A novel RSA--like cryptosystem based on a generalization of Rédei rational functions

A novel RSA–like cryptosystem based on a generalization of the Rédei rational functions

Nadir Murru, Francesco M. Saettone

Department of Mathematics "G. Peano", University of Turin
Via Carlo Alberto 10, 10122, Torino, ITALY
nadir.murru@unito.it, francesco.saettone@edu.unito.it

Abstract. In this paper we present a novel RSA–like cryptosystem. Specifically, we define a novel product that arises from a cubic field connected to the cubic Pell equation. We discuss some interesting properties and remarks about this product that can also be evaluated through a generalization of the Rédei rational functions. We then exploit these results to construct a novel RSA–like scheme that is more secure than RSA in broadcast applications. Moreover, our scheme is robust against the Wiener attack and against other kind of attacks that exploit the knowledge of a linear relation occurring between two plaintexts.

Keywords: cubic Pell equation, Public cryptography, Rédei function, RSA.

1 Introduction

RSA cryptosystem is one of the most famous public key scheme and is based on the existence of an one–way trapdoor function, which is easy to compute and difficult to invert without knowing some information. However, some attacks are possible when, e.g., the private key is small [23] or the public key is small [5]. Further attacks have been reviewed in [11] exploiting possible extra information (such as the knowledge of linear relations occurring between two plaintexts). Moreover, RSA leaks some vulnerabilities in broadcast applications [9]. Hence, during the years, RSA–like schemes (see, e.g., [2] [6], [13], [15], [17]) have been proposed in order to overcome some of the previous vulnerabilities.

In this paper, we present a novel RSA–like scheme that is more secure than RSA in some of the previous situations, like broadcast scenarios or considering the Wiener attack and others. Our scheme is based on a particular group equipped with a non–standard product that we have found working on a cubic field related to the cubic Pell equation (which is a generalization of the Pell equation, one of the most famous equations in number theory). This group appears to have many interesting properties and connections that should be further investigated. In fact, we would like to point out that in this work we give a first idea about the potentiality of this group in cryptographic applications, with the aim of providing an original point of view for exploiting number theory in cryptography and opening new studies. Certainly, our scheme should be more

investigated under several perspectives, such as its efficiency. However, it appears very promising due to the definition itself and the many properties and connections to different topics.

The paper is structured as follows. In Section 2, we introduce a group with a non–standard product starting from a cubic field. Section 3 is devoted to the presentation of our cryptosystem and its discussion. Moreover, we see that powers with respect to our product can be evaluated by means of a generalization of the Rédei rational functions (Rédei rational functions are classical and very interesting functions in number theory). In section 4 we present the conclusion.

2 A product related to the cubic Pell equation

The Pell equation $x^2 - dy^2 = 1$, for d positive integer non–square and x, y unknowns, is one of the most famous Diophantine equations. Its generalization to the cubic case is given by the following equation:

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1 \tag{1}$$

where r is a given non–cubic integer and x, y, z unknown numbers whose values we are seeking over the integers. This equation is considered the more natural generalization of the Pell equation, since it arises considering the unitary elements of a cubic field as well as the Pell equation can be introduced considering unitary elements of a quadratic field. Specifically, let $(\mathbb{F}, +, \cdot)$ be a field and $t^3 - r$ an irreducible polynomial in $\mathbb{F}[t]$. Let us consider the quotient field $\mathbb{A} = \mathbb{F}[t]/(t^3 - r) = \{x + yt + zt^2 : x, y, z \in \mathbb{F}\}$. The quotient field $\mathbb{A}$ naturally induces a product between triples of elements of $\mathbb{F}$ as follows:

$$(x_1, y_1, z_1)\bullet(x_2, y_2, z_2) := (x_1x_2+(y_2z_1+y_1z_2)r, x_2y_1+x_1y_2+rz_1z_2, y_1y_2+x_2z_1+x_1z_2)$$

for $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{F}^3$ and the norm of an element is given by

$$N(x, y, z) := x^3 + ry^3 + r^2z^3 - 3rxyz,$$

see, e.g., [1], p.98. Considering the unitary elements we get the cubic Pell curve

$$\mathcal{C} = \{(x, y, z) \in \mathbb{F}^3 : x^3 + ry^3 + r^2z^3 - 3rxyz = 1\}.$$

In [4], Christofferson widely studied the more general equation

$$x^3 + rb^2y^3 + r^2bz^3 - 3rbxyz = c,$$

whose the cubic Pell equation is a particular case for $b = c = 1$ and r not a cube, providing also a complete bibliography up to 1956.

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

$$(\bar{x}, \bar{y}, \bar{z}) := (-x + ryz, rz^2 - xy, y^2 - xz).$$

Proof. The proof is straightforward and is left to the reader.

