries

Let \( N = pq \) be a product of two odd primes \( p \) and \( q \). Using the generalized Euclidean algorithm to compute the greatest common divisor between \( p \) and \( q \), two integer numbers, \( \lambda_1, \lambda_2 \in \mathbb{Z}_p \), such that \( \lambda_1 p + \lambda_2 q = 1 \), are efficiently computed. Thus, setting \( \psi_1 = \lambda_2 q \) and \( \psi_2 = \lambda_1 p \), so that \( \psi_1 + \psi_2 = 1 \), it is easily verified that \( \psi_1 \) and \( \psi_2 \) satisfy the relations

\[
\begin{cases}
\psi_1 \psi_2 = 0 \mod N \\
\psi_1^2 = \psi_1 \mod N \\
\psi_2^2 = \psi_2 \mod N.
\end{cases}
\]

and that \( \psi_1 = 1 \mod p \), \( \psi_1 = 0 \mod q \), and \( \psi_2 = 0 \mod p \), \( \psi_2 = 1 \mod q \). According to the Chinese Reminder Theorem (CRT), using \( \psi_1 \) and \( \psi_2 \), every element \( a \) in \( \mathbb{Z}_N \) can be represented as

\[
a = a_1 \psi_1 + a_2 \psi_2 \mod N,
\]

where \( a_1 \in \mathbb{Z}_p \) and \( a_2 \in \mathbb{Z}_q \) are calculated as \( a_1 = a \mod p \), \( a_2 = a \mod q \).

The four roots \( x_1, x_2, x_3, x_4 \in \mathbb{Z}_N \) of (1), represented as positive numbers, are obtained using the CRT from the roots \( u_1, u_2 \in \mathbb{Z}_p \) and \( v_1, v_2 \in \mathbb{Z}_q \) of the two equations \( u^2 = C \mod p \) and \( v^2 = C \mod q \), respectively. The roots \( u_1 \) and \( u_2 = p - u_1 \) are of different parity, as well as \( v_1 \) and \( v_2 = q - v_1 \). If \( p \) is congruent 3 modulo 4, the root \( u_1 \) can be computed in deterministic polynomial-time as \( \pm C^{\frac{p+1}{4}} \mod p \); the same holds for \( q \). If \( p \) is congruent 1 modulo 4, an equally simple algorithm is not known, however \( u_1 \) can be computed in probabilistic polynomial-time using Tonelli’s algorithm ([2] p.156) once a quadratic non-residue modulo \( p \) is known (this computation is the probabilistic part of the algorithm), or using the (probabilistic) Cantor-Zassenhaus algorithm ([5][13][16] to factor the polynomial \( u^2 - C \mod p \). Using the previous notations, the
four roots of (1) can be written as

\[
\begin{align*}
    x_1 &= u_1 \psi_1 + v_1 \psi_2 \pmod{N} \\
    x_2 &= u_1 \psi_1 + v_2 \psi_2 \pmod{N} \\
    x_3 &= u_2 \psi_1 + v_1 \psi_2 \pmod{N} \\
    x_4 &= u_2 \psi_1 + v_2 \psi_2 \pmod{N}.
\end{align*}
\]

(3)

**Lemma 1** Let \( N = pq \) be a product of two prime numbers. Let \( C \) be a quadratic residue modulo \( N \), the four roots \( x_1, x_2, x_3, x_4 \) of the polynomial \( x^2 - C \) are partitioned into two sets \( X_1 = \{x_1, x_4\} \) and \( X_2 = \{x_2, x_3\} \) such that the roots in the same set have different parity, i.e. \( x_1 = 1 + x_4 \pmod{2} \) and \( x_2 = 1 + x_3 \pmod{2} \). Furthermore, assuming that \( u_1 \) and \( v_1 \) in equation (3) have the same parity, the residues modulo \( p \) and modulo \( q \) of each root in \( X_1 \) have the same parity, while each root in \( X_2 \) has residues of different parity.

