Finite Fields and Their Applications 39 (2016) 179–194

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics

Emanuele Bellini [*], Nadir Murru [*]

ARTICLE INFO

Article history:
Received 11 November 2015
Received in revised form 21 January 2016
Accepted 22 January 2016
Available online xxxx
Communicated by Neal Koblitz

MSC:
11T71
94A60
14G50
68P25

Keywords:
Rédei function
RSA
Public cryptography

ABSTRACT

We define an isomorphism between the group of points of a conic and the set of integers modulo a prime equipped with a non-standard product. This product can be efficiently evaluated through the use of Rédei rational functions. We then exploit the isomorphism to construct a novel RSA-like scheme. We compare our scheme with classic RSA and with RSA-like schemes based on the cubic or conic equation. The decryption operation of the proposed scheme turns to be two times faster than RSA, and involves the lowest number of modular inversions with respect to other RSA-like schemes based on curves. Our solution offers the same security as RSA in a one-to-one communication and more security in broadcast applications.

1. Introduction

RSA cryptosystem security is based on the existence of an one-way trapdoor function [8,35], which is easy to compute and difficult to invert without knowing some information, i.e., the trapdoor. Consider $N = pq$, where p and q are two primes of roughly the same size, and e an invertible element in $\mathbb{Z}_{\phi(N)}$ ($\phi(N)$ Euler totient function). Given the function $\tau_{N,e}(x) = x^e \pmod{N}$, it is not known if there exists a probabilistic

[*] Corresponding authors.
E-mail addresses: eemanuele.bellini@gmail.com (E. Bellini), nadir.murru@unito.it (N. Murru).

http://dx.doi.org/10.1016/j.ffa.2016.01.011
1071-5797/

polynomial time algorithm in N which can invert τ, for any $x \in \mathbb{Z}_N^*$, without knowing either p, q, $\phi(N)$ or the inverse d of e in $\mathbb{Z}_{\phi(N)}$. Thus the pair (N, e), called the public key, is known to anyone, while the triple (p, q, d), called the secret key, is only known to the receiver of an encrypted message. The ciphertext C is obtained as $C = M^e \pmod N$, and the original message M is obtained with the exponentiation $M = C^d \pmod N$.

Factoring N is the most common tried way for breaking RSA. Some attacks are possible when either the private exponent d is small [34], or the public exponent e is small [5,6]. Several other methods, which exploit extra information leaked by erroneous implementations of the cryptosystem, exist (e.g., see [17]).

Besides one-to-one communication scenario, there also exist other cryptographic scenarios, such as broadcast applications, where RSA leaks additional vulnerabilities (e.g., see [11]).

RSA-like schemes (e.g., see [14,15,23]) have been proposed in order to avoid some of these attacks. Some of these schemes turn to have also a faster decryption procedure. They are based on isomorphism between two groups, one of which is the set of points over a curve, usually a cubic or a conic.

In this work we present an improvement of such schemes. We provide a new RSA-like scheme based on isomorphism over a conic, with the fastest isomorphism with respect to the ones known by the authors. Furthermore, our scheme uses a different set of conics with respect to that of [23], which owns the fastest decryption procedure. We provide security proofs and efficiency comparisons.

In Section 2 we give an overview of the use of conic equations in cryptography and we introduce RSA-like schemes based on isomorphism. In Section 3 we introduce a parametrization of certain conics and we introduce the isomorphism used for the cryptographic scheme. In Section 4 we describe our scheme, highlighting connections with Rédei rational functions and differences with other schemes based on the Pell equation and Dickson polynomials. In Section 5 we discuss security issues. We prove that our scheme is as secure as RSA in an one-to-one communication scenario, while it is more secure in a broadcast scenario. We also show that our scheme is secure against partially known-plaintext attacks. Finally, in Section 6 we expose some efficiency considerations and comparisons with special focus on the decryption procedure, where our scheme presents the lowest computational complexity if compared to all known similar schemes.

2. Related works

In this section we provide a quick overview of the use of conic equations to construct cryptographic protocols. Then we define a generic RSA-like scheme based on an isomorphism between two groups.

2.1. The use of conic equations in cryptography

The use of conic equations is not novel in cryptography, in particular to build RSA-like cryptosystems.

In [16] the Pell analogue of RSA protocol, Diffie–Hellman key-exchange, and computing square roots modulo n, is presented. Specifically, as far as it concerns RSA, it is noticed that where RSA sends one encrypted message C about the size of N, the Pell version has to send twice as many bits per message, without having increased the security of the system.

In [9] RSA, Rabin and ElGamal variants of Pell's equation are presented proving that the proposed solutions are as secure as the original schemes. The proposed schemes are claimed to have also the same asymptotic complexity as the original schemes.

Three RSA-like schemes based on Pell's equation are presented in [23]. All three schemes have a faster decryption procedure than RSA. The first two schemes are proved to be as secure as RSA in a one-to-one communication scenario and more secure in a broadcast scenario since they increase the complexity of some low exponent attacks such as [11]. The third scheme is the Pell analogue of [30] scheme. It is proved to be semantically secure (recall RSA is not) and it is derived by randomizing the second scheme in a standard way described in [30].

An implementation of Scheme II of [23] is analyzed in [29]. The scheme is implemented using GMP library [10], and compared in its favor against a RSA implementation using the same library [2].

