A multi-factor RSA-like scheme with fast decryption based on Rédei rational functions over the Pell hyperbola

Emanuele Bellini, Nadir Murru

Abstract

We propose a generalization of an RSA-like scheme based on Rédei rational functions over the Pell hyperbola. Instead of a modulus which is a product of two primes, we define the scheme on a multi-factor modulus, i.e. on a product of more than two primes. This results in a scheme with a decryption which is quadratically faster, in the number of primes factoring the modulus, than the original RSA, while preserving a better security. The scheme reaches its best efficiency advantage over RSA for high security levels, since in these cases the modulus can contain more primes. Compared to the analog schemes based on elliptic curves, as the KMOV cryptosystem, the proposed scheme is more efficient. Furthermore a variation of the scheme with larger ciphertext size does not suffer of impossible group operation attacks, as it happens for schemes based on elliptic curves.

Keywords: cryptography, Pell conic, Rédei rational functions, RSA

1 Introduction

RSA is the most widespread asymmetric encryption scheme. Its security is based on the fact that the trapdoor function $\tau_{N,e}(x) = x^e \mod N$, with $N = pq$ product of two large prime integers, and e an invertible element in $\mathbb{Z}_{\phi(N)}$ ($\phi(N)$ being the Euler totient function), cannot be inverted by a polynomial-time in N algorithm without knowing either the integers p, q, $\phi(N)$ or the inverse d of e modulo $\phi(N)$. Thus the pair (N, e), called the public key, is known to everyone, while the triple (p, q, d), called the secret key, is only known to the receiver of an encrypted message.
Both encryption and decryption are performed through an exponentiation modulo N. Precisely, the ciphertext C is obtained as $C = M^e \pmod N$, and the original message M is obtained with the exponentiation $M = C^d \pmod N$. While usually the encryption exponent is chosen to be small, the decryption exponent is about the size of N, implying much slower performances during decryption with respect to encryption.

Through the years many proposal have been presented trying to speed up the decryption process. In this work we present the fastest, to the authors knowledge, of such decryption algorithms whose security is based on the factorization problem.
The presented scheme exploits different properties of Rédei rational functions, which are classical functions in number theory. The proposed decryption algorithm is quadratically, on the number of primes composing the modulus N, faster than RSA.

The work is divided as follows. In Section **??** an overview of the main schemes based on the factorization problem which successfully improved RSA decryption step is presented. In Section **??** the main theoretical results underlying our scheme are described. Section **??** is devoted to the presentation of the cryptographic scheme, and in Section **??** and **??** its security and efficiency are discussed, respectively. Section **??** concludes the work.

2 Related work

In this section we briefly overview the main cryptographic schemes based on the factorization problem that have been introduced in order to improve RSA decryption step.
Usually, the general technique to speed up the RSA decryption step $C = M^e \pmod N$ is to compute the exponentiation modulo each factor of N and then obtain N using the Chinese Remainder Theorem.

2.1 Multifactor RSA

There exists variants of RSA scheme which exploit a modulus with more than 2 factors to achieve a faster decryption algorithm. This variants are sometimes called Multifactor RSA ([**?**]), or Multiprime RSA ([**?**], [**?**]). The first proposal exploiting a modulus of the form $N = p_1p_2p_3$ has been patented by Compaq ([**?**], [**?**]) in 1997. About at the same time Takagi [**?**] proposed an even faster solution using the modulus $N = p^r q$, for which the exponentiation modulo p^r is computed using the Hensel lifting method [**?**, p.137]. Later, this solution has been generalized to the modulus $N = p^r q^s$ [**?**].
According to [**?**] the appropriate number of primes to be chosen in order to resist state-of-the-art factorization algorithms depends from the modulus size, and, precisely, it can be: up to 3 primes for 1024, 1536, 2048, 2560, 3072, and 3584 bit modulus, up to 4 for 4096, and up to 5 for 8192.

2.2 RSA-like schemes

Another solution which allows to obtain even faster decryption is to use RSA-like schemes based on isomorphism as [**?**], [**?**], [**?**], [**?**]. As an additional property, these schemes owns better security properties with respect to RSA, avoiding small exponent attacks to either d ([**?**]) or e ([**?**], [**?**]), and vulnerabilities which appear when switching from one-to-one communication scenario to broadcast scenario (e.g., see [**?**]).
The aforementioned schemes are based on isomorphism between two groups, one of which is the set of points over a curve, usually a cubic or a conic. A complete overview on RSA-like schemes based on conics can be found in [**?**]. In general, schemes based on cubic curves have a computationally more expensive addition operation compared to schemes based on conic equations.

2.3 Generalizing RSA-like scheme with multifactor modulus

As done when generalizing from RSA to Multiprime RSA, in [**?**] a generalization of [**?**], [**?**] has been proposed, thus generalizing a RSA-like scheme based on elliptic curves and a modulus $N = pq$ to a similar scheme based on the generic modulus $N = p^r q^s$.
In this paper we present a similar generalization of the scheme [**?**], which is based on the Pell's equation, to the modulus $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ for $r > 2$, obtaining the fastest decryption of all schemes discussed in this section.

