A novel RSA–like cryptosystem based on a product related to the cubic Pell equation and Rédei rational functions

Nadir Murru, Francesco M. Saettone

University of Torino, Department of Mathematics

27/10/2017

Public Key Cryptography – RSA scheme

- small private or public exponent $\Longrightarrow$ RSA scheme can be attacked

Public Key Cryptography – RSA scheme

- small private or public exponent $\implies$ RSA scheme can be attacked
- based on isomorphisms between two groups, (the set of points over a curve, usually a cubic or a conic)

RSA–like schemes, state of the art

- Pell analogue of RSA protocol, Lemmermeyer 2006

RSA–like schemes, state of the art

- Pell analogue of RSA protocol, Lemmermeyer 2006
- RSA–like scheme based on isomorphism between the Pell conic and $\mathbb{Z}_N^*$, Padhye et al. 2006–2013

$$m \mapsto \left(\frac{m^{-1} + m}{2}, \frac{m^{-1} - m}{2\sqrt{D}} \right)$$

RSA–like schemes, state of the art

- RSA–like scheme based on Brahamagupta–Bhaskara equation, Thomas et al. 2011–2013

RSA–like schemes, state of the art

- RSA–like scheme based on Brahamagupta–Bhaskara equation, Thomas et al. 2011–2013
- RSA type cryptosystem based on cubic curves, Koyama et al. 1995–2017

$$m \mapsto \left(\frac{a^2 m}{(m-1)^2}, \frac{a^3 m}{(m-1)^3} \right)$$

RSA–like schemes, state of the art

- RSA–like scheme based on the Pell conic (E. Bellini, N. Murru, Finite Fields and their Applications, 2016)

RSA–like schemes, state of the art

- RSA–like scheme based on the Pell conic (E. Bellini, N. Murru, Finite Fields and their Applications, 2016)
- Decryption operation two times faster than RSA

RSA–like schemes, state of the art

- Lowest number of modular inversions based on curves

$$m \mapsto \left(\frac{m^2 + D}{m^2 - D}, \frac{2m}{m^2 - D} \right)$$

RSA–like schemes, state of the art

- Lowest number of modular inversions based on curves

$$m \mapsto \left(\frac{m^2 + D}{m^2 - D}, \frac{2m}{m^2 - D} \right)$$

- Same security as RSA in a one–to–one communication and more security in broadcast applications

RSA–like scheme of higher order

- An RSA–like scheme based on the cubic Pell equation

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1$$

for r non–cubic integer

RSA–like scheme of higher order

- An RSA–like scheme based on the cubic Pell equation

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1$$

  for r non–cubic integer
- More security than RSA–like schemes

RSA–like scheme of higher order

- An RSA–like scheme based on the cubic Pell equation

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1$$

  for r non–cubic integer
- More security than RSA–like schemes
- New ideas for exploiting number theory in cryptography

RSA–like scheme of higher order

- An RSA–like scheme based on the cubic Pell equation

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1$$

  for r non–cubic integer
- More security than RSA–like schemes
- New ideas for exploiting number theory in cryptography
- Study the efficiency

A group over the cubic Pell surface

$\mathbb{F}$ field, the cubic Pell surface is

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

A group over the cubic Pell surface

$\mathbb{F}$ field, the cubic Pell surface is

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

Define the product

$$(x_1, y_1, z_1) \bullet (x_2, y_2, z_2) =$$

$$(x_1x_2 + (y_2z_1 + y_1z_2)r, x_2y_1 + x_1y_2 + rz_1z_2, y_1y_2 + x_2z_1 + x_1z_2)$$

A group over the cubic Pell surface

- $(\mathcal{C}, \bullet)$ is a group

A group over the cubic Pell surface

- $(\mathcal{C}, \bullet)$ is a group
- identity is $(1, 0, 0)$

A group over the cubic Pell surface

- $(\mathcal{C}, \bullet)$ is a group
- identity is $(1, 0, 0)$
- $(x, y, z)^{-1} = (-x + ryz, rz^2 - xy, y^2 - xz)$.

Consider $\mathbb{F}$ as a topological field $\implies$ $\mathcal{C}$ as the topology induced as a subset of $\mathbb{F}^3$.

Consider $\mathbb{F}$ as a topological field $\implies$ $\mathcal{C}$ as the topology induced as a subset of $\mathbb{F}^3$.

The cubic Pell curve $\mathcal{C}$, i.e.,

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

endowed with $\bullet$, can be studied as a topological group.

- $\mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$,

$$((x_1, y_1, z_1), (x_2, y_2, z_2)) \longmapsto (x_1 x_2, y_1 y_2, z_1 z_2)$$

is a continuous mapping

- $\mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$,

$$((x_1, y_1, z_1), (x_2, y_2, z_2)) \longmapsto (x_1 x_2, y_1 y_2, z_1 z_2)$$

  is a continuous mapping
- 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 $N(x, y, z) = 1$.

- $\mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$,

$$((x_1, y_1, z_1), (x_2, y_2, z_2)) \longmapsto (x_1 x_2, y_1 y_2, z_1 z_2)$$

  is a continuous mapping
- 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 $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$, the discrete one.