**Proof.** Since \( u_1 \) and \( v_1 \) have the same parity by assumption, then also \( u_2 \) and \( v_2 \) have the same parity. The connection between \( x_1 \) and \( x_4 \) is shown by the following chain of equalities

\[
x_4 = u_2 \psi_1 + v_2 \psi_2 = (p - u_1) \psi_1 + (q - v_1) \psi_2 = -x_1 \pmod{N} = N - x_1,
\]

because \( p \psi_1 = 0 \pmod{N} \) and \( q \psi_2 = 0 \pmod{N} \), and \( x_1 \) is less than \( N \) by assumption, thus \(-x_1 \pmod{N} = N - x_1\) is positive and less than \( N \). A similar chain connects \( x_2 \) and \( x_3 \) in \( X_2 \); the conclusion follows because \( N \) is odd and thus \( x_1 \) and \( x_4 \) as well as \( x_2 \) and \( x_3 \) have different parity.

\[\square\]

2.1 The Mapping \( \mathcal{R} : x \to x^2 \)

The mapping \( \mathcal{R} : x \to x^2 \) is four-to-one and partitions \( \mathbb{Z}_N^* \) into disjoint subsets \( u \) of four elements specified by equation (3). Let \( \mathcal{U} \) be the group of the four square roots of unity, that is the roots of \( x^2 = 1 \) consisting of the four-tuple

\[
\mathcal{U} = \{1, a, -a, -1\}.
\]

Obviously, \( \mathcal{U} \) is a group of order 4 and exponent 2. Each subset \( u \), consisting of the four square roots of a given quadratic residue, may be described as a coset \( m \mathcal{U} \) of \( \mathcal{U} \), i.e.

\[
u = m \mathcal{U} = \{m, am, -am, -m\}.
\]

The number of these cosets is \( \phi(N) / 4 \), and they form a group which is isomorphic to a subgroup of \( \mathbb{Z}_N^* \) of order \( \phi(N) / 4 \). Once a coset \( u = \{x_1, x_2, x_3, x_4\} \) is given, a problem is to identify (labelling) the four elements contained in it.

By Lemma I each \( x_i \) is identified by the pair of bits

\[
b_p = (x_i \pmod{p}) \pmod{2}, \quad b_q = (x_i \pmod{q}) \pmod{2}.
\]

In summary, the table

| root | \( b_p \) | \( b_q \) |
|-------|-----------|-----------|
| \( x_1 \) | \( u_1 \) mod 2 | \( v_1 \) mod 2 |
| \( x_2 \) | \( u_1 \) mod 2 | \( v_2 \) mod 2 |
| \( x_3 \) | \( u_2 \) mod 2 | \( v_1 \) mod 2 |
| \( x_4 \) | \( u_2 \) mod 2 | \( v_2 \) mod 2 |
shows that two bits identify (label) the four roots. On the other hand, the expression of these two bits involves the prime factorization of $N$, that is $p$ and $q$, but when the factors of $N$ are not available, it is no longer possible to compute these parity bits, and the problem is to find which parameters can be used and which is the minimum number of required additional bits to be disclosed in order to label a given root among the four ones.

Adopting the convention introduced along with equation (3), a parity bit, namely $b_0 = x \mod 2$ distinguishes $x_1$ from $x_4$, and $x_2$ from $x_3$, therefore it may be one of the parameters to be used in identifying the four roots. It remains to find how to distinguish between roots having the same parity, without knowing the factors of $N$.

### 2.2 Dedekind sums

A Dedekind sum is denoted by $s(h, k)$ and defined as follows [12]. Let $h, k$ be relatively prime and $k \geq 1$, then we set

$$s(h, k) = \sum_{j=1}^{k} \left( \left( \frac{hj}{k} \right) \right) \left( \left( \frac{j}{k} \right) \right) \tag{4}$$

where the symbol $(x)$, defined as

$$(x) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2} & \text{if } x \text{ is not an integer} \\ 0 & \text{if } x \text{ is an integer}, \end{cases} \tag{5}$$

denotes the well-known sawtooth function of period 1. The Dedekind sum satisfies the following properties, see [6, 8, 12] for proofs and details:

1) $h_1 = h_2 \mod k \Rightarrow s(h_1, k) = s(h_2, k)$

2) $s(-h, k) = -s(h, k)$

3) $s(h, k) + s(k, h) = -\frac{1}{4} + \frac{1}{12} \left( \frac{k}{h} + \frac{h}{n} + \frac{n}{h} \right)$, a property known as the reciprocity theorem for the Dedekind sums.