Remark 1. In $\mathbb{F}^3$ an element (x, y, z) is invertible with respect to $\bullet$ if and only if $N(x, y, z) \neq 0$ and its inverse is

$$\left(\frac{\bar{x}}{N(x,y,z)}, \frac{\bar{y}}{N(x,y,z)}, \frac{\bar{z}}{N(x,y,z)}\right).$$

Remark 2. When $\mathbb{F} = \mathbb{R}$, the cubic Pell curve $\mathcal{C}$ contains the solutions of the cubic Pell equation.

Remark 3. The Pell equation can be introduced considering the unitary elements of $\mathbb{R}[t]/(t^2 - d)$, d positive integer non–square, where the product between elements is

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + y_1x_2).$$

Starting from $\mathbb{A}$, we can introduce a new group with a non–standard product having interesting properties that can be also exploited for creating a novel RSA–like cryptosystem. Let us consider the quotient group $B := \mathbb{A}^*/\mathbb{F}^*$. An element in B is the equivalence class of elements in $\mathbb{A}^*$, i.e., $[m + nt + pt^2] \in B$ is the equivalence class of $m + nt + pt^2 \in \mathbb{A}^*$ defined by

$$[m + nt + pt^2] := \{\lambda m + \lambda nt + \lambda pt^2 : \lambda \in \mathbb{F}^*\}.$$

We can now rewrite the elements of B. Given $m + nt + pt^2 \in \mathbb{A}^*$, if $m \neq 0$ and $n = p = 0$, then

$$[m + nt + pt^2] = [m] = [1_{\mathbb{F}^*}].$$

If $n \neq 0$ and $p = 0$, then

$$[m + nt + pt^2] = [m + nt] = [m + t].$$

Finally, if $p \neq 0$, then

$$[m + nt + pt^2] = [m + nt + t^2].$$

Thus, the group B is

$$B = \{[m + nt + t^2] : m, n \in \mathbb{F}\} \cup \{[m + t] : m \in \mathbb{F}\} \cup \{[1_{\mathbb{F}^*}]\}.$$

Now, we can write the elements of B with a new notation. Fixed an element $\alpha \notin \mathbb{F}$, the elements of B can be written as couples of the kind (m, n), with $m, n \in \mathbb{F}$, or (m, α), with $m \in \mathbb{F}$, or (α, α). Hence the group B is

$$B = (\mathbb{F} \times \mathbb{F}) \cup (\mathbb{F} \times \{\alpha\}) \cup (\{\alpha\} \times \{\alpha\}).$$

With this new notation and remembering that $\mathbb{A} = \mathbb{F}[x]/(t^3 - r)$, we can obtain a commutative product $\odot$ in B, where (α, α) is the identity, having the following rules:

– $(m,\alpha)\odot(p,\alpha)=(mp,m+p)$

– $(m,n)\odot(p,\alpha)=\begin{cases}\left(\dfrac{mp+r}{n+p},\dfrac{m+np}{n+p}\right), & \text{if} \quad n+p\neq 0\\ \left(\dfrac{mp+r}{m-n^2},\alpha\right), & \text{if} \quad n=-p, m-n^2\neq 0\\ (\alpha,\alpha), & \text{otherwise}\end{cases}$

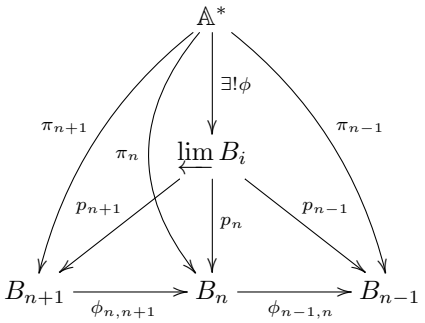
– $(m,n)\odot(p,q)=\begin{cases}\left(\dfrac{mp+(n+q)r}{m+p+nq},\dfrac{np+mq+r}{m+p+nq}\right), & \text{if} \quad m+p+nq\neq 0\\ \left(\dfrac{mp+(n+q)r}{np+mq+r},\alpha\right), & \text{if} \quad m+p+nq=0, np+mq+r\neq 0\\ (\alpha,\alpha), & \text{otherwise}\end{cases}$

As a consequence, the following proposition holds.