The use of Rédei rational function for a cryptographic scheme is introduced in [13]. Though, the two schemes are inefficient with respect to RSA, since a larger modulo ($\mathcal{O}(n^2)$ instead of $\mathcal{O}(n)$) is used for the public exponent, and no isomorphism is exploited, making both encryption and decryption slower than RSA.

In [31] the advantages of key generation of a cryptosystem based on Pell's equation versus standard RSA (and some variants) key generation are discussed. The authors claim their key generation prevents Wiener attacks [34].

A symmetric cryptographic scheme based on the Brahmagupta–Bhãskara equation has been proposed in [21], attacked in [36], corrected in the author's replay, and re-attacked in [1] with a known-plaintext attack.

A combination of Arnold Cat Map, Chaotic Map, and Brahmagupta–Bhãskara equation has also been used to build cryptosystems for image encryption and decryption (e.g., see [27,32]).

Based on Pell's equation, in [24], a claimed Identity-Based Encryption scheme is presented. The efficiency of its implementation using GMP library [10] is analyzed in [25].

Also a Dynamic Threshold Multi Secret Sharing scheme [28] and a Signature scheme [18] have been recently published.

Other RSA type cryptosystems based on elliptic curves exist, such as [15,14,7]. These schemes have a computationally more expansive addition operation compared to schemes based on Pell's equation, such as [23].

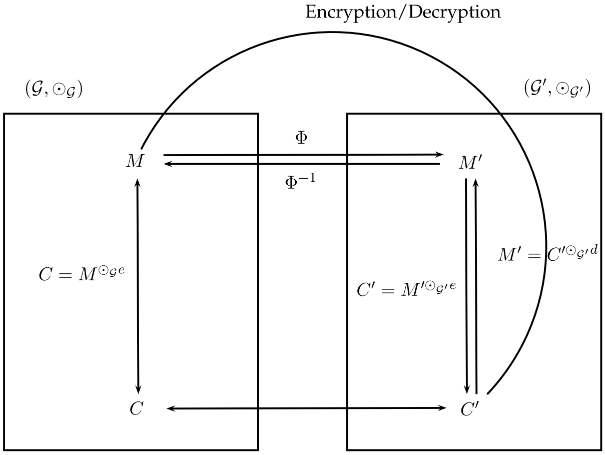
Encryption/Decryption
$(\mathcal{G}, \odot_{\mathcal{G}})$
$(\mathcal{G}', \odot_{\mathcal{G}'})$
M
Φ
Φ^{-1}
M'
$C = M^{\odot_{\mathcal{G}} e}$
$C' = M'^{\odot_{\mathcal{G}'} e}$
$M' = C'^{\odot_{\mathcal{G}'} d}$
C
C'

Fig. 1. RSA-like scheme based on isomorphism.

2.2. RSA-like schemes based on isomorphism

In the following we use multiplicative notation for groups. In particular, for a group $\mathcal{G}$ with operation $\odot_{\mathcal{G}}$ and an element $G \in \mathcal{G}$, we use the following notation for the exponentiation with respect to the group operation

$$G^{\odot_{\mathcal{G}} x} = \underbrace{G \odot_{\mathcal{G}} \ldots \odot_{\mathcal{G}} G}_{x \text{ times}} .$$

In [15], the concept of RSA-type schemes based on the isomorphism between two groups has been introduced in order to have a faster decryption with respect to the original RSA scheme. Such a scheme can be obtained by finding an efficiently computable isomorphism

$$\Phi : (\mathcal{G}, \odot_{\mathcal{G}}) \to (\mathcal{G}', \odot_{\mathcal{G}'})$$

between two groups, in such a way that, in the decryption procedure, the use of the exponentiation in $\mathcal{G}'$ and the inverse of the isomorphism is more efficient than just applying the exponentiation in $\mathcal{G}$. The scheme is visualized in Fig. 1. The message M is encrypted into the ciphertext C', either by first applying the exponentiation in $\mathcal{G}$ and then the isomorphism, or by first applying the isomorphism and then the exponentiation in $\mathcal{G}'$. The decryption follows the inverse process.

Usually $\mathcal{G}$ is the set of points of a curve over the ring $\mathbb{Z}_N$ provided with a group law, N the product of two primes, and $\mathcal{G}'$ is a subgroup of $\mathbb{Z}_N^*$. The first proposed curve in [15] was a singular cubic curve, while a particular set of conics was proposed in [23] providing a more efficient isomorphism inverse. In our work we propose another set of conics and we consider $\mathcal{G}' = \mathbb{Z}_N^*$ provided with a non-standard group law, yielding a more efficient isomorphism inverse.

3. Product of points over conics

In this section, we use an irreducible polynomial of degree 2 to define a quotient field that induces a product over certain conics. This product gives a group structure to the conics. Then, we introduce a parametrization that allows us to define a bijection between a conic and a set of parameters, yielding a group structure on this set. Finally, we determine the order of this group. In Section 4 we use the bijection, which turns out to be an isomorphism, to construct our RSA-like scheme.

3.1. A group structure over conic curves

Conics are the most simple non-linear curves and the Pell hyperbola defined by

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

where D is a given positive integer (non-square), is one of the most popular, since it contains all the solutions of the famous Pell equation. A group structure can be defined over the Pell hyperbola by means of the following product between points in $\mathcal{H}$:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 + Dy_1y_2, y_1x_2 + x_1y_2),$$

see, e.g., [33] and [12].