4) $12ks(h, k) = k + 1 - 2 \left( \frac{h}{k} \right) \mod 8$ for $k$ odd, a property connecting Dedekind sums and Jacobi symbols.

The properties 1), 2), and 3) allow us to compute a Dedekind sum by a method that mimics the Euclidean algorithm and has the same efficiency. In the sequel we need the following Lemma:

**Lemma 2** If $k = 1 \mod 4$, then, for any $h$ relatively prime with $k$, the denominator of $s(h, k)$ is odd.

**PROOF.** In the definition of $s(h, k)$ we can stop the summation to $k - 1$ because $\left( \left( \frac{k}{k} \right) \right) = 0$, furthermore, from the identity $((-x)) = -(x)$ it follows $\sum_{j=1}^{k-1} \left( \left( \frac{hj}{k} \right) \right) = 0$ for every integer $h$ [12], then we may write

$$s(h, k) = \sum_{j=1}^{k-1} \left( \frac{j}{k} - \frac{1}{2} \right) \left( \frac{hj}{k} - \left\lfloor \frac{hj}{k} \right\rfloor - \frac{1}{2} \right) = \sum_{j=1}^{k-1} \frac{j}{k} \left( \frac{hj}{k} - \left\lfloor \frac{hj}{k} \right\rfloor - \frac{1}{2} \right),$$

4
since \( \left( \frac{hj}{k} \right) \) is never 0, because \( j < k \) and \( h \) is relatively prime with \( k \) by hypothesis. The last summation can be split into the sum of two summations such that

- the first summation \( \sum_{j=1}^{k-1} \frac{hj}{k} \left( \frac{hj}{k} - \left\lfloor \frac{hj}{k} \right\rfloor \right) \) has the denominator patently odd;

- the second summation is evaluated as \(-\frac{1}{2} \sum_{j=1}^{k-1} \frac{j}{k} = -\frac{k-1}{4}.

In conclusion, the denominator of \( s(h, k) \) is odd because \( s(h, k) \) is a sum of a fraction with odd denominator with \(-\frac{k-1}{4}\), which is an integer number by hypothesis.

\[ \square \]

3 Rabin scheme: primes \( p \equiv q \equiv 3 \mod 4 \)

As said in the introduction, an important issue in using the Rabin scheme is the choice of the right root at the decrypting stage. When \( p \equiv q \equiv 3 \mod 4 \), a solution to the identification problem was proposed by Williams [17] and is reported in the following, slightly modified from [10], along with three different solutions.

3.1 Williams’ scheme

Williams [10][17] proposed an implementation of the Rabin cryptosystem using a parity bit and the Jacobi symbol. The decryption process is based on the observation that, setting \( D = \frac{1}{2} (\frac{(p-1)(q-1)}{4} + 1) \), if \( b = a^2 \mod N \) and \( \left( \frac{a}{N} \right) = 1 \), we have \( a = \pm b^D \), by Lemma 1 in [17].

Public-key: \([N, S]\), where \( S \) is an integer such that \( \left( \frac{S}{N} \right) = -1 \).

Encrypted message \([C, c_1, c_2]\), where

\[ c_1 = \frac{1}{2} \left[ 1 - \left( \frac{m}{N} \right) \right] \quad , \quad \bar{m} = S^{c_1} m \mod N \quad , \quad c_2 = \bar{m} \mod 2 \quad , \quad \text{and} \quad C = \bar{m}^2 \mod N . \]

Decryption stage:

compute \( m' = C^D \mod N \) and \( N - m' \), and choose the number, \( m'' \) say, with the parity specified by \( c_2 \). The original message is recovered as

\[ m = S^{-c_1} m'' . \]

3.2 A second scheme: Variant I

We describe here a variant again exploiting the Jacobi symbol, but in a different way. The detailed process consists of the following steps
Public-key: \([N]\).