3 Product of points over the Pell hyperbola

In [**?**], we introduced a novel RSA–like scheme based on an isomorphism between certain conics (whose the Pell hyperbola is a special case) and a set of parameters equipped with a non–standard product. In Section **??**, we generalize this scheme considering a prime power modulus $N = p_1^{e_1} \cdots p_r^{e_r}$. In this section, we recall some definitions and properties given in [**?**] in order to improve the readability of the paper. Then, we study properties of the involved products and sets in $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_N$.

3.1 A group structure over the Pell hyperbola over a field

Let $\mathbb{K}$ be a field and $x^2 - D$ an irreducible polynomial over $\mathbb{K}[x]$. Considering the quotient field $\mathbb{A}[x] = \mathbb{K}[x]/(x^2 - D)$, the induced product over $\mathbb{A}[x]$ is

$$(p + qx)(r + sx) = (pr + qsD) + (qr + ps)x.$$

The group of unitary elements of $\mathbb{A}^*[x] = \mathbb{A}[x] - \{0_{\mathbb{A}[x]}\}$ [1] is $\{p + qx \in \mathbb{A}^*[x] : p^2 - Dq^2 = 1\}$. Thus, we can introduce the commutative group

[1] The element $0_{\mathbb{A}[x]}$ is the zero polynomial.

$(\mathcal{H}_{D,\mathbb{K}}, \otimes)$, where

$$\mathcal{H}_{D,\mathbb{K}} = \{(x, y) \in \mathbb{K} \times \mathbb{K} : x^2 - Dy^2 = 1\}$$

and

$$(x, y) \otimes (w, z) = (xw + yzD, yw + xz), \quad \forall (x, y),\ (w, z) \in \mathcal{H}_{D,\mathbb{K}}. \tag{1}$$

It is worth noting that $(1, 0)$ is the identity and the inverse of an element (x, y) is $(x, -y)$.

Remark 1. When $\mathbb{K} = \mathbb{R}$, the conic $\mathcal{H}_{D,\mathbb{K}}$, for D a non–square integer, is called the Pell hyperbola since it contains all the solutions of the Pell equation and $\otimes$ is the classical Brahamagupta product, see, e.g., [**?**].

3.2 A parametrization of the Pell hyperbola

From now on let $\mathbb{A} = \mathbb{A}[x]$.
Starting from $\mathbb{A}^*$, we can derive a parametrization for $\mathcal{H}_{D,\mathbb{K}}$. In particular, let us consider the group $\mathbb{A}^*/\mathbb{K}^*$, whose elements are the equivalence classes of $\mathbb{A}^*$ and can be written as

$$\{[a + x] : a \in \mathbb{K}\} \cup \{[1_{\mathbb{K}^*}]\}.$$

The induced product over $\mathbb{A}^*/\mathbb{K}^*$ is given by

$$[a + x][b + x] = [ab + ax + bx + x^2] = [D + ab + (a + b)x]$$

and, if $a + b \neq 0$, we have

$$[a + x][b + x] = [\frac{D + ab}{a + b} + x]$$

else

$$[a + x][b + x] = [D + ab] = [1_{\mathbb{K}^*}].$$

This construction allows us to define the set of parameters $\mathcal{P}_{\mathbb{K}} = \mathbb{K} \cup \{\alpha\}$, with α not in $\mathbb{K}$, equipped with the following product:

$$\begin{cases} a \odot b = \dfrac{D + ab}{a + b}, & a + b \neq 0 \\ a \odot b = \alpha, & a + b = 0 \end{cases} . \tag{2}$$

We have that $(\mathcal{P}_{\mathbb{K}}, \odot)$ is a commutative group with identity α and the inverse of an element a is the element b such that $a + b = 0$. Now, consider the following parametrization for the conic $\mathcal{H}_{D,\mathbb{K}}$:

$$y = \frac{1}{m}(x+1)\,.$$

It can be proved that the following isomorphism between $(\mathcal{H}_{D,\mathbb{K}}, \otimes)$ and $(\mathcal{P}_{\mathbb{K}}, \odot)$ holds:

$$\Phi_D : \begin{cases} \mathcal{H}_{D,\mathbb{K}} & \to \mathcal{P}_{\mathbb{K}} \\ (x,y) & \mapsto \dfrac{1+x}{y} \quad \forall (x,y) \in \mathcal{H}_{D,\mathbb{K}}, \quad y \neq 0 \\ (1,0) & \mapsto \alpha \\ (-1,0) & \mapsto 0\ , \end{cases} \tag{3}$$

and

$$\Phi_D^{-1} : \begin{cases} \mathcal{P}_{\mathbb{K}} & \to \mathcal{H}_{D,\mathbb{K}} \\ m & \mapsto \left(\dfrac{m^2+D}{m^2-D}\,, \dfrac{2m}{m^2-D} \right) \quad \forall m \in \mathbb{K}\,, \\ \alpha & \mapsto (1,0)\ , \end{cases} \tag{4}$$

see [**?**] and [**?**].