Proposition 2. *$(B,\odot)$ is a commutative group with identity (α,α). The inverse of an element (m,n), with $m-n^2\neq 0$, is $\left(\frac{nr-m^2}{m-n^2},\frac{r-mn}{m-n^2}\right)$. The inverse of an element (m^2,m) is $(-m,\alpha)$. Viceversa, the inverse of an element (m,α) is $(-m^2,m)$.*

Remark 4. When $\mathbb{F}=\mathbb{R}$, the element α can be viewed as ∞ and the points in B of the kind (m,∞), (∞,∞) as points at infinity.
Furthermore, if we consider $\mathbb{F}=\mathbb{Z}_p$ where p is prime, then we have a field, so $B=\mathbb{A}^*/\mathbb{F}^*=\mathbb{Z}_p^*[t]/\mathbb{Z}_p^*$ is a field too. It is easy to notice that the point $0=[0:0:0]\notin B$ and we can consider the equivalence relation $\sim$ induced by the action of $\mathbb{Z}_p^*$ on the set $\mathbb{Z}_p^*[t]$ such that $b_1\sim b_2 \iff \exists\lambda\in\mathbb{Z}_p^* : b_1=\lambda b_2$ and now it is clear that B is a projective space.

Remark 5. If $\mathbb{F}$ is not a finite field, let us denote B as B_0, $B_1=B_0^*/\mathbb{F}^*$, $B_n=B_{n-1}^*/\mathbb{F}^*$ and so $\forall n$, then we have $B_{n+1}\subset B_n$ and so we have a directed system, in fact $\forall n \quad B_n\subset B_0$; moreover let us consider the family of maps $\{\phi_{n,n+1}\}_n$ with $\phi_{n,n+1}:B_{n+1}\hookrightarrow B_n$, where $\phi_{n,n}=id_{B_n}$, such that $\phi_{n,n+1}\circ\phi_{n+1,m}=\phi_{n,m}$ and $\phi_{n,m}:B_m\hookrightarrow B_n$. At this point it is clear that $(\{B_n\},\phi_{n,n+1})$ is a projective system, hence we naturally consider the inverse limit $\varprojlim B_i$, that is equipped with a family of projection maps $\{p_n\}_n$ such that the inverse limit has the following universal property, showed by the commutative diagram



with $\pi_n \circ p_n^{-1} = id_{B_n}$

Remark 6. We consider $\mathbb{F}$ as a topological field, so that $\mathcal{C}$ has the topology induced as a subset of $\mathbb{F}^3$. The cubic Pell curve

$$\mathcal{C} = \{(x, y, z) \in \mathbb{F}^3 : N(x, y, z) := x^3 + ry^3 + r^2z^3 - 3rxyz = 1\},$$

endowed with the non standard product we have previously defined, can be studied as a topological group. Indeed the group operation

$$\mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}\ , ((x_1, y_1, z_1), (x_2, y_2, z_2)) \longmapsto (x_1x_2, y_1y_2, z_1z_2)$$

is a continuous mapping and the inversion map $\mathcal{C} \longrightarrow \mathcal{C},\ (x, y, z) \longmapsto (\bar{x}, \bar{y}, \bar{z})$ is likewise continuous, according to the fact that $N(x, y, z) = 1$. If $\mathbb{F} = \mathbb{R}$, then we can consider $\mathcal{C}$ equipped with the Euclidean topology, otherwise if $\mathbb{F} = \mathbb{Z}_p$, then the discrete topology is the most natural topology we can put on it, but maybe it is not the only one interesting, even if the only one that is T_0.

3 A public–key cryptosystem

3.1 The scheme

When $\mathbb{F} = \mathbb{Z}_p$ (and fixing $\alpha = \infty$), the situation is interesting for cryptographic applications. Indeed, in this case we have $\mathbb{A} = GF(p^3)$, i.e., $\mathbb{A}$ is the Galois field of order p^3. Thus, by construction, B is a cyclic group of order $\dfrac{p^3-1}{p-1} = p^2+p+1$, with respect to a well–defined product, and an analogous of the little Fermat's theorem holds:

$$(m, n)^{\odot p^2+p+1} \equiv (\infty, \infty) \pmod{p}, \tag{2}$$

where the power is evaluated by using the product $\odot$, for any $m \in \mathbb{Z}_p$ and $n \in \mathbb{Z}_p \cup \{\infty\}$.

Remark 7. It follows from (2) that

$$(m, n)^{\odot (p^2+p+1)(q^2+q+1)} \equiv (\infty, \infty) \pmod{N},$$

where $N = pq$, for p and q prime numbers. This does not mean that, when B is constructed over $\mathbb{Z}_N$, B is a group. In this case we only have an analogous of the Euler's theorem. In other words when we construct B over $\mathbb{Z}_p$ (p prime) our product $\odot$ works like the standard product in $\mathbb{Z}_p$. Moreover, when we consider B over $\mathbb{Z}_N$, our product $\odot$ works like the standard product in $\mathbb{Z}_N$.

As a consequence we can construct a public–key cryptosystem similar to the RSA scheme, but using our product $\odot$.