Let $\mathbb{K}$ be an ordinary field, the previous product can be generalized in order to provide a group structure over the conics

$$\mathcal{C}_{\mathbb{K}} = \{(x, y) \in \mathbb{K} \times \mathbb{K} : x^2 + Hxy - Dy^2 = 1\}.$$

When clear from the context we write $\mathcal{C}$ instead of $\mathcal{C}_{\mathbb{K}}$, omitting the subscript.

Let $x^2 - Hx - D$ be an irreducible polynomial over $\mathbb{K}[x]$ and let us consider the quotient field

$$\mathbb{A} = \mathbb{K}[x]/(x^2 - Hx - D).$$

Given $p + qx$ and $r + sx$ in $\mathbb{A}$, the induced product is

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

We now want to define the conjugate over $\mathbb{A}$ of an element $p + qx$ with respect to $\mathbb{K}$. Notice that $\mathbb{A}$ is an extension of degree 2 over $\mathbb{K}$ and so the minimal polynomial of $p+qx$ over $\mathbb{K}$ has degree 2. Thus, we are looking for an element $r + sx$ such that the sum and the product between this element and its conjugate $p + qx$ is in $\mathbb{K}$. It is immediate to see that $s = -q$. Moreover, since

$$(p+qx)(r-qx) = (pr - q^2 D) + (rq - pq - q^2 H)x$$

we obtain that $r = p+qH$. Thus, the conjugate $\overline{p+qx}$ of an element $p+qx$ is $(p+qH)-qx$. Then, the norm of $p+qx$ over $\mathbb{K}$ is given by the product of the conjugates of $p+qx$, which is

$$(p+qx)(\overline{p+qx}) = p^2 + Hpq - Dq^2 \,.$$

The group of unitary elements of $\mathbb{A}^* = \mathbb{A} - \{0\}$ is

$$\mathcal{U} = \{p + qx \in \mathbb{A}^* : p^2 + Hpq - Dq^2 = 1\}.$$

Consequently, there is a bijection between $\mathcal{U}$ and the conic $\mathcal{C}$ which determines a commutative group structure over the conic by means of the product

$$(x,y) \odot_{\mathcal{C}} (u,v) = (xu + yvD, yu + xv + yvH), \quad \forall (x,y),(u,v) \in \mathcal{C}. \tag{1}$$

Proposition 1. *$(\mathcal{C}, \odot_{\mathcal{C}})$ is a commutative group with identity $(1,0)$ and the inverse of an element (x,y) is $(x+Hy,-y)$.*

3.2. A group structure on the set of parameters

We can use the following parametrization for the conic $\mathcal{C}$:

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

Definition 1. Let us define the set of parameters $\mathcal{P}_{\mathbb{K}} = \mathbb{K} \cup \{\alpha\}$, with α not in $\mathbb{K}$. From the parametrization we can derive the following bijection between $\mathcal{C}$ and $\mathcal{P}_{\mathbb{K}}$:

$$\Phi_{H,D} : \begin{cases} \mathcal{C} & \to \mathcal{P}_{\mathbb{K}} \\ (x,y) & \mapsto \dfrac{1+x}{y} \quad \forall (x,y) \in \mathcal{C}, \quad y \neq 0 \\ (1,0) & \mapsto \alpha \\ (-1,0) & \mapsto -\dfrac{H}{2}\,, \end{cases} \tag{2}$$

and

$$\Phi^{-1}_{H,D} : \begin{cases} \mathcal{P}_{\mathbb{K}} & \to \mathcal{C} \\ m & \mapsto \left(\dfrac{m^2+D}{m^2+Hm-D}, \dfrac{2m+H}{m^2+Hm-D} \right) \quad \forall m \in \mathbb{K}\,. \\ \alpha & \mapsto (1,0) \end{cases} \tag{3}$$

For the seek of simplicity, we only write Φ when there is no confusion. This bijection allows us to derive from $\odot_{\mathcal{C}}$ the following product over the set of parameters $\mathcal{P}_{\mathbb{K}}$:

$$\begin{cases} a \odot_{\mathcal{P}_{\mathbb{K}}} b = \dfrac{D+ab}{H+a+b}, & a+b \neq -H \\ a \odot_{\mathcal{P}_{\mathbb{K}}} b = \alpha, & a+b=-H \end{cases}. \tag{4}$$

Proposition 2. *$(\mathcal{P}_{\mathbb{K}}, \odot_{\mathcal{P}_{\mathbb{K}}})$ is a commutative group with identity α and the inverse of an element a is the element b such that $a+b=-H$ and Φ is an isomorphism between $\mathcal{C}$ and $\mathcal{P}_{\mathbb{K}}$.*

The above parametrization of the conic $\mathcal{C}$ has been introduced in [3], where the authors used it in order to study approximations of irrationalities over conics. The commutative group $(\mathcal{P}_{\mathbb{K}}, \odot_{\mathcal{P}_{\mathbb{K}}})$ can be also directly derived from $\mathbb{A}^*$ and it is possible to show that the quotient group $\mathcal{B} = \mathbb{A}^*/\mathbb{K}^*$ and $\mathcal{P}_{\mathbb{K}}$ are isomorphic [3].