**Encrypted message** \([C, b_0, b_1]\), where

\[ C = m^2 \mod N, \quad b_0 = m \mod 2 \quad \text{and} \quad b_1 = \frac{1}{2} \left[ 1 + \left( \frac{m}{N} \right) \right]. \]

**Decryption stage**:
- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by \(b_0\), say \(z_1\) and \(z_2\),
- compute the numbers
  \[ \frac{1}{2} \left[ 1 + \left( \frac{z_1}{N} \right) \right] \quad \frac{1}{2} \left[ 1 + \left( \frac{z_2}{N} \right) \right] \]
  and take the root corresponding to the number equal to \(b_1\).

**Remark.** The two additional bits are sufficient to uniquely identify \(m\) among the four roots because, as previously observed, the roots have the same parity in pairs, and within each of these pairs the roots have opposite Jacobi symbol modulo \(N\). In fact, roots with the same parity are of the form \(a_1\psi_1 + a_2\psi_2\) and \(a_1\psi_1 - a_2\psi_2\) (or \(-a_1\psi_1 + a_2\psi_2\)), whence the conclusion follows from

\[
\left( \frac{a}{N} \right) = \left( \frac{a_1\psi_1 + a_2\psi_2}{pq} \right) \left( \frac{a_1\psi_1 + a_2\psi_2}{p} \right) \left( \frac{a_1\psi_1 + a_2\psi_2}{q} \right) = \left( \frac{a_1}{p} \right) \left( \frac{a_2}{q} \right) \tag{6}
\]

and the fact that \(-1\) is a nonresidue modulo a Blum prime.

### 3.3 A second scheme: Variant II

We recall here a second variant exploiting the Jacobi symbol which, at some extra computational costs and further information in the public key, requires the delivery of no further bit, since the information needed for a deterministic decryption is carried by the encrypted message itself [7].

Let \(\xi\) be an integer such that \(\left( \frac{\xi}{p} \right) = -\left( \frac{\xi}{q} \right) = 1\), for example \(\xi = \alpha^2\psi_1 - \psi_2 \mod N\), with \(\alpha \in \mathbb{Z}_N^\ast\). The detailed process consists of the following steps

**Public-key:** \([N, \xi]\).

**Encrypted message** \([C]\), where \(C\) is obtained as follows

\[ C' = m^2 \mod N, \quad b_0 = m \mod 2, \quad b_1 = \frac{1}{2} \left[ 1 - \left( \frac{m}{N} \right) \right] \quad \text{and} \quad C = C'(-1)^{b_1} \xi^{b_0} \mod N. \]

**Decryption stage**:
- compute \(d_0 = \frac{1}{2} \left[ 1 - \left( \frac{C}{q} \right) \right]\), and set \(C'' = C\xi^{-d_0}\)
- compute \(d_1 = \frac{1}{2} \left[ 1 - \left( \frac{C}{N} \right) \right]\), and \(C' = C''(-1)^{d_1}\)
- compute, as in (3), the four roots of \(C'\), written as positive numbers,
- take the root identified by \(d_0\) and \(d_1\)

**Remark.** Note that the Jacobi symbol \(\left( \frac{C}{N} \right)\) discloses the message parity to an eavesdropper.
3.4 A scheme based on Dedekind sums

Let \( m \in \mathbb{Z}_N \) be the message to be encrypted, with \( N = pq, p \equiv q \equiv 3 \mod 4 \). The detailed process consists of the following steps:

**Public-key:** \([N]\).

**Encrypted message** \([C,b_0,b_1]\), where

\[
C = m^2 \mod N, \quad b_0 = m \mod 2, \quad \text{and} \quad b_1 = s(m,N) \mod 2,
\]

where, due to Lemma\(^2\), the Dedekind sum can be taken modulo 2 since the denominator is odd.