The following steps describe the keys generation:

– choose two prime numbers p, q

– compute $N = pq$
– choose an integer e such that $(e, (p^2+p+1)(q^2+q+1)) = 1$
– choose a non–cube integer r in $\mathbb{Z}_p$, $\mathbb{Z}_q$ and $\mathbb{Z}_N$
– compute d such that $ed \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)}$

The public encryption key is (N, e, r) and the secret decryption key is (p, q, d). Given a pair of messages m_1 and m_2 in $\mathbb{Z}_N$, they can be encrypted by

$$(c_1, c_2) \equiv (m_1, m_2)^{\odot e} \pmod{N}.$$

The receiver can decrypt the messages evaluating

$$(c_1, c_2)^{\odot d} \pmod{N}.$$

3.2 Some remarks

In the following, we discuss some peculiarities of our cryptosystem.

First, our scheme is more secure than RSA in broadcast scenarios, i.e., when the plaintext is encrypted for different receivers using the same public exponent and it is possible to recover the plaintext message by solving a set of congruences of polynomials [9]. However, this attack can not be applied when the trapdoor function is not a simple monomial power as in RSA [12]. Thus, this kind of attacks fails in our scheme.

Another classical attack against the RSA scheme is the Wiener attack [23]. Said e and d the public and private exponents, respectively, in the RSA scheme the following relation holds

$$ed - k\varphi(N) = 1$$

for a certain integer k, where φ is the Euler totient function and $N = pq$ (for p and q prime numbers) is the modulo with respect to messages are encrypted and decrypted. For large values of N the following bounds hold:

$$N - 3\sqrt{N} < \varphi(N) < N \tag{3}$$

The Wiener attack exploits properties of continued fractions. Indeed, thanks to the previous inequalities, we have

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{1}{2d^2},$$

i.e., by Legendre theorem, d is the denominator of a convergent of the continued fraction expansion of $\frac{e}{N}$ and consequently the private exponent d can be recovered. In our case, the role of $\varphi(N)$ is substituted by $(p^2+p+1)(q^2+q+1)$. This leads to a less efficient evaluation of the decryption exponent, however in this situation inequalities similar to (3) can not be found, making the Wiener attack not usable against our scheme. Moreover, for the same reason, further attacks exploiting continued fractions, reviewed in [7], fail in our case.

Remark 8. The private exponent d can be effectively recovered by using the Wiener attack if it is less than $N^{1/4}$, where N is the RSA–modulo. A typical size of the RSA–modulo is 1024–bit. Thus, in this case, it is required that the size of d must be at least 256 bits long in order to avoid the Wiener attack, but this is unfortunate for low–power devices [3]. Using the proposed scheme, the dimension of the private exponent could be less than 256 bits without being affected by the Wiener attack.

Finally, our scheme appears to be robust against another class of attack presented in [20] (see also [11], section 3.1, for a review of the attack). We recall this attack here for the reader. It is supposed that it is known a linear relation between two plaintexts M_1 and M_2:

$$M_2 = M_1 + \Delta$$

where Δ is known and $C_1 \equiv M_1^e \pmod N$, $C_2 \equiv M_2^e \pmod N$. In this case, the attack can retrieve the plaintext messages evaluating the greatest common divisor of the polynomials

$$x^e - C_1 \pmod N, \quad (x+\Delta)^e - C_2 \pmod N.$$

In our case, the situation is more complicated, since the exponentiation yields rational functions and not polynomials. Moreover, in our case, we deal with bivariate polynomials.

3.3 Evaluation of the powers with respect to $\odot$ by means of generalized Rédei functions

The Rédei rational functions were introduced by Rédei in [21] from the development of $(z+\sqrt{d})^n$, where z is an integer and d a non–square positive integer. We can define the Rédei polynomials $N_n(d,z)$ and $D_n(d,z)$ as follows:

$$(z+\sqrt{d})^n = N_n(d,z) + D_n(d,z)\sqrt{d}, \quad \forall n \geq 0.$$

The Rédei polynomials have the following closed form:

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

The Rédei rational functions are defined by

$$Q_n(d,z) = \frac{N_n(d,z)}{D_n(d,z)}, \quad \forall n \geq 1$$

and can be also evaluated by means of powers of matrices. Indeed, we have

$$\begin{pmatrix} z & d \\ 1 & z \end{pmatrix}^n = \begin{pmatrix} N_n & dD_n \\ D_n & N_n \end{pmatrix},$$

see [8].

They are classical and interesting functions in number theory since, for instance, they provide approximations of square roots, are permutations in finite fields and Rédei polynomials belong to the class of the Dickson polynomials [14]. Moreover, they have been applied in several contexts, like the creation of a cryptographic system based on the Dickson scheme [18] and the generation of pseudorandom sequences [22].