Let us observe that when $\mathbb{K} = \mathbb{Z}_p$, with p prime, $\mathbb{A}$ is a finite field with p^2 elements, i.e., it is the Galois field $GF(p^2)$. Moreover, $\mathcal{B}$ has order $(p^2-1)/(p-1) = p+1$ and consequently we have that $\mathcal{P}_{\mathbb{Z}_p}$ and $\mathcal{C}_{\mathbb{Z}_p}$ are cyclic groups of order $p+1$.

Remark 1. Thus, an analogue of the Fermat little theorem holds in $\mathcal{P}_{\mathbb{Z}_p}$ and $\mathcal{C}_{\mathbb{Z}_p}$, i.e.,

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

and

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

where powers are performed using products $\odot_{\mathcal{P}_{\mathbb{Z}_p}}$ and $\odot_{\mathcal{C}_{\mathbb{Z}_p}}$, respectively.

4. A public-key cryptosystem

In this section we develop a RSA-like scheme exploiting the properties of the product $\odot_{\mathcal{P}_{\mathbb{Z}_p}}$ and the isomorphism Φ redefined to make sense also when the conic is considered over the ring $\mathbb{Z}_N$. In particular, we will exploit the fact that an analogue of the Fermat little theorem holds in $\mathcal{P}_{\mathbb{Z}_p}$. Moreover, we see that powers with respect to this product can be evaluated in a fast way and the decryption operation in our scheme involves only one modular inverse, by means of the definition of Φ.

4.1. Preliminaries

In order to insert a trapdoor in our scheme we would like to extend the ideas of Section 3 to hold for the conic

$$\mathcal{H}_{\mathbb{Z}_N} = \{(x,y) \in \mathbb{Z}_N \times \mathbb{Z}_N : x^2 - Dy^2 = 1 \pmod{N}\},$$

where $\pm D \in \mathbb{Z}_N^*$ are quadratic non-residues modulo N and $N = pq$ with p, q prime numbers. The condition on D will ensure the isomorphism inverse to be well defined. The condition on $-D$ will ensure the powers with respect to $\odot_{\mathcal{P}_{\mathbb{Z}_N}}$ to be well defined. To lighten the notation, in the remainder of the paper we omit the subscript $\mathbb{Z}_N$ from $\mathcal{H}_{\mathbb{Z}_N}$ and $\mathcal{P}_{\mathbb{Z}_N}$ where there is no ambiguity.

Thus, we are working on a conic $\mathcal{C}$ where $H = 0$ and $\mathbb{K} = \mathbb{Z}_N$. Since $\mathbb{Z}_N$ is not a field we need to refine some of the definitions. In particular, in this case, the map $\Phi_{0,D} : \mathcal{H} \to \mathcal{P}$ of Definition 1 is not an isomorphism. However, considering

$$\mathcal{H}^* = \{(x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N^* : x^2 - Dy^2 = 1 \pmod N\}$$

we have that $|\mathcal{H}^*| = |\mathbb{Z}_N^*|$ as proved in the following proposition. From now on we also omit the subscripts $0, D$ from $\Phi_{0,D}$.

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

1. $\forall(x_1, y_1), (x_2, y_2) \in \mathcal{H}^*$, $\Phi(x_1, y_1) = \Phi(x_2, y_2) \Leftrightarrow (x_1, y_1) = (x_2, y_2)$;
2. $\forall m_1, m_2 \in \mathbb{Z}_N^*$, $\Phi^{-1}(m_1) = \Phi^{-1}(m_2) \Leftrightarrow m_1 = m_2$;
3. $\forall m \in \mathbb{Z}_N^*$, *we have* $\Phi^{-1}(m) \in \mathcal{H}^*$ *and* $\forall(x, y) \in \mathcal{H}^*$, *we have* $\Phi(x, y) \in \mathbb{Z}_N^*$.

Proof.

1. We have that

$$\Phi(x_1, y_1) = \Phi(x_2, y_2) \Leftrightarrow (1 + x_1)y_2 = (1 + x_2)y_1.$$

Squaring both members and multiplying them by D, we obtain

$$D(1 + x_1)^2 y_2^2 = D(1 + x_2)^2 y_1^2.$$

Since $(x_1, y_1), (x_2, y_2) \in \mathcal{H}^*$, we get

$$(1 + x_1)^2(x_2^2 - 1) = (1 + x_2)^2(x_1^2 - 1)^2$$

from which it is easy to prove that $x_1 = x_2$ and $y_1 = y_2$.

2. We have that

$$\Phi^{-1}(m_1) = \Phi^{-1}(m_2) \Leftrightarrow \left(\frac{m_1^2 + D}{m_1^2 - D}, \frac{2m_1}{m_1^2 - D}\right) = \left(\frac{m_2^2 + D}{m^2 - D}, \frac{2m_2}{m_2^2 - D}\right).$$

Direct calculations show that this equality holds only when $m_1 = m_2$.

3. Using the explicit forms of Φ and Φ^{-1} the proof is straightforward. □

We recall the definition of $\Phi_{H,D}$ with $H = 0$ where we consider it only between $\mathcal{H}^*$ and $\mathbb{Z}_N^*$.