**Decryption stage**:
- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by \( b_0 \), say \( z_1 \) and \( z_2 \),
- compute the numbers

\[
s(z_1,N) \mod 2 \quad \text{and} \quad s(z_2,N) \mod 2,
\]

and take the root corresponding to the number equal to \( b_1 \).

The algorithm works because \( s(z_1,N) \mod 2 \neq s(z_2,N) \mod 2 \) by the following Lemma.

**Lemma 3** If \( k \) is the product of two Blum primes \( p \) and \( q \), \( (x_1,k) = 1 \), and \( x_2 = x_1(\psi_1 - \psi_2) \), then

\[
s(x_1,k) + s(x_2,k) = 1 \mod 2.
\]

**Proof.**

By property 4), that compares the value of the Dedekind sum with the value of the Jacobi symbol, we have

\[
12Ns(x_1,N) = N + 1 - 2\left(\frac{x_1}{N}\right) \mod 8 \quad \text{and} \quad 12Ns(x_2,N) = N + 1 - 2\left(\frac{x_2}{N}\right) \mod 8;
\]

summing the two expressions (member by member) and taking into account that \( N = 1 \mod 4 \) we have

\[
12N(s(x_1,N) + s(x_2,N)) = 2N + 2 - 2\left[\left(\frac{x_1}{N}\right) + \left(\frac{x_2}{N}\right)\right] \mod 8,
\]

since \( 12N = 4 \mod 8, 2N = 2 \mod 8 \). Now, we have previously shown that the sum of the two Jacobi symbols is 0, then, applying Lemma\(^2\) we have

\[
4(s(x_1,N) + s(x_2,N)) = 4 \mod 8 \rightarrow s(x_1,N) + s(x_2,N) = 1 \mod 2,
\]

which concludes the proof.
4 Root identification for any pair of primes

If \( p \) and \( q \) are not both Blum primes, the identification of \( m \) among the four roots of the equation \( x^2 - C \), where \( C = m^2 \mod N \), can be given by the pair \([b_0, b_1]\) where

\[
b_0 = x_i \mod 2 \quad \text{and} \quad b_1 = (x_i \mod p) + (x_i \mod p) \mod 2,
\]
as a consequence of Lemma\(^{[1]}\) The bit \( b_0 \) can be computed at the encryption stage without knowing \( p \) and \( q \), while \( b_1 \) requires, in this definition, the knowledge of \( p \) and \( q \) and cannot be directly computed knowing only \( N \).

In principle, a way to get \( b_1 \) is to publish a pre-computed binary list (or table) that has in position \( i \) the bit \( b_1 \) pertaining to the message \( m = i \). This list does not disclose any useful information on the factorization of \( N \), because, even if we know that the residues modulo \( p \) and modulo \( q \) have the same parity, we do not know which parity, and if these residues have different parity we do not know which parity of which residue. Although the list makes the task theoretically feasible, its size is of exponential complexity with respect to \( N \) and thus practically unrealizable.

While searching for different ways of obtaining \( b_1 \), or some other identifying information, several approaches have been investigated:

- to extend the method of the previous section, based on quadratic residuacity, to any pair of primes, by using power residue symbols of higher order; unfortunately, we will show next that this endangers the security of the private key, that is the factorization of \( N \).

- to define a polynomial function that assumes the values in the above mentioned list at the corresponding integer positions; unfortunately this solution is not practical because this polynomial has a degree roughly equal to \( N \), and is not sparse, then it is more complex than the list.

- to exploit group isomorphisms; this approach will be described with some details because it could be of practical interest, although not being optimal, in that it relies on the hardness of the Discrete Logarithm problem and it may require to communicate more bits than the theoretical lower bound of 2.

4.1 Residuacity

In Section\(^{[3]}\) the Jacobi symbol, i.e. the quadratic residuacity, was used to distinguish the roots in the Rabin cryptosystem, when \( p = q = 3 \mod 4 \). For primes congruent 1 modulo 4, Legendre symbols cannot distinguish numbers of opposite sign, therefore quadratic residuacity is not sufficient anymore to identify the roots. Higher power residue symbols could in principle do the desired job, but unfortunately their use unveils the factorization of \( N \), as the following argument shows.