Proposition 1. *When $\mathbb{K} = \mathbb{Z}_p$, p prime, $(\mathcal{P}_{\mathbb{K}}, \odot)$ and $(\mathcal{H}_{D,\mathbb{K}}, \otimes)$ are cyclic groups of order $p+1$ and*

$$m^{\odot(p+2)} = m \pmod p, \quad \forall m \in \mathcal{P}_{\mathbb{Z}_p}$$

or, equivalently

$$(x,y)^{\otimes(p+2)} = (x,y) \pmod p, \quad \forall (x,y) \in \mathcal{H}_{D,\mathbb{Z}_p},$$

*where powers are performed using products $\odot$ and $\otimes$, respectively. See [**?**].*

The powers in $\mathcal{P}_{\mathbb{K}}$ can be efficiently computed by means of the Rédei rational functions [**?**], which are classical functions in number theory. They are defined by considering the development of

$$(z + \sqrt{D})^n = A_n(D,z) + B_n(D,z)\sqrt{D},$$

for z integer and D non–square positive integer. The polynomials $A_n(D,z)$ and $B_n(D,z)$ defined by the previous expansion are called Rédei polynomials and can be evaluated by

$$M^n = \begin{pmatrix} A_n(D,z) & DB_n(D,z) \\ B_n(D,z) & A_n(D,z) \end{pmatrix}$$

where

$$M = \begin{pmatrix} z & D \\ 1 & z \end{pmatrix}.$$

From this property, it follows that the Rédei polynomials are linear recurrent sequences with characteristic polynomial $t^2 - 2zt + (z^2 - D)$. The Rédei rational functions are defined by

$$Q_n(D, z) = \frac{A_n(D, z)}{B_n(D, z)}, \quad \forall n \geq 1.$$

Proposition 2. *Let $m^{\odot n}$ be the n–th power of $m \in \mathcal{P}_{\mathbb{K}}$ with respect to $\odot$, then*

$$m^{\odot n} = Q_n(D, m).$$

*See [**?**].*

Remark 2. The Rédei rational functions can be evaluated by means of an algorithm of complexity $O(\log_2(n))$ with respect to addition, subtraction and multiplication over rings [**?**].

3.3 Properties of the Pell hyperbola over a ring

In this section, we study the case $\mathbb{K} = \mathbb{Z}_{p^r}$ that we will exploit in the next section for the construction of a cryptographic scheme. In what follows, we will omit from $\mathcal{H}_{D,\mathbb{K}}$ the dependence on D when it will be clear from the context.

First, we need to determine the order of $\mathcal{H}_{\mathbb{Z}_{p^r}}$ in order to have a result similar to Proposition **??** also in this situation.

Theorem 1. *The order of the cyclic group $\mathcal{H}_{\mathbb{Z}_{p^r}}$ is $p^{r-1}(p+1)$, i.e., the Pell equation $x^2 - Dy^2 = 1$ has $p^{r-1}(p+1)$ solutions in $\mathbb{Z}_{p^r}$ for $D \in \mathbb{Z}_{p^r}^*$ quadratic non–residue in $\mathbb{Z}_p$.*

Proof. Since, by Proposition **??**, the Pell equation in $\mathbb{Z}_p$ has $p+1$ solutions, then we need to prove the following

1. any solution of the Pell equation in $\mathbb{Z}_p$, generates p^{r-1} solutions of the same equation in $\mathbb{Z}_{p^r}$;
2. all the solutions of the Pell equation in $\mathbb{Z}_{p^r}$ are generated as in the previous step.

(**??**) Let (x_0, y_0) be a solution of $x^2 - Dy^2 \equiv 1 \pmod{p}$. We want to prove that for any integer $0 \leq k < p^{r-1}$, there exists one and only one integer h such that $(x_0 + kp, y_0 + hp)$ is solution of $x^2 - Dy^2 \equiv 1 \pmod{p^r}$. Indeed, we have

$$(x_0 + kp)^2 - D(y_0 + hp)^2 = 1 + vp + 2x_0kp + k^2p^2 - 2Dy_0hp - Dh^2p^2,$$

since $x_0^2 - Dy_0^2 = 1 + vp$ for a certain integer v. Thus, we have that $(x_0 + kp, y_0 + hp)$ is solution of $x^2 - Dy^2 \equiv 1 \pmod{p^r}$ if and only if

$$Dph^2 + 2Dy_0h - v - 2x_0k - k^2p \equiv 0 \pmod{p^{r-1}}.$$

Hence, we have to prove that there is one and only one integer h that satisfies the above identity. The above equation can be solved in h by completing the square and reduced to

$$(2Dph + 2Dy_0)^2 \equiv s \pmod{p^{r-1}}, \tag{5}$$

where $s = (2Dy_0)^2 + 4(v + 2x_0k + k^2p)Dp$. Let us prove that s is a quadratic residue in $\mathbb{Z}_{p^{r-1}}$. Indeed,

$$s = 4D((x_0 + kp)^2 - 1)$$

and surely the Jacobi symbol $\left(\frac{s}{p^{r-1}}\right) = \left(\frac{s}{p}\right)^{r-1} = 1$ if r is odd.