Definition 2. We consider the bijection Φ between $\mathcal{H}^*$ and $\mathbb{Z}_N^*$ as

$$\Phi : \begin{cases} \mathcal{H}^* & \to \mathbb{Z}_N^* \\ (x, y) & \mapsto \dfrac{1+x}{y} \end{cases}$$

and its inverse

$$\Phi^{-1} : \begin{cases} \mathbb{Z}_N^* & \to \mathcal{H}^* \\ m & \mapsto \left(\dfrac{m^2 + D}{m^2 - D}, \dfrac{2m}{m^2 - D} \right) \end{cases} .$$

The products over $\mathcal{H}^*$ and $\mathbb{Z}_N^*$ still follow the same rules seen in the previous section, i.e.,

$$(x_1, y_1) \odot_{\mathcal{H}} (x_2, y_2) = (x_1 x_2 + D y_1 y_2, y_1 x_2 + x_1 y_2), \quad \forall (x_1, y_1), (x_2, y_2) \in \mathcal{H}$$

and

$$a \odot_{\mathcal{P}} b = \frac{D + ab}{a + b}, \quad \forall a, b \in \mathbb{Z}_N^*, \quad a + b \in \mathbb{Z}_N^*.$$

As a consequence of Remark 1, given $l = \operatorname{lcm}(p+1, q+1)$ and $r = 1 \pmod{l}$ we have

$$m^{\odot_{\mathcal{P}} r} = m \pmod{N}, \quad \forall m \in \mathbb{Z}_N^*$$

and

$$(x, y)^{\odot_{\mathcal{H}} r} = (x, y) \pmod{N}, \quad \forall (x, y) \in \mathcal{H}_N^*,$$

where powers are performed using products $\odot_{\mathcal{P}}$ and $\odot_{\mathcal{H}}$, respectively.

Remark 2. In [4] the authors prove that powers with respect to the product $\odot_{\mathcal{P}}$ can be evaluated by the Rédei rational functions [26]. These functions arise from the development of $(z + \sqrt{D})^n$, where z is an integer and D is a non-square positive integer. One can write

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

where

$$A_n(D,z)=\sum_{k=0}^{[n/2]}\binom{n}{2k}D^k z^{n-2k},\quad B_n(D,z)=\sum_{k=0}^{[n/2]}\binom{n}{2k+1}d^k z^{n-2k-1}.$$

These polynomials can be also determined by

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

with

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

The Rédei rational functions $Q_n(D,z)$ are defined by

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

The powers with respect to the product $\odot_{\mathcal{P}}$ can be evaluated as follows:

$$z^{\odot_{\mathcal{P}} n}=\underbrace{z\odot_{\mathcal{P}}\ldots\odot_{\mathcal{P}} z}_{n\text{ times}}=Q_n(D,z).$$

In this way, the exponentiation in $\mathcal{P}$ can be performed efficiently. Indeed, in [20] the author exhibits an algorithm of complexity $O(log_2(n))$ with respect to addition, subtraction and multiplication to evaluate Rédei rational functions $Q_n(D,z)$ over a ring.

4.2. The scheme

In this section, we explicitly describe the key generation, the encryption and the decryption algorithms. The following steps show the key generation:

- choose two prime numbers p, q and compute $N=pq$;
- choose an integer e such that $\gcd(e,\operatorname{lcm}(p+1)(q+1))=1$.
  The pair (N,e) is called the *public* or *encryption key*;
- evaluate $d=e^{-1}\pmod{\operatorname{lcm}(p+1)(q+1)}$.
  The triple (p,q,d) is called the *secret* or *decryption key.*

Now, let us consider the set

$$\tilde{\mathbb{Z}}_N^*=\left\{\frac{m^2+D}{m^2-D}:\forall m,D\in\mathbb{Z}_N^*,\pm D\text{ quadratic non-residues modulo }N\right\}.$$

Let us suppose that we want to encrypt two messages $(M_x,M_y)\in\tilde{\mathbb{Z}}_N^*\times\mathbb{Z}_N^*$. The following steps describe the encryption algorithm:

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

Once (C, D) are sent to the receiver, the decryption algorithm is described as follows:

- compute $C^{\odot_{\mathcal{P}} d} \pmod{N} = M$;
- retrieve the plaintexts (M_x, M_y) by means of Φ^{-1}, i.e.
  $(M_x, M_y) = \Phi^{-1}(M) = \left(\dfrac{M^2 + D}{M^2 - D}, \dfrac{2M}{M^2 - D}\right) \pmod{N}$.

4.3. Some remarks

In the previous section, we have introduced an RSA-like scheme based on the Pell equation. Our scheme has some important differences with respect to other similar schemes.

First of all, we have considered Pell's equation $x^2 - Dy^2 = 1$ in $\mathbb{Z}_N$, where D is not a quadratic residue, while in [23] the author worked on the complementary case, i.e., when D is a quadratic residue.

Moreover, we have used a particular parametrization which allowed us to define an original product $\odot_{\mathcal{P}_{\mathbb{Z}_P}}$ connected to Rédei rational functions. We have seen that in this case an analogue of the Fermat little theorem holds, i.e.,

$$m^{\odot_{\mathcal{P}_{\mathbb{Z}_P}} p+2} = m \pmod{p}, \quad \forall m \in \mathcal{P}_{\mathbb{Z}_p}, \quad p \text{ prime},$$

when $\mathbb{K}$ is a finite field. For this reason, the decryption key is computed modulo $\operatorname{lcm}(p + 1)(q + 1)$, while in RSA schemes (and also in [23]) it is computed modulo $\operatorname{lcm}(p - 1)(q - 1)$. Furthermore, it is known that Rédei rational functions can be exploited for the construction of cryptographic systems following the Dickson scheme (see, [22] and [19]). However, in these schemes the decryption key is computed modulo $\operatorname{lcm}(p^2 - 1)(q^2 - 1)$, which is much less efficient.