Let \( 2^k \) and \( 2^h \) be the even exponents of \( \mathbb{Z}_p \) and \( \mathbb{Z}_q \), respectively, that is \( 2^k \) strictly divides \( (p - 1) \) and \( 2^h \) strictly divides \( q - 1 \), and assume that \( k \geq h \). Then the rational power residue symbols \( x^{\frac{2^i}{2^k}} \mod p \) and \( x^{\frac{2^i}{2^h}} \mod q \) can distinguish, respectively, between \( u_1 \) and \( u_2 \) and between \( v_1 \) and \( v_2 \), therefore the function \( x^{\frac{2^i(N)}{2^k}} \mod N \) would identify \( m \) among the \( 2^{k+h} \) \( 2^k \)-th roots of unity in \( \mathbb{Z}_N^* \). The idea would be to make these roots publicly available and label them, so that who sends the message can tell which of them corresponds to the message actually sent. There are two
problems: first the exponent $\frac{\varphi(N)}{2k}$ should also be available, but necessarily in some masked form in order to hide the factors of $N$, but most importantly among the public $2^k$-th roots of unity we would find the square roots, and in particular $K \equiv \psi_1 - \psi_2$. But the greatest common divisor of $K + 1 = 2\psi_1$ and $N$ yields $q$, so $N$ is factored.

4.2 Polynomial function

We may construct an identifying polynomial as an interpolation polynomial choosing a prime $P$ greater than $N$. Actually the polynomial

$$L(x) = \sum_{j=1}^{N-1} (1 - (x - j)^{P-1}) \left((j \mod p) + (j \mod q) \mod 2\right)$$

assumes the value 1 in $0 < m < N$, if the residues of $m$ modulo $p$ and modulo $q$ have different parity, and assumes the value 0 elsewhere. Unfortunately, as said, the complexity of $L(x)$ is prohibitive and makes this function practically useless.

4.3 Group isomorphisms

We have previously shown that in the Rabin scheme two more bits are sufficient for the decryption, and can be easily computed, when Blum primes are used. When non-Blum primes are used, instead, every known function that computes the two identifying bits is prohibitively complex. In this section, we describe a practical method that can have an acceptable complexity, although it requires a one-way function that might be weaker than factoring.

A possible solution is to use a function $\vartheta$ defined from $\mathbb{Z}_N$ into a group $\mathbb{G}$ of the same order, and define a function $\vartheta_1$ such that $\vartheta_1(x_1) = \vartheta(x_2)$. The public key consists of the two functions $\vartheta$ and $\vartheta_1$. At the encryption stage both are evaluated at the same argument, the message $m$, and the minimum information necessary to distinguish their values is delivered together with the encrypted message. The decryption operations are obvious. The true limitation of this scheme is that $\vartheta$ must be a one-way function, otherwise two square roots that allow us to factor $N$ can be recovered as in the residuacity subsection.

Following this approach, we propose the following solution, based on the hardness of computing discrete logarithms.

Given $N$, let $P = \mu N + 1$ be a prime (the smallest prime), that certainly exists by Dirichlet’s theorem, that is congruent 1 modulo $N$. Let $g$ be a primitive element generating the multiplicative group $\mathbb{Z}_P^\times$.

Define $g_1 = g^\mu$ and $g_2 = g^{\mu(\psi_1 - \psi_2)}$, and let $m$ denote the message, as usual.

**Public key**: $[N, g_1, g_2]$.

**Encryption stage**: $[C, b_0, d_1, d_2, p_1, p_2]$, where $C = m^2 \mod N$, $b_0 = m \mod 2$, $p_1$ is a position in the binary expansion of $g_1^m \mod P$ whose bit $d_1$ is different from the bit in the corresponding position of the binary expansion of $g_2^m \mod P$ and $p_2$ is a position in the binary expansion of $g_1^m \mod P$ whose bit $d_2$ is different from the bit in the corresponding position of the binary expansion of $g_2^{-m} \mod P$. 