Here, we see that the powers of elements in B can be evaluated by means of a certain generalization to the cubic case of the Rédei functions.

Starting from the development of $(z_1 + z_2\sqrt[3]{r} + \sqrt[3]{r^2})^n$, with $z_1, z_2, r \in \mathbb{F}$ and r non–cube, we can introduce three sequences of polynomials $A_n(r, z_1, z_2)$, $B_n(r, z_1, z_2)$, $C_n(r, z_1, z_2)$ that generalize the Rédei polynomials. We define

$$(z_1+z_2\sqrt[3]{r}+\sqrt[3]{r^2})^n = A_n(r, z_1, z_2)+B_n(r, z_1, z_2)\sqrt[3]{r}+C_n(r, z_1, z_2)\sqrt[3]{r^2}, \quad \forall n \geq 0.$$

Hence, the rational functions $\dfrac{A_n}{C_n}$ and $\dfrac{B_n}{C_n}$, for $n \geq 1$ can be considered a generalization to the cubic case of the Rédei rational functions.

Remark 9. Let us observe that for introducing the generalized Rédei functions, it is not necessary to work in a field. Indeed, the previous definition works even in the case that z_1, z_2, r belongs to a commutative ring with identity. Indeed, the original Rédei polynomials were introduced in $\mathbb{Z}$. We have chosen to define the generalized Rédei polynomials in the field $\mathbb{F}$ only for being consistent with the notation used for introducing B as a group and not introducing new notation.

In the following proposition, we see that also the generalized Rédei polynomials can be evaluated by means of a matricial approach.

Proposition 3. *Let $A_n(r, z_1, z_2), B_n(r, z_1, z_2), C_n(r, z_1, z_2)$ be the generalized Rédei polynomials, then*

$$\begin{pmatrix} z_1 & r & rz_2 \\ z_2 & z_1 & r \\ 1 & z_2 & z_1 \end{pmatrix}^n = \begin{pmatrix} A_n & rC_n & rB_n \\ B_n & A_n & rC_n \\ C_n & B_n & A_n \end{pmatrix}, \quad \forall n \geq 0$$

Proof. In the following, for the seek of simplicity we omit the dependence on r, z_1, z_2. We prove the thesis by induction on n.
Basis: for $n = 0$ we have $A_0 = 1, B_0 = 0, C_0 = 0$ and $(z_1 + z_2\sqrt[3]{r} + \sqrt[3]{r^2})^0 = 1$, i.e.,

$$\begin{pmatrix} z_1 & r & rz_2 \\ z_2 & z_1 & r \\ 1 & z_2 & z_1 \end{pmatrix}^0 = \begin{pmatrix} A_0 & 0 & 0 \\ 0 & A_0 & 0 \\ 0 & 0 & A_0 \end{pmatrix}.$$

Similarly, it is straightforward to check the cases $n = 1, 2$.
Inductive step: we assume the statement holds for some natural number $n - 1$ and we prove that holds for n too. We have

$$\begin{pmatrix} z_1 & r & rz_2 \\ z_2 & z_1 & r \\ 1 & z_2 & z_1 \end{pmatrix}^n = \begin{pmatrix} z_1 & r & rz_2 \\ z_2 & z_1 & r \\ 1 & z_2 & z_1 \end{pmatrix}^{n-1} \begin{pmatrix} z_1 & r & rz_2 \\ z_2 & z_1 & r \\ 1 & z_2 & z_1 \end{pmatrix} =$$

$$= \begin{pmatrix} A_{n-1} & rC_{n-1} & rB_{n-1} \\ B_{n-1} & A_{n-1} & rC_{n-1} \\ C_{n-1} & B_{n-1} & A_{n-1} \end{pmatrix} \begin{pmatrix} z_1 & r & rz_2 \\ z_2 & z_1 & r \\ 1 & z_2 & z_1 \end{pmatrix}.$$

Thus, we have to show that

$$\begin{cases} A_n = z_1 A_{n-1} + r z_2 C_{n-1} + r B_{n-1} \\ B_n = z_1 B_{n-1} + z_2 A_{n-1} + r C_{n-1} \\ C_n = z_1 C_{n-1} + z_2 B_{n-1} + A_{n-1} \end{cases}.$$

By definition of generalized Rédei polynomials, we have

$$(z_1 + z_2 \sqrt[3]{r} + \sqrt[3]{r^2})^n = A_n + B_n \sqrt[3]{r} + C_n \sqrt[3]{r^2}.$$

On the other hand

$$(z_1 + z_2 \sqrt[3]{r} + \sqrt[3]{r^2})^n = (z_1 + z_2 \sqrt[3]{r} + \sqrt[3]{r^2})^{n-1}(z_1 + z_2 \sqrt[3]{r} + \sqrt[3]{r^2}) =$$

$$= (A_{n-1} + B_{n-1} \sqrt[3]{r} + C_{n-1} \sqrt[3]{r^2})(z_1 + z_2 \sqrt[3]{r} + \sqrt[3]{r^2})$$

from which, expanding the last product, the thesis easily follows.