Finally, in the previous section we have seen that we can send message pairs in $\tilde{\mathbb{Z}}_N^* \times \mathbb{Z}_N^*$. We can observe that also in other RSA-like schemes that exploit the Pell equation we are not able to encrypt all message pairs in $\mathbb{Z}_N^* \times \mathbb{Z}_N^*$. In the next example we see a message pair that can be encrypted using our scheme, but that cannot be encrypted with the analogous scheme developed in [23].

Example 1. Let us consider $p = 11$, $q = 13$, and $N = 143$. We choose $e = 5$ as the public exponent and consequently $d = 5^{-1} \pmod{168} = 101$ is the secret one.

Let us suppose that we want to send the message pair $(M_x, M_y) = (83, 135) \in \tilde{\mathbb{Z}}_N^* \times \mathbb{Z}_N^*$. We obtain $D = \dfrac{M_x^2 - 1}{M_x} \pmod{N} = 54$ and $M = \Phi(M_x, M_y) \pmod{N} = 61$. Now we encrypt M evaluating

$$61^{\odot_{\mathcal{P}}5} \pmod N = 38.$$

If we want to retrieve the original message we compute

$$38^{\odot_{\mathcal{P}}101} \pmod N = 61$$

and

$$\Phi^{-1}(61) \pmod N = (83, 135).$$

Example 2. If we try to use the scheme II in [23] for encrypting the message pair $(M_x, M_y) = (83, 135)$ we have to compute

$$Z_1 = M_x M_y \pmod N = 51, \quad Z_1^{-1} \pmod N = 129$$

and to solve the system

$$\begin{cases} X - aY = Z_1 \pmod N \\ X + aY = Z_1^{-1} \pmod N \end{cases}$$

where $Y = M_y$ and the unknowns are X and a. In this way, we get

$$X = 98, \quad a = 11.$$

We can observe that in this case a is not invertible in $\mathbb{Z}_N$ and consequently we cannot compute the value a^{-1} which is necessary for the decryption. However, this is a very rare situation when N is large, and finding a non-invertible element of $\mathbb{Z}_N$ is equivalent to factorize N itself.

5. Security of the proposed scheme

In this section we first prove that our scheme offers the same security as RSA in a one-to-one communication scenario. Then we provide evidence that our scheme is secure against partially known plaintext attacks, and against some attacks of which RSA is vulnerable in a broadcast scenario. We conclude with a comment on semantic security.

5.1. Security reduction to RSA

We show, with a standard reduction argument, that breaking our scheme is equivalent to breaking RSA scheme.

Theorem 1. *The following sentences are equivalent*

1. *There exists a probabilistic polynomial time algorithm $A1$ such that for all $C, D \in \mathbb{Z}_N^*$, if $C = \Phi(M_x, M_y)^{\odot_{\mathcal{P}}e}$ and $D = (M_x^2 - 1)^2/M_y^2 \pmod N$, then $A1(C, D, e, N) = (M_x, M_y)$, where D quadratic non-residue modulo N, $(M_x, M_y) \in \tilde{\mathbb{Z}}_N \times \mathbb{Z}_N$.*

2. *There exists a probabilistic polynomial time algorithm $A2$ such that for all $M \in \mathbb{Z}_N^*$, if $C = M^e \pmod{N}$, then $A2(C, e, N) = M$.*

Proof. First assume 1 and prove 2.

Given C, e, N we want to compute M using $A1$.

Choose D random quadratic non-residue modulo N.

Compute $(M_x, M_y) = A1(C, D, e, N)$.

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

Now assume 2 and prove 1.

Given C, D, e, N we want to compute (M_x, M_y) using $A2$.

Compute $A2(C, e, N) = M$.

Compute $(M_x, M_y) = \Phi^{-1}(M) = \left(\dfrac{M^2 + D}{M^2 - D}, \dfrac{2M}{M^2 - D}\right) \pmod{N}$.

This completes the proof. □

5.2. Partially known plaintext attack

Consider the case where the attacker is provided with the one of the two plaintext coordinates. Since $D = \frac{M_x^2 - 1}{M_y^2} \pmod{N}$, the attacker has to solve the quadratic congruence $M_x^2 - DM_y^2 - 1 = 0 \pmod{N}$ with respect to either M_x or M_y. It is well known that computing square roots modulo a composite integer N, when the square root exists, is equivalent to factoring N itself.

5.3. Broadcast applications

As many other RSA-like schemes, such as [14,15,23], our scheme is more secure than the original RSA scheme when considering broadcast applications. In such a scenario the plaintext M is encrypted for r receivers using the same public exponent e and different moduli N_i for each receiver, with $i = 1, \ldots, r$. In [11] it is shown that, even if the messages are public linear combinations of each other, if $r > e$ it is possible to recover M by solving a set of r congruences of polynomials of degree e. However, as shown for example in [14] and [15], this kind of attacks fails when the trapdoor function is not a simple monomial power as in RSA. This allows the use of smaller exponents e even in broadcast scenarios.