Decryption stage:
- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by \( b_0 \), say \( z_1 \) and \( z_2 \),
- compute \( A = g_{z_1}^1 \mod P \) and \( B = g_{z_2}^2 \mod P \) - between \( z_1 \) or \( z_2 \) the root is selected that has the correct bits \( d_1 \) and \( d_2 \) in both the given position \( p_1 \) and \( p_2 \) of the binary expansion of \( A \) or \( B \).

The algorithm is justified by the following Lemma.

Lemma 4 The power \( g_0 = g^a \) generates a group of order \( N \) in \( \mathbb{Z}_p^* \), thus the correspondence \( x \leftrightarrow g_0^x \) establishes an isomorphism between a multiplicative subgroup of \( \mathbb{Z}_p^* \) and the additive group of \( \mathbb{Z}_N \). The four roots of \( x^2 = C \mod N, C = m^2 \mod N \) are in a one-to-one correspondence with the four powers \( g_0^a \mod P, g_0^m \mod P, g_0^{m(\psi_1 - \psi_2)} \mod P \) and \( g_0^{-m(\psi_1 - \psi_2)} \mod P \).

Proof. The first part is due to the choice of \( P \): the group generated by \( g_0 \) has order \( N \), thus, the isomorphism follows immediately. The second part is a consequence of Section 2.1.

The price to pay is the costly arithmetic in \( GF(P) \), and the equivalence of the security of the Rabin cryptosystem with the hardness of factoring is now conditioned on the complexity of computing the discrete logarithm in \( \mathbb{Z}_p \).

5 The Rabin signature

In the introduction, we anticipated that a Rabin signature of a message \( m \) may consists of a pair \([n, S]\), however, if \( x^2 = m \mod N \) has no solution, this signature cannot be directly generated. To overcome this obstruction, a random pad \( U \) was proposed [10], and attempts are repeated until \( x^2 = mU \mod N \) is solvable, and the signature is the triple \((m, U, S)\), [10]. A verifier compares \( mU \mod N \) with \( S^2 \) and accepts the signature as valid when these two numbers are equal.

Aim of this section is to present a modified version of this scheme where \( U \) is computed deterministically.

Now, the quadratic equation \( x^2 = m \mod N \) is solvable if and only if \( m \) is a quadratic residue modulo \( N \), that is \( m \) is a quadratic residue modulo \( p \) and modulo \( q \). When \( m \) is not a quadratic residue, we show below how to exploit the Jacobi symbol to compute a suitable pad and obtain quadratic residues modulo \( p \) and \( q \). Let

\[
f_1 = \frac{m_1}{2} \left[ 1 - \left( \frac{m_1}{p} \right) \right] + \frac{1}{2} \left[ 1 + \left( \frac{m_1}{p} \right) \right], \quad f_2 = \frac{m_2}{2} \left[ 1 - \left( \frac{m_2}{q} \right) \right] + \frac{1}{2} \left[ 1 + \left( \frac{m_2}{q} \right) \right].
\]

Writing \( m = m_1\psi_1 + m_2\psi_2 \), the equation

\[
x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = m_1f_1\psi_1 + m_2f_2\psi_2
\]

is always solvable modulo \( N \) because \( m_1f_1 \) and \( m_2f_2 \) are clearly quadratic residues modulo \( p \) and modulo \( q \), respectively, since

\[
\left( \frac{m_1}{p} \right) = \left( \frac{f_1}{p} \right), \quad \left( \frac{m_2}{q} \right) = \left( \frac{f_2}{q} \right),
\]

so that

\[
\left( \frac{m_1f_1}{p} \right) = \left( \frac{m_1}{p} \right) \left( \frac{f_1}{p} \right) = 1, \quad \left( \frac{m_2f_2}{q} \right) = \left( \frac{m_2}{q} \right) \left( \frac{f_2}{q} \right) = 1.
\]
Note that if \( p \) and \( q \) are Blum primes, it is possible to choose \( f_1 = \left( \frac{m_1}{p} \right) \) and \( f_2 = \left( \frac{m_2}{q} \right) \). Thus we can describe the following procedure:

**Public-key:** \( N \)

**Signed message:** \([U, m, S]\), where \( U = R^2 [f_1 \psi_1 + f_2 \psi_2] \mod N \) is the padding factor, with \( R \) a random number, and \( S \) is any solution of the equation \( x^2 = mU \mod N \)

**Verification:** compute \( mU \mod N \) and \( S^2 \mod N \); the signature is valid if and only if these two numbers are equal.