In the next proposition, we see that these functions can be used in order to evaluate powers of elements (z_1, z_2) in B.

Proposition 4. *Given $(z_1, z_2) \in B$ and let $A_n(r, z_1, z_2), B_n(r, z_1, z_2), C_n(r, z_1, z_2)$ be the generalized Rédei polynomials, we have*

$$(z_1, z_2)^{\odot n} = \begin{cases} \left(\dfrac{A_n}{C_n}, \dfrac{B_n}{C_n} \right), & \text{if} \quad C_n \neq 0 \\ \left(\dfrac{A_n}{B_n}, \alpha \right), & \text{if} \quad B_n \neq 0,\ C_n = 0 \\ (\alpha, \alpha), & \text{if} \quad B_n = C_n = 0 \end{cases},$$

for $n \geq 1$.

Proof. By the previous proposition, we have

$$\begin{pmatrix} A_n & rC_n & rB_n \\ B_n & A_n & rC_n \\ C_n & B_n & A_n \end{pmatrix} \begin{pmatrix} A_m & rC_m & rB_m \\ B_m & A_m & rC_m \\ C_m & B_m & A_m \end{pmatrix} = \begin{pmatrix} A_{m+n} & rC_{m+n} & rB_{m+n} \\ B_{m+n} & A_{m+n} & rC_{m+n} \\ C_{m+n} & B_{m+n} & A_{m+n} \end{pmatrix},$$

from which we get

$$\begin{cases} A_{m+n} = A_m A_n + r B_m C_n + r B_n C_m \\ B_{m+n} = A_m B_n + A_n B_m + r C_m C_n \\ C_{m+n} = A_m B_n + B_m B_n + A_n C_m \end{cases}.$$

Thus, if $C_m, C_n \neq 0$ and $C_{m+n} = A_m B_n + B_m B_n + A_n C_m \neq 0$, i.e., $\frac{A_n}{C_n} + \frac{A_m}{C_m} + \frac{B_m B_n}{C_n C_m} \neq 0$ (that is the condition $m+p+nq \neq 0$ for the product $(m,n) \odot (p,q)$), we have

$$\begin{cases} \dfrac{A_{m+n}}{C_{m+n}} = \dfrac{\dfrac{A_n}{C_n}\dfrac{A_m}{C_m} + r\dfrac{B_m}{C_m} + r\dfrac{B_n}{C_n}}{\dfrac{A_m}{C_m} + \dfrac{B_n}{C_n}\dfrac{B_m}{C_m} + \dfrac{A_n}{C_n}} \\ \dfrac{B_{m+n}}{C_{m+n}} = \dfrac{\dfrac{B_n}{C_n}\dfrac{A_m}{C_m} + \dfrac{B_m}{C_m}\dfrac{A_n}{C_n} + r}{\dfrac{A_m}{C_m} + \dfrac{B_n}{C_n}\dfrac{B_m}{C_m} + \dfrac{A_n}{C_n}} \end{cases}$$

and this is equivalent to say that

$$\left(\frac{A_{m+n}}{C_{m+n}}, \frac{B_{m+n}}{C_{m+n}}\right) = \left(\frac{A_n}{C_n}, \frac{B_n}{C_n}\right) \odot \left(\frac{A_m}{C_m}, \frac{B_m}{C_m}\right).$$

In the case that $B_{m+n} \neq 0$ $C_{m+n} = A_m B_n + B_m B_n + A_n C_m = 0$, i.e., $\frac{A_n}{C_n} + \frac{A_m}{C_m} + \frac{B_m B_n}{C_n C_m} = 0$ (that is the condition $m+p+nq = 0$ for the product $(m,n) \odot (p,q)$), then we have

$$\left(\frac{A_{m+n}}{B_{m+n}}, \alpha\right) = \left(\frac{A_m}{C_m}, \frac{B_m}{C_m}\right) \odot \left(\frac{A_n}{C_n}, \frac{B_n}{C_n}\right).$$

Now, considering that $\left(\dfrac{A_1}{C_1}, \dfrac{B_1}{C_1}\right) = (z_1, z_2)$, the thesis follows.

When we consider elements of the kind (z, α) in B, the previous generalized Rédei functions can not be applied for evaluating the powers. However, in the following proposition, we see how these powers can be evaluated in a similar way.