5.4. Semantic security

Our scheme can be easily transformed into a semantically secure scheme using standard techniques which introduce randomness in the process of generating the ciphertext. An example of these techniques is given in [23], when transforming scheme II into scheme III.

Table 1
Comparison of decryption costs for a $(2\log N)$-bit plaintext.

	Decryption costs	Ciphertext size	$\Phi^{-1}(x)$
RSA	$2\mathrm{E}^d_{\mathbb{Z}_N}$	$2\log N$	–
[23]-I	$1\mathrm{E}^d_{\mathbb{Z}_N}+3\mathrm{M}+3\mathrm{I}$	$3\log N$	$\left(\frac{x^{-1}+x}{2}, \frac{x^{-1}-x}{2\sqrt{D}}\right)$
[23]-II	$1\mathrm{E}^d_{\mathbb{Z}_N}+2\mathrm{M}+3\mathrm{I}$	$2\log N$	$\left(\frac{x^{-1}+x}{2}, \frac{x^{-1}-x}{2\sqrt{D}}\right)$
[15]-II	$1\mathrm{E}^d_{\mathbb{Z}_N}+6\mathrm{M}+2\mathrm{I}$	$2\log N$	$\left(\frac{a^2x}{(x-1)^2}, \frac{a^3x}{(x-1)^3}\right)$
Our scheme	$1\mathrm{E}^d_{\mathcal{P}}+3\mathrm{M}+1\mathrm{I}$	$2\log N$	$\left(\frac{x^2+D}{x^2-D}, \frac{2x}{x^2-D}\right)$

6. Efficiency comparison with RSA-like schemes

In this section we take into consideration the most efficient and secure published RSA-like scheme based on Pell's equation, i.e. [23], and make a comparison with our proposed scheme.

Recall that the isomorphism used in the schemes of [23] is given by

$$\Phi : \begin{cases} \mathcal{H}_N & \to \mathbb{Z}_N^* \\ (x,y) & \mapsto x - Dy \pmod{N} \end{cases}$$

while the isomorphism used in [15], where $\mathcal{E} = \{(x,y) \in \mathbb{Z}_N^* \colon y^2 + axy = x^3 \pmod{N}\}$, is

$$\Phi : \begin{cases} \mathcal{E} & \to \mathbb{Z}_N^* \\ (x,y) & \mapsto 1 + \frac{ax}{y} \pmod{N} = \frac{x^3}{y^2} \pmod{N} \end{cases}$$

Both inverses are provided in Table 1. In practice the public exponent e is usually chosen small and with an efficient binary representation, i.e. $e = 2^{2^i}+1$, $i = 1,2,3,4$. Thus the exponentiation x^e performed during the encryption is usually much faster than x^d, which is done during decryption. For this reason our comparison concerns only decryption time.

Notice also that all three schemes in [23] can only encrypt messages of size $2\log N$, and thus a fair comparison with RSA is done if considering encryption messages of the same size (rather than $\log N$-bit plaintext), which means RSA exponentiation must be applied two times in parallel, both during encryption and decryption.

In Table 1, we indicate with M the modular multiplication (including squaring), with I the modular inverse and with $\mathrm{E}^y_{\mathcal{G}}$ the modular exponentiation x^y in the group $\mathcal{G}$. Notice that, by the observation in Remark 2, both the operations $\mathrm{E}^d_{\mathbb{Z}_N}$ and $\mathrm{E}^d_{\mathcal{P}}$ can be performed in $\mathcal{O}(\log_2 N)$ with respect to addition, subtraction and multiplication.

In Table 1 we report the decryption costs of RSA, the first two schemes of [23], the second scheme of [15], and our scheme.

RSA is the only scheme requiring two exponentiations. All other schemes require one exponentiation and one application of the isomorphism inverse ([23]-I requires also the application of the isomorphism). Notice that our isomorphism has the lowest number of inversions, i.e. one, and only one more multiplication than [23]-II, yielding the fastest isomorphism inverse.

7. Conclusions

We have presented an original RSA-like scheme based on an isomorphism between a conic and the set $\mathbb{Z}_N^*$ with a non-standard product. The scheme is complementary to the fastest original RSA-like scheme based on conics, and furthermore it has a faster isomorphism inverse operation. We have also proved that our solution provides a two times faster decryption operation than the original RSA scheme, while offering the same security in a one-to-one communication and more security in broadcast applications.

References

[1] G. Alvarez, L. Hernández Encinas, J. Muñoz Masqué, Known-plaintext attack to two cryptosystems based on the BB equation, IEEE Trans. Circuits Syst. II, Express Briefs 55 (5) (2008) 423–426.

[2] Rajorshi Biswas, Shibdas Bandyopadhyay, Anirban Banerjee, A fast implementation of the RSA algorithm using the GNU MP library, in: National Workshop on Cryptography, IIIT-Calcutta, 2003, pp. 1–15.

[3] Stefano Barbero, Umberto Cerruti, Nadir Murru, Generalized Rédei rational functions and rational approximations over conics, Int. J. Pure Appl. Math. 64 (2) (2010) 305–317.