If r is even we have that

$$\left(\frac{s}{p^{r-1}}\right) = \left(\frac{4}{p^{r-1}}\right)\left(\frac{D}{p^{r-1}}\right)\left(\frac{(x_0 + kp)^2 - 1}{p^{r-1}}\right) = 1$$

since $\left(\frac{4}{p^{r-1}}\right) = 1$, $\left(\frac{D}{p^{r-1}}\right) = \left(\frac{D}{p}\right)^{r-1} = -1$ by hypothesis on D, $\left(\frac{(x_0 + kp)^2 - 1}{p^{r-1}}\right) = -1$, since $(x_0 + kp)^2 - 1 \equiv Dy_0^2 \pmod{p}$.

Now, let $\pm t$ be the square roots of s. It is easy to note that

$$t \equiv 2Dy_0 \pmod{p}, \quad -t \equiv -2Dy_0 \pmod{p}$$

or

$$-t \equiv 2Dy_0 \pmod{p}, \quad t \equiv -2Dy_0 \pmod{p}.$$

Let us call $\bar{t}$ the only one between t and $-t$ that is equal to $2Dy_0$ in $\mathbb{Z}_p$. Hence, Equation (**??**) is equivalent to the linear equation

$$ph \equiv (\bar{t} - 2Dy_0)(2D)^{-1} \pmod{p^{r-1}},$$

which has one and only one solution, since $\bar{t} - 2Dy_0 \equiv 0 \pmod{p}$. Note that, if $\bar{t}$ is not equal to $2Dy_0$ in $\mathbb{Z}_p$ the above equation has no solutions. Thus, we have proved that any solution of the Pell equation in $\mathbb{Z}_p$ generates p^{r-1} solutions of the Pell equation in $\mathbb{Z}_{p^r}$.

(**??**) Now, we prove that all the solutions of the Pell equation in $\mathbb{Z}_{p^r}$ are generated as in step **??**.
Let $(\bar{x}, \bar{y})$ be a solution of $x^2 - Dy^2 \equiv 1 \pmod{p^r}$, i.e., $\bar{x}^2 - D\bar{y}^2 = 1 + wp^r$, for a certain integer w. Then $x_0 = \bar{x} - kp$ and $y_0 = \bar{y} - hp$, for h, k integers, are solutions of $x^2 - Dy^2 \equiv 1 \pmod{p}$. Indeed,

$$(\bar{x} - kp)^2 - D(\bar{y} - hp)^2 = 1 + wp^r - 2\bar{x}kp + k^2p^2 + 2D\bar{y}hp - Dh^2p^2\,.$$

□

As a consequence of the previous theorem, an analogous of the Euler theorem holds for the product $\otimes$.

Theorem 2. *Let p, q be prime numbers and $N = p^r q^s$, then for all $(x, y) \in \mathcal{H}_{\mathbb{Z}_N}$ we have*

$$(x, y)^{\otimes p^{r-1}(p+1)q^{s-1}(s+1)} \equiv (1, 0) \pmod{N}$$

for $D \in \mathbb{Z}_N^*$ quadratic non–residue in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

Proof. By Theorem **??**, we know that

$$(x, y)^{\otimes p^{r-1}(p+1)} \equiv (1, 0) \pmod{p^r}$$

and

$$(x, y)^{\otimes q^{s-1}(s+1)} \equiv (1, 0) \pmod{q^s}.$$

Thus, said $(a, b) = (x, y)^{\otimes p^{r-1}(p+1)q^{s-1}(s+1)}$, we have

$$(a, b) \equiv (1, 0) \pmod{p^r},$$

i.e., $a = 1 + kp^r$ and $b = hp^r$ for some integers h, k. On the other hand, we have

$$(a, b) \equiv (1, 0) \pmod{q^s} \Leftrightarrow (1 + kp^r, hp^r) \equiv (1, 0) \pmod{q^s}.$$

We can observe that $1 + kp^r \equiv 1 \pmod{q^s}$ if and only if $k = k'q^s$ for a certain integer k'. Similarly, it must be $h = h'q^s$, for an integer h'. Hence, we have that $(a, b) = (1 + k'p^r q^s, h'p^r q^s) \equiv (1, 0) \pmod{N}$. □

Corollary 1. *Let $p_1, ..., p_r$ be primes and $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, then for all $(x, y) \in \mathcal{H}_{\mathbb{Z}_N}$ we have*

$$(x, y)^{\otimes \Psi(N)} = (1, 0) \pmod{N},$$

where

$$\Psi(N) = p_1^{e_1-1}(p_1 + 1) \cdot \ldots \cdot p_r^{e_r-1}(p_r + 1),$$

for $D \in \mathbb{Z}_N^*$ quadratic non–residue in $\mathbb{Z}_{p_i}$, for $i = 1, ..., r$.

Now, we can observe that when we work on $\mathbb{Z}_N$, the map Φ_D is not an isomorphism. Indeed, the orders of $\mathcal{H}_{D,\mathbb{Z}_N}$ and $\mathcal{P}_{\mathbb{Z}_N}$ do not coincide. However, it is still a morphism and we also have $|\mathbb{Z}_N^*| = |\mathcal{H}_{\mathbb{Z}_N}^*|$, because of the following proposition.