Proposition 5. *Given $(z_1, \alpha) \in B$ and let $\bar{A}_n(r, z_1)$, $\bar{B}_n(r, z_1)$, $\bar{C}_n(r, z_1)$ be polynomials defined by*

$$(z_1 + \sqrt[3]{r})^n = \bar{A}_n(r, z_1) + \bar{A}_n(r, z_1)\sqrt[3]{r} + \bar{A}_n(r, z_1)\sqrt[3]{r^2}, \quad \forall n \geq 1.$$

We have that

1. $$\begin{pmatrix} z_1 & 0 & r \\ 1 & z_1 & 0 \\ 0 & 1 & z_1 \end{pmatrix}^n = \begin{pmatrix} \bar{A}_n & \bar{C}_n & r\bar{B}_n \\ \bar{B}_n & \bar{A}_n & \bar{C}_n \\ \bar{C}_n & \bar{B}_n & \bar{A}_n \end{pmatrix}, \quad \forall n \geq 0$$

2. $$(z_1, \alpha)^{\odot n} = \begin{cases} \left(\dfrac{\bar{A}_n}{\bar{C}_n}, \dfrac{\bar{B}_n}{\bar{C}_n}\right), & \text{if} \quad \bar{C}_n \neq 0 \\ \left(\dfrac{\bar{A}_n}{\bar{B}_n}, \alpha\right), & \text{if} \quad \bar{B}_n \neq 0,\ \bar{C}_n = 0 \\ (\alpha, \alpha), & \text{if} \quad \bar{B}_n = \bar{C}_n = 0 \end{cases}$$

Proof. The proofs are similar to proofs of Propositions 3 and 4 and are left to the reader.

Remark 10. As we have already pointed out, the generalized Rédei functions can be used for evaluating powers in B even in the case that we are working in a ring and not in the field $\mathbb{F}$. Let us note that in this case B is not a group but the product is well–defined and the powers can be evaluated by Propositions 4 and 5. In this case conditions "$\neq 0$" means "is invertible".

4 Conclusion

In this paper, we have proposed a novel RSA–like scheme that is more secure than RSA in broadcast applications and is not affected by the Wiener attack. Moreover, it appears more robust than RSA with respect to other attacks that exploit the knowledge of a linear relation occurring between two plaintexts. This scheme has been developed by using a new group equipped with a non–standard product whose powers can be evaluated by means of some generalized Rédei functions. This group and its product have shown many interesting properties and relations highlighting that they are worth investigating due to their perspectives. Certainly, in this work we have only given an idea of their use in cryptographic applications, but the present scheme should be further discussed and improved. In the following, we advise some further studies:

- In [16], the author exhibits an algorithm of complexity $O(log_2(n))$ with respect to addition, subtraction and multiplication to evaluate Rédei rational functions over a ring. It will be interesting to study a similar algorithm in order to obtain an efficient method for evaluating the generalized Rédei functions introduced in this paper, so that the encryption cost of our algorithm is equal to the encryption cost of the RSA scheme or less considering that in our scheme we encrypt two messages at once.
- We conjecture that $(B, \odot)$ and $(\mathcal{C}, \bullet)$ are isomorphic. Proving this fact and finding the isomorphism lead to important consequences. First, the isomorphism could be exploited in order to improve our scheme following the ideas of RSA–like schemes based on isomorphism between two groups (see, e.g., [12] and [19]). Moreover, in this way a method for generating the solutions of the cubic Pell equation could be found (note that such a method is still missing [1]). As a special case, we will also state that the number of solutions of the cubic Pell equation in $\mathbb{Z}_p$ is $p^2 + p + 1$ (as numerical simulations appear to confirm). One could try to show that $B \simeq \mathcal{C}$ using the Short Five Lemma [10]: if in the following diagram we have two exact sequences, that is $\ker g = \operatorname{Im} f$ and $\ker k = \operatorname{Im} h$, whew both k and g are surjections and both h and f are injections, under the hypothesis that two of the down arrows are isomorphism, then the last down arrow is an isomorphism too.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{f} & \mathbb{Z}_p[t]/(\beta(t)) & \xrightarrow{g} & \mathbb{A} & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow id & & \downarrow id & & \\ 0 & \longrightarrow & \mathcal{C} & \xrightarrow[h]{} & \mathbb{Z}_p[t]/(\beta(t)) & \xrightarrow[k]{} & \mathbb{A} & \longrightarrow & 0 \end{array}$$