[4] Stefano Barbero, Umberto Cerruti, Nadir Murru, Solving the Pell equation via Rédei rational functions, Fibonacci Q. 48 (4) (2010) 348–357.

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

[6] Don Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Cryptol. 10 (4) (1997) 233–260.

[7] N. Demytko, A new elliptic curve based analogue of RSA, in: Advances in Cryptology – EUROCRYPT'93, Springer, 1994, pp. 40–49.

[8] Shafi Goldwasser, Mihir Bellare, Lecture notes on cryptography, in: Summer Course "Cryptography and Computer Security" at MIT 1999, 1996, 1999.

[9] Marc Gysin, Jennifer Sebery, How to use Pell's equation in cryptography, preprint, 1999.

[10] Torbjörn Granlund, The GMP Development Team, GNU MP: the GNU Multiple Precision arithmetic library, 5.0.5 ed., http://gmplib.org/, 2012.

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

[12] Michael J. Jacobson, Hugh C. Williams, K. Taylor, Karl Dilcher, Solving the Pell Equation, Springer, 2009.

[13] P. Anuradha Kameswari, R. Chaya Kumari, Cryptosystems with Rédei rational function via Pell-conics, Int. J. Comput. Appl. 54 (15) (2012).

[14] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, Scott A. Vanstone, New public-key schemes based on elliptic curves over the ring Z_n, in: Advances in Cryptology – CRYPTO'91, Springer, 1992, pp. 252–266.

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

[16] Franz Lemmermeyer, Introduction to Cryptography, 2006.

[17] Arjen Lenstra, James P. Hughes, Maxime Augier, Joppe Willem Bos, Thorsten Kleinjung, Christophe Wachter, Ron was wrong, Whit is right, Tech. report, IACR, 2012.

[18] Aditya Mani Mishra, A digital signature scheme based on Pell equation, Int. J. Adv. Res. Sci. Eng. Technol. 1 (1) (2014).

[19] Winfried Muller, Rupert Nobauer, Cryptanalysis of the Dickson scheme, in: Advances in Cryptology, vol. 219, 1986, pp. 50–61.

[20] Willi More, Fast evaluation of Rédei functions, Appl. Algebra Eng. Commun. Comput. 6 (3) (1995) 171–173.

[21] N. Rama Murthy, M.N.S. Swamy, Cryptographic applications of Brahmagupta–Bhãskara equation, IEEE Trans. Circuits Syst. I, Regul. Pap. 53 (7) (2006) 1565–1571.

[22] Rupert Nobauer, Cryptanalysis of the Rédei scheme, Contrib. Gen. Algebra 3 (1984) 255–264.

[23] Sahadeo Padhye, A public key cryptosystem based on Pell equation, IACR Cryptol. ePrint Arch. 2006 (2006) 191.

[24] Kondala Rao, P.S. Avadhani, D. Lalitha Bhaskari, K.V.S.S.R.S.S. Sarma, An identity based encryption scheme based on Pell's equation with Jacobi symbol, Int. J. Appl. Sci. Eng. Res. 1 (2013) 17–20.

[25] Kondala Rao, P.S. Avadhani, D. LalithaBhaskari, Public key cryptosystem based on Pell's equation with Jacobi symbol, Int. J. Appl. Sci. Eng. Res. 4 (2015).

[26] László Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern, Acta Sci. Math. 11 (1946) 85–92.

[27] Deergha K. Rao, Ch. Gangadhar, VLSI realization of a secure cryptosystem for image encryption and decryption, in: 2011 International Conference on Communications and Signal Processing (ICCSP), IEEE, 2011, pp. 543–547.

[28] M. Kondala Rao, K.V.S.S.R.S. Sarma, P.S. Avadhani, D. Lalitha Bhaskari, A model on dynamic threshold multi-secret sharing scheme using Pell's equation with Jacobi symbol, in: 2013 Tenth International Conference on Information Technology: New Generations (ITNG), IEEE, 2013, pp. 773–776.

[29] K.V.S.S.R.S.S. Sarma, P.S. Avadhani, Public key cryptosystem based on Pell's equation using the Gnu Mp library, Int. J. Comput. Sci. Eng. 3 (2) (2011) 739–743.

[30] Kouichi Sakurai, Tsuyoshi Takagi, New semantically secure public-key cryptosystems from the RSA-primitive, in: Public Key Cryptography, vol. 2274, Springer, 2002, pp. 1–16.

[31] T. Chandra Segar, R. Vijayaragavan, Pell's RSA key generation and its security analysis, in: 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE, 2013, pp. 1–5.

[32] Anu Thomas, Manu Jose, VLSI realization of a secure cryptosystem based on BB equation, chaotic map and Arnold cat map, in: National Conference on Emerging Trends in VLSI, Embedded and Communication Systems, 2013.

[33] Oswald Veblen, John Wesley Young, Projective Geometry, vol. 1, Boston Ginn and Co., 1918.

[34] Michael J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inf. Theory 36 (3) (1990) 553–558.

[35] Andrew C. Yao, Theory and application of trapdoor functions, in: 23rd Annual Symposium on Foundations of Computer Science, 1982, SFCS'08, IEEE, 1982, pp. 80–91.

[36] Amr M. Youssef, A comment on "Cryptographic applications of Brahmagupta–Bhãskara equation", IEEE Trans. Circuits Syst. 54 (4) (2007) 927–928.