Proposition 3. *With the above notation, we have that*

1. $\forall (x_1, y_1), (x_2, y_2) \in \mathcal{H}_{\mathbb{Z}_N}^*$, $\Phi_D(x_1, y_1) = \Phi_D(x_2, y_2) \Leftrightarrow (x_1, y_1) = (x_2, y_2)$;

2. $\forall m_1, m_2 \in \mathbb{Z}_N^*$, $\Phi_D^{-1}(m_1) = \Phi_D^{-1}(m_2) \Leftrightarrow m_1 = m_2$;

3. $\forall m \in \mathbb{Z}_N^*$, *we have* $\Phi^{-1}(m) \in \mathcal{H}_{\mathbb{Z}_N}^*$ *and* $\forall (x, y) \in \mathcal{H}_{\mathbb{Z}_N}^*$, *we have* $\Phi_D(x, y) \in \mathbb{Z}_N^*$.

See [?].

As a consequence, we have an analogous of the Euler theorem also for the product $\odot$, i.e., for all $m \in \mathbb{Z}_N^*$ the following holds

$$m^{\odot \Psi(N)} = \alpha \pmod{N},$$

where $\odot$ is the special product in $\mathcal{P}_{\mathbb{Z}_N}$ defined in Equation **??**.

4 The cryptographic scheme

In this section, we describe our public–key cryptosystem based on the properties studied in the previous section.

4.1 Key generation

The key generation is performed by the following steps:

- choose r prime numbers $p_1, \ldots, p_r$, r odd integers $e_1, \ldots, e_r$ and compute $N = \prod_{i=1}^{r} p_i^{e_i}$;
- choose an integer e such that $\gcd(e, \operatorname{lcm} \prod_{i=1}^{r} p_i^{e_i - 1}(p_i + 1)) = 1$;
- evaluate $d = e^{-1} \pmod{\operatorname{lcm} \prod_{i=1}^{r} p_i^{e_i - 1}(p_i + 1)}$.

The public or encryption key is given by (N, e) and the secret or decryption key is given by $(p_1, \ldots, p_r, d)$.

4.2 Encryption

We can encrypt pair of messages $(M_x, M_y) \in \mathbb{Z}_N^* \times \mathbb{Z}_N^*$, such that $\left(\frac{M_x^2 - 1}{N}\right) = -1$. This condition will ensure that we can perform all the operations. The encryption of the messages is performed by the following steps:

- compute $D = \dfrac{M_x^2 - 1}{M_y^2} \pmod{N}$, so that $(M_x, M_y) \in \mathcal{H}_{D, \mathbb{Z}_N}^*$;
- compute $M = \Phi(M_x, M_y) = \dfrac{M_x + 1}{M_y} \pmod{N}$;
- compute the ciphertext $C = M^{\odot e} \pmod{N} = Q_e(D, M) \pmod{N}$

Notice that not only C, but the pair (C, D) must be sent through the insecure channel.

4.3 Decryption

The decryption is performed by the following steps:

- compute $C^{\odot d} \pmod N = Q_d(D, C) \pmod N = M$;
- compute $\Phi^{-1}(M) = \left(\frac{M^2 + D}{M^2 - D}, \frac{2M}{M^2 - D}\right) \pmod N$ for retrieving the messages (M_x, M_y).

5 Security of the encryption scheme

The proposed scheme can be attacked by solving one of the following problems:

1. factorizing the modulus $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$;
2. computing $\Psi(N) = p_1^{e_1 - 1}(p_1 + 1) \cdot \ldots \cdot p_r^{e_r - 1}(p_r + 1)$, or finding the number of solutions of the equation $x^2 - Dy^2 \equiv 1 \mod N$, i.e. the curve order, which divides $\Psi(N)$;
3. computing Discrete Logarithm problem either in $(\mathcal{H}^*_{\mathbb{Z}_N}, \otimes)$ or in $(\mathcal{P}^*_{\mathbb{Z}_N}, \odot)$;
4. finding the unknown d in the equation $ed \equiv 1 \mod \Psi(N)$;
5. finding an impossible group operation in $\mathcal{P}_{\mathbb{Z}_N}$;
6. computing M_x, M_y from D.

5.1 Factorizing N or computing the curve order

It is well known that the problem of factorizing $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ is equivalent to that of computing the Euler totient function $\phi(N) = p_1^{e_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_r^{e_r - 1}(p_r - 1)$, e.g. see [**?**] or [**?**, Section 10.4].
In our case we need to show the following

Proposition 4. *The problem of factorizing N is equivalent to computing $\Psi(N) = p_1^{e_1 - 1}(p_1 + 1) \cdot \ldots \cdot p_r^{e_r - 1}(p_r + 1)$ or the order of the group $\mathcal{P}^*_{\mathbb{Z}_N}$ (or equivalently of $\mathcal{H}^*_{\mathbb{Z}_N}$), which is a divisor of $\Psi(N)$.*

Proof. Clearly, knowing the factorization of N yields $\Psi(N)$.
Conversely, suppose N and $\Psi(N)$ are known. A factorization of N can be found by applying Algorithm **??** recursively.