This signature scheme has several interesting features:

1. the signature is possible using every pair of primes, therefore, it could be used with the modulo of any RSA public key, for example;
2. different signatures of the same document are different;
3. the verification needs only two multiplications, therefore it is fast enough to be used in authentication protocols.

## 6 Conclusions and Remarks

In principle, the Rabin scheme is very efficient because only one square is required for encryption, furthermore it is provable as secure as factoring. Nevertheless, it is well known \([4, 15]\) that it presents some drawbacks, mainly due to the four-to-one mapping, that may discourage its use to conceal the content of a message, namely:

- the root identification requires the delivery of additional information, which may not be easily computed, especially when not both primes are Blum primes;
- many proposed root identification methods, based on the message semantics, have a probabilistic character and cannot be used in some circumstances;
- the delivery of two bits together with the encrypted message exposes the process to active attacks by maliciously modifying these bits. For example, suppose an attacker \( A \) sends an encrypted message to \( B \) asking that the decrypted message be delivered to a third party \( C \) (a friend of \( A \)). If in the encrypted message the bit that identifies the root among the two roots of same parity had been deliberately changed, \( A \) can get a root from \( C \) that combined with the original message allows to factor the Rabin public-key. Even Variant II is not immune to those kind of active attacks.

In conclusion, the Rabin scheme may come with some hindrance when used to conceal a message, while it seems effective when applied to generate electronic signature or as a hash function. However, the previous observations do not exclude the practical use of the Rabin scheme (as it is actually profitably done in some standardized protocols), when other properties like integrity and authenticity are to be taken care of, along with message secrecy, in a public-encryption protocol.
7 Acknowledgments

This work has been partially done while the first author was Visiting Professor with the University of Trento, funded by CIRM, and he would like to thank the Department of Mathematics for the friendly and fruitful atmosphere offered. The third author has been supported by the Swiss National Science Foundation under grant No. 132256.

References

[1] T.M. Apostol, Introduction to Analytic Number Theory, Springer, New York, 1976.
[2] E. Bach, J. Shallit, Algorithmic Number Theory, MIT, Cambridge Mass., 1996.
[3] D. J. Bernstein, Proving tight security for Rabin-Williams signatures, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 70–87.
[4] J. A. Buchmann, Introduction to Cryptography, Springer, New York, 1999.
[5] D.G. Cantor, H. Zassenhaus, A new Algorithm for Factoring Polynomials over Finite Fields, Math. Comp., Vol. 36, N. 154, April 1981, pp.587-592.
[6] R. Dedekind, Schreiben an Herrn Borchardt, J. Reine Angew. Math., 83, 1877, pp.265-292.
[7] D.M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, G. Segev, More Constructions of Lossy and Correlation-Secure Trapdoor Functions, PKC 2010, Springer LNCS 6056 (2010), pp.279-295.
[8] E. Grosswald, Topics from the Theory of Numbers, Birkhäuser, Basel, 2009.
[9] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.
[10] J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Security, Springer, New York, 2003.
[11] M. Rabin, Digitalized signature as intractable as factorization, Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1978.
[12] H. Rademacher, E. Grosswald, Dedekind Sums, MAA, New York, 1972.
[13] M. Elia, D. Schipani, Improvements on the Cantor-Zassenhaus Factorization Algorithm, www.arxiv.org, 2011.
[14] B. Schneier, Applied cryptography, Wiley, 1996.
[15] J. Hoffstein, J. Pipher, J.H. Silverman, An introduction to mathematical cryptography, Springer, New York, 2008.
[16] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge Univ. Press, 1999.
[17] H.C. Williams, A modification of the RSA public-key encryption procedure, IEEE Trans. on Inform. Th., IT-26(6), November 1980, pp.726-729.