So our goal is to find an appropriate $(\beta(t))$ and the maps previously introduced, with particular attention to the degree of the polynomial $(\beta(t))$. For now, we were only able to find the following morphism

$$\epsilon : \begin{cases} B \to \mathcal{C} \\ (m,n) \mapsto \left(\dfrac{m^3+6mnr+n^3r+r^2}{m^3+rn^3+r^2-3rmn}, \dfrac{3(m^2n+mr+n^2r)}{m^3+rn^3+r^2-3rmn}, \dfrac{3(m^2+mn^2+nr)}{m^3+rn^3+r^2-3rmn} \right) \\ (m,\alpha) \mapsto \left(1, \dfrac{3m^2}{m^3+r}, \dfrac{3m}{m^3+r} \right) \\ (\alpha,\alpha) \mapsto (1,0,0) \end{cases}$$

Moreover, let us recall that $\mathbb{Z}_p$ has non–cubic residues only when $p \equiv 1 \pmod 3$, and consequently 3 divides p^2+p+1. Thus, when we consider $\mathbb{F} = \mathbb{Z}_p$, we are able to construct the group B only for the prime numbers p such that p^2+p+1 is divisible by 3. Then we have observed that we have $|Im\epsilon| = \frac{|B|}{3}$.

– The scheme should be studied from a computational point of view, in order to give more precise and effective results about its efficiency and security. In this paper, we have only investigated some improvements regarding the security from a theoretical point of view.

References

1. E. J. Barbeau, Pell's equation, Springer, New York, 2003.
2. E. Bellini, N. Murru, An efficient and secure RSA-like cryptosystem exploiting Rdei rational functions over conics, Finite Fields and their Applications, Vol. 39, 179–194, 2016.
3. D. Boneh, Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc., Vol. 46, 203–213, 1999.
4. S. Christofferson, Über eine Klasse von kubischen diophantischen Gleichungen mit drei Unbekannten, Arkiv för Matematik, Vol. 3, No. 4, 355–364, 1957.
5. D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Cryptol., Vol. 10, No. 4, 233–260, 1997.
6. N. Demytko, A new elliptic curve based analogue of RSA, Eurocrypt 1993, LNCS 765, Springer-Verlag, 40–49, 1994.
7. A. Dujella, Continued fractions and RSA with small secret exponent, Tatra Mt. Math. Publ., Vol. 29, 101–112, 2004.

8. J. von zur Gathen, Tests for permutation polynomials, SIAM J. Comput., Vol. 20, 591–602, 1991.
9. J. Hastad, On using RSA with low exponent in a public key network, Advances in Cryptology, CRYPTO85 Proceedings, Springer, 403–408, 1986.
10. N. Jacobson, Basic Algebra II, W. H. Freeman and Company, San Francisco, 1989.
11. M. Joye, J. J. Quisquater, Protocol failure for RSA–like functions using Lucas sequences and elliptic curves, Lecture Notes in Computer Science, Vol. 1189, 93–100, 1997.
12. K. Koyama, Fast RSA–type schemes based on singular cubic curves $y^2 + axy \equiv$ (mod n), Advances in Cryptology, EUROCRYPT95, Springer, 329–340, 1995.
13. K. Koyama, U. M. Maurer, T. Okamoto, S. A. Vanstone, New public–key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, Advances in Cryptology, CRYPTO'91, Springer, 252–266, 1992.
14. R. Lidl, G. L. Mullen, G. Turnwald, Dickson polynomials, Pitman Monogr. Surveys Pure Appl. Math. 65, Longman, 1993.
15. J. H. Loxtou, D. S. P. Khoo, G. J. Bird, J. Seberry, A cubic RSA code equivalent to factorization, Journal of Cryptology, Vol. 5, No. 2, 139–150, 1992.
16. W. More, Fast evaluation on Rédei functions, Appl. Algebra Commun. Comput., VOl. 6, No. 3, 171–173, 1995.
17. D. Naccache, J. Stern, A new public–key cryptosystem, Eurocrypt 1997, LNCS 1233, Springer–Verlag, 27–36, 1998.
18. R. Nobauer, Cryptanalysis of the Rédei scheme, Contributions to General Algebra, Vol. 3, 255–264, 1984.
19. S. Padhye, A public key cryptosystem based on Pell equation, IACR Cryptol. ePrint Arch., 191, 2006.
20. J. Patarin, Some serious protocol failures for RSA with exponent e of less than 32 bits, CIRM Luminy, France, 25–29 Sept. 1995.
21. L. Rédei, Uber eindeuting umkehrbare polynome in endlichen korpen, Acta Sci. Math. (Szeged), Vol. 11, 85–92, 1946.
22. A. Topuzoglu, A. Winterhof, Topics in geometry, coding theory and cryptography, Algebra and Applications, Vol. 6, 135–166, 2006.
23. M. J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inform. Theory, Vol. 36, 553–558, 1990.