□

Remark 3. Algorithm **??** is an adaptation of the general algorithm in [**?**, Section 10.4], used to factorize N by only knowing $\phi(N)$ (Euler totient function) and N itself. The main idea of the Algorithm **??** comes from the fact that $x^{\odot\Psi(N)} = 1 \pmod N$ for all $x \in \mathbb{Z}_N^*$, which is the analog of the Euler theorem in $\mathcal{P}_{\mathbb{Z}_N}$. Notice that, because of Step **??**, Algorithm **??** is a probabilistic algorithm. Thus, to find a non-trivial factor, it might be necessary to run the algorithm more than once. We expect that a deeper analysis of the algorithm will lead to a similar probabilistic behaviour than the algorithm in [**?**], which returns a non-trivial factor with probability 1/2.

Algorithm 1 Find a factor of N by knowing N and $\Psi(N)$

```
1:  function FIND FACTOR(N,Ψ(N))
2:      h = 0
3:      t = Ψ(N)
4:      while IsEven(t) do
5:          h = h + 1
6:          t = t / 2
7:      a = Random(N − 1)
8:      d = gcd(a, N)
9:      if d ≠ 1 then
10:         return d
11:     b = a^{⊙t} mod N
12:     for j = 0, ..., h − 1 do
13:         d = gcd(b + 1, N)
14:         if d ≠ 1 or d ≠ N then
15:             return d
16:         b = b^2 mod N
17:     return 0
```

Since we proved that the problems **??** and **??** are equivalent, we can only focus on the factorization problem.
According to [**?**], state-of-the-art factorization methods as the Elliptic Curve Method [**?**] or the Number Field Sieve [**?**], [**?**] are not effective if in the following practical cases

- $|N| = 1024, 1536, 2048, 2560, 3072, 3584$ and $N = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ with $e_1 + e_2 + e_3 \leq 3$ and $p_i, i = 1, 2, 3$ greater than approximately the size of $\sqrt[3]{N}$.
- $|N| = 4096$ and $N = p_1^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4}$ with $e_1 + e_2 + e_3 + e_4 \leq 4$ and $p_i, i = 1, \ldots, 4$ greater than approximately the size of $\sqrt[4]{N}$.
- $|N| = 8192$ and $N = p_1^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4} p_5^{e_5}$ with $e_1 + e_2 + e_3 + e_4 + e_5 \leq 5$ and $p_i, i = 1, \ldots, 5$ greater than approximately the size of $\sqrt[5]{N}$.

Notice that currently, the largest prime factor found by the Elliptic Curve Method is a 274 bit digit integer [**?**]. Note also that the Lattice Factoring Method (LFM) of Boneh, Durfee, and Howgrave-Graham [**?**] is designed to factor integers of the form $N = p^u q$ only for large u.

5.2 Computing the Discrete Logarithm

Solving the discrete logarithm problem in a conic curve can be reduced to the discrete logarithm problem in the underlying finite field [**?**]. In our case the curve is defined over the ring $\mathbb{Z}_N$. Solving the DLP over $\mathbb{Z}_N$ without knowing the factorization of N is as hard as solving the DLP over a prime finite field of approximately the same size. As for the factorization problem, the best known algorithm to solve DLP on a prime finite field is the Number Field Sieve. When the size of N is greater than 1024 then the NFS can not be effective.

5.3 Solving the private key equation

In the case of RSA, small exponent attacks ([**?**], [**?**], [**?**]) can be performed to find the unknown d in the equation $ed \equiv 1 \mod \Psi(N)$. Generalization of these attacks can be performed on RSA variants where the modulus is of the form $N = p_1^{e_1} p_2^{e_2}$ [**?**]. It has already been argued in [**?**], [**?**] and [**?**] that this kind of attacks fails when the trapdoor function is not a simple monomial power as in RSA, as it is in the proposed scheme.

5.4 Finding an impossible group operation

In the case of elliptic curves over $\mathbb{Z}_N$, as in the generalized KMOV cryptosystem [**?**], it could happen that an impossible addition between two curve points occurs, yielding the factorization of N. This is due to the fact that the addition formula requires to perform an inversion in the underlying ring $\mathbb{Z}_N$. However, as shown by the same authors of [**?**], the occurrence of an impossible addition is very unlikely for N with few and large prime factors. In our case an impossible group operation may occur if $a + b$ is not invertible in $\mathbb{Z}_N$, i.e. if $\gcd(a + b, N) \neq 1$, yielding in fact a factor of N. However, also in our case, if N contains a few large prime factors, impossible group operations occur with negligible probability, as shown by the following proposition.

Proposition 5. *The probability to find an invertible element in $\mathcal{P}_{\mathbb{Z}_N}$ is approximately*

$$1 - \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)$$

Proof. The probability to find an invertible element in $\mathcal{P}_{\mathbb{Z}_N}$ is given by dividing the number of non-invertible elements in $\mathcal{P}_{\mathbb{Z}_N}$ by the total number

of elements of this set, as follows:

$$\frac{|\mathcal{P}_{\mathbb{Z}_N}| - \#\{\text{invertible elements in } \mathcal{P}_{\mathbb{Z}_N}\}}{|\mathcal{P}_{\mathbb{Z}_N}|} = \tag{6}$$

$$= \frac{|\mathbb{Z}_N| + 1 - (\#\{\text{invertible elements in } \mathbb{Z}_N\} + 1)}{|\mathbb{Z}_N| + 1} = \tag{7}$$

$$= \frac{N - \phi(N)}{N+1} = \tag{8}$$

$$\sim 1 - \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) \tag{9}$$

where we used $N \sim N+1$ and $\phi(N) = N\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)$. □

This probability tends to zero for large prime factors.

Let us notice that, in the Pell curve case, it is possible to avoid such situation, by performing encryption and decryption in $\mathcal{H}^*_{\mathbb{Z}_N}$, without exploiting the isomorphism operation. Here the group operation $\otimes$ is defined between two points on the Pell curve, as in Equation **??**, and does not contain the inverse operation. In the resulting scheme the ciphertext is obtained as $(C_x, C_y) = (M_x, M_y)^{\otimes e}$, where the operation $\otimes$ depends on D. Thus the triple (C_x, C_y, D) must be transmitted, resulting in a non-compressed ciphertext.

5.5 Recovering the message from D

To recover the message pair (M_x, M_y) from $D = \frac{M_x^2 - 1}{M_y^2} \pmod N$, the attacker must solve the quadratic congruence $M_x^2 - DM_y^2 - 1 = 0 \pmod N$ with respect to the two unknowns M_x and M_y. Even if one of the two coordinates is known (partially known plaintext attack), it is well known that computing square roots modulo a composite integer N, when the square root exists, is equivalent to factoring N itself.

5.6 Further comments

As a conclusion to this section, we only mention that as shown in [**?**], RSA-like schemes based on isomorphism own the following properties: they are more secure than RSA in the broadcast scenario, they can be transformed to semantically secure schemes using standard techniques which introduce randomness in the process of generating the ciphertext.

6 Efficiency of the encryption scheme

Recall that our scheme encrypts and decrypts messages of size $2\log N$. To decrypt a ciphertext of size $2\log N$ using CRT, standard RSA requires four full exponentiation modulo $N/2$-bit primes. Basic algorithms to compute $x^d \mod p$ requires $O(\log d \log^2 p)$, which is equal to $O(\log^3 p)$ if $d \sim p$.
Using CRT, if $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, our scheme requires at most r exponentiation modulo N/r-bit primes.
This means that the final speed up of our scheme with respect to RSA is

$$\frac{4 \cdot (N/2)^3}{r \cdot (N/r)^3} = r^2/2 \tag{10}$$

When $r = 2$ our scheme is two times faster than RSA, as it has already been shown in [**?**]. If $r = 3$ our scheme is 4.5 time faster, with $r = 4$ is 8 times faster, and with $r = 5$ is 12.5 times faster.

7 Conclusions

We generalized an RSA-like scheme based on the Pell hyperbola from a modulus that was a product of two primes to a generic modulus. We showed that this generalization leads to a very fast decryption step, up to 12 times faster than original RSA for the security level of a modulus of 8192 bits. The scheme preserves all security properties of RSA-like schemes, which are in general more secure than RSA, especially in a broadcast scenario. Compared to similar schemes based on elliptic curves it is more efficient. We also pointed that a variation of the scheme with non-compressed ciphertext does not suffer of impossible group operation attacks.

8 Appendix

Let us consider $p = 5$, $q = 7$, $r = 3$ and $s = 5$, so that the modulo used in our scheme is $N = p^r \cdot q^s = 2100875$. We choose $e = 359$ as the public exponent and consequently

$$d = 359^{-1} \pmod{(p^r+p^{r-1})(q^s+q^{s-1})} = 359^{-1} \pmod{2881200} = 1139639$$

is the secret one.

Let us suppose that we want to send the message pair

$$(M_x, M_y) = (956443, 745523) \in \mathbb{Z}_N^* \times \mathbb{Z}_N^*.$$

We evaluate $D = \dfrac{M_x^2 - 1}{M_x} \pmod N = 1660987$, in order that (M_x, M_y) lies on the conic $x^2 - Dy^2 = 1 \pmod N$.

For encrypting this message, we first evaluate the corresponding parameter of the point (M_x, M_y) by means of

$$M = \Phi(M_x, M_y) \pmod N = \frac{M_x + 1}{M_y} \pmod N = 2082503.$$

Now we encrypt M evaluating

$$2082503^{\odot 359} \pmod N = Q_{359}(1660987, 2082503) \pmod N = 550197 = C.$$

If we want to retrieve the original message from the cyphertext C, we evaluate

$$550197^{\odot 1139639} \pmod N = Q_{1139639}(1660987, 550197) \pmod N = 2082503 = M$$

and

$$\Phi^{-1}(M) \pmod N = \left(\frac{M^2 + D}{M^2 - D}, \frac{2M}{M^2 - D}\right) \pmod N = (956443, 745523).$$

References

[BCM10a] Stefano Barbero, Umberto Cerruti, and Nadir Murru, *Generalized Rédei rational functions and rational approximations over conics*, Int. J. Pure Appl. Math **64** (2010), no. 2, 305–317.

[BCM10b] ———, *Solving the Pell equation via Rédei rational functions*, The Fibonacci Quarterly **48** (2010), no. 4, 348–357.

[BDHG99] Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham, *Factoring $n = p^r q$ for large r.*, Crypto, vol. 1666, Springer, 1999, pp. 326–337.

[BL93] Daniel J Bernstein and Arjen K Lenstra, *A general number field sieve implementation*, The development of the number field sieve, Springer, 1993, pp. 103–126.

[BM16] Emanuele Bellini and Nadir Murru, *An efficient and secure RSA–like cryptosystem exploiting Rédei rational functions over conics*, Finite Fields and Their Applications **39** (2016), 179–194.

[BN17] Maher Boudabra and Abderrahmane Nitaj, *A new generalization of the KMOV cryptosystem*, Journal of Applied Mathematics and Computing (2017), 1–17.

[BS02] Dan Boneh and Hovav Shacham, *Fast variants of RSA*, CryptoBytes **5** (2002), no. 1, 1–9.

[CFPR96] Don Coppersmith, Matthew Franklin, Jacques Patarin, and Michael Reiter, *Low-exponent RSA with related messages*, Advances in Cryptology–EUROCRYPT'96, Springer, 1996, pp. 1–9.

[CHLS98] Thomas Collins, Dale Hopkins, Susan Langford, and Michael Sabin, *Public key cryptographic apparatus and method*, December 8 1998, US Patent 5,848,159.

[CKLQ02] Mathieu Ciet, François Koeune, Fabien Laguillaumie, and Jean-Jacques Quisquater, *Short private exponent attacks on fast variants of RSA*, UCL Crypto Group Technical Report Series CG-2002/4, University Catholique de Louvain (2002).

[Coh13] Henri Cohen, *A course in computational algebraic number theory*, vol. 138, Springer Science & Business Media, 2013.

[com02] *Cryptography using Compaq multiprime technology in a parallel processing environment*, 2002, http://nonstop.compaq.com/view.asp?IOID=4523.

[Cop97] Don Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, Journal of Cryptology **10** (1997), no. 4, 233–260.

[Has86] Johan Hastad, *On using RSA with low exponent in a public key network*, Advances in Cryptology–CRYPTO'85 Proceedings, Springer, 1986, pp. 403–408.

[JWTD09] Michael J Jacobson, Hugh C Williams, K Taylor, and Karl Dilcher, *Solving the Pell equation*, Springer, 2009.

[KMOV92] Kenji Koyama, Ueli M Maurer, Tatsuaki Okamoto, and Scott A Vanstone, *New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$*, Advances in Cryptology–CRYPTO'91, Springer, 1992, pp. 252–266.

[Koy95] Kenji Koyama, *Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 \pmod{n}$*, Advances in Cryptology–EUROCRYPT'95, Springer, 1995, pp. 329–340.

[LJ87] Hendrik W Lenstra Jr, *Factoring integers with elliptic curves*, Annals of mathematics (1987), 649–673.

[LKYL00] Seongan Lim, Seungjoo Kim, Ikkwon Yie, and Hongsub Lee, *A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$*, Indocrypt, Springer, 2000, pp. 283–294.

[LLJMP93] Arjen K Lenstra, Hendrik W Lenstra Jr, Mark S Manasse, and John M Pollard, *The number field sieve*, The development of the number field sieve, Springer, 1993, pp. 11–42.

[LPS17] Yao Lu, Liqiang Peng, and Santanu Sarkar, *Cryptanalysis of an RSA variant with moduli $n = p^r q^l$*, Journal of Mathematical Cryptology **11** (2017), no. 2, 117–130.

[Mil75] Gary L Miller, *Riemann's hypothesis and tests for primality*, Proceedings of seventh annual ACM symposium on Theory of computing, ACM, 1975, pp. 234–239.

[Mor95] Willi More, *Fast evaluation of Rédei functions*, Appl. Algebra Eng. Commun. Comput. **6** (1995), no. 3, 171–173.

[MV92] Alfred J Menezes and Scott A Vanstone, *A note on cyclic groups, finite fields, and the discrete logarithm problem*, Applicable Algebra in Engineering, communication and computing **3** (1992), no. 1, 67–74.

[Pad06] Sahadeo Padhye, *A Public Key Cryptosystem Based on Pell Equation.*, IACR Cryptology ePrint Archive **2006** (2006), 191.

[Réd46] László Rédei, *Über eindeutig umkehrbare polynome in endlichen körpern redei*, Acta Sci. Math. (1946), no. 11, 85–92.

[Sho09] Victor Shoup, *A computational introduction to number theory and algebra*, Cambridge university press, 2009.

[Tak98] Tsuyoshi Takagi, *Fast RSA-type cryptosystem modulo $p^k q$*, Advances in Cryptology–CRYPTO'98, Springer, 1998, pp. 318–326.

[Wie90] Michael J Wiener, *Cryptanalysis of short RSA secret exponents*, Information Theory, IEEE Transactions on **36** (1990), no. 3, 553–558.

[Zim] Zimmermann, *50 largest factors found by ECM*, `https://members.loria.fr/PZimmermann/records/top50.html`, Accessed 2017-07-28.