A parametrization group

- $\mathbb{A} = \mathbb{F}[t]/(t^3 - r)$

A parametrization group

- $\mathbb{A} = \mathbb{F}[t]/(t^3 - r)$
- $B := \mathbb{A}^*/\mathbb{F}^*$ whose elements are the equivalence class of $m + nt + pt^2 \in \mathbb{A}^*$, i.e.,

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

A parametrization group

The group B can be rewritten as

A parametrization group

The group B can be rewritten as

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

A parametrization group

The group B can be rewritten as

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

Fixed $\alpha \notin \mathbb{F}$, the elements of B can be written as

A parametrization group

The group B can be rewritten as

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

Fixed $\alpha \notin \mathbb{F}$, the elements of B can be written as

- (m, n), with $m, n \in \mathbb{F}$

A parametrization group

The group B can be rewritten as

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

Fixed $\alpha \notin \mathbb{F}$, the elements of B can be written as

- (m, n), with $m, n \in \mathbb{F}$
- (m, α), with $m \in \mathbb{F}$

A parametrization group

The group B can be rewritten as

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

Fixed $\alpha \notin \mathbb{F}$, the elements of B can be written as

- (m, n), with $m, n \in \mathbb{F}$
- (m, α), with $m \in \mathbb{F}$
- (α, α).

A parametrization group

The group B can be rewritten as

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

Fixed $\alpha \notin \mathbb{F}$, the elements of B can be written as

- (m, n), with $m, n \in \mathbb{F}$
- (m, α), with $m \in \mathbb{F}$
- (α, α).

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

An operation over B

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

An operation over B

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

An operation over B

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

Some properties of B

Proposition 1

$(B, \odot)$ *is a commutative group with identity* (α, α).

Some properties of B

Proposition 1

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

Some properties of B

Proposition 1

$(B, \odot)$ 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 $(-m, \alpha)$.

Some properties of B

Proposition 1

$(B, \odot)$ 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 $(-m^2, m)$.

Some properties of B

When $\mathbb{F} = \mathbb{Z}_p$ (and fixing $\alpha = \infty$), we have

- $\mathbb{A} = GF(p^3)$, i.e., $\mathbb{A}$ is the Galois field of order p^3.

Some properties of B

When $\mathbb{F} = \mathbb{Z}_p$ (and fixing $\alpha = \infty$), we have

- $\mathbb{A} = GF(p^3)$, i.e., $\mathbb{A}$ is the Galois field of order p^3.
- B is a cyclic group of order $\frac{p^3 - 1}{p - 1} = p^2 + p + 1$, with respect to a well–defined product

Some properties of B

When $\mathbb{F} = \mathbb{Z}_p$ (and fixing $\alpha = \infty$), we have

- $\mathbb{A} = GF(p^3)$, i.e., $\mathbb{A}$ is the Galois field of order p^3.
- B is a cyclic group of order $\dfrac{p^3 - 1}{p - 1} = p^2 + p + 1$, with respect to a well–defined product
- an analogous of the little Fermat's theorem holds:

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

The cryptographic scheme

The following steps describe the keys generation:

The cryptographic scheme

The following steps describe the keys generation:

- choose two prime numbers p, q

The cryptographic scheme

The following steps describe the keys generation:

- choose two prime numbers p, q
- compute $N = pq$

The cryptographic scheme

The following steps describe the keys generation:

- choose two prime numbers p, q
- compute $N = pq$
- choose an integer e such that $(e, (p^2 + p + 1)(q^2 + q + 1)) = 1$

The cryptographic scheme

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 $\mathbb{Z}_p$ and $\mathbb{Z}_q$

The cryptographic scheme

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 $\mathbb{Z}_p$ and $\mathbb{Z}_q$
- compute d: $ed \equiv 1 \bmod (p^2 + p + 1)(q^2 + q + 1)$

The cryptographic scheme

The public encryption key is (N, e, r).

The cryptographic scheme

The public encryption key is (N, e, r).

The secret decryption key is (p, q, d).

The cryptographic scheme

The public encryption key is (N, e, r).

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

The cryptographic scheme

The public encryption key is (N, e, r).

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

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

The cryptographic scheme

The public encryption key is (N, e, r).

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

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

The receiver can decrypt the messages evaluating

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

Security

If a linear relation between two plaintexts M_1 and M_2 is known, i.e.,

$$M_2 = M_1 + \Delta$$

Security

If a linear relation between two plaintexts M_1 and M_2 is known, i.e.,

$$M_2 = M_1 + \Delta$$

where Δ is known, then the attacker can retrieve the plaintext messages evaluating the g.c.d. of the polynomials

Security

If a linear relation between two plaintexts M_1 and M_2 is known, i.e.,

$$M_2 = M_1 + \Delta$$

where Δ is known, then the attacker can retrieve the plaintext messages evaluating the g.c.d. of the polynomials

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

Security

In our case, the situation is more complicated, since the exponentiation yields rational functions and not polynomials.

Security

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.

Rédei rational functions

They arise from the development of

$$(z+\sqrt{d})^n = N_n(d,z) + D_n(d,z)\sqrt{d},$$

Rédei rational functions

They arise from the development of

$$(z+\sqrt{d})^n = N_n(d,z) + D_n(d,z)\sqrt{d},$$

$\forall z \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{Z}$ non–square.

Rédei rational functions

They arise from the development of

$$(z+\sqrt{d})^n = N_n(d,z) + D_n(d,z)\sqrt{d},$$

$\forall z \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{Z}$ non–square.

We have

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

Rédei rational functions

They arise from the development of

$$(z+\sqrt{d})^n = N_n(d,z) + D_n(d,z)\sqrt{d},$$

$\forall z \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{Z}$ non–square.

We have

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

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

Rédei rational functions

Definition 1

The Rédei rational functions are defined as

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

Generalized Rédei functions

Let $r \in \mathbb{F}$ be a non–cubic element.

Generalized Rédei functions

Let $r \in \mathbb{F}$ be a non–cubic element.

Let us consider

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

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

Generalized Rédei functions

Let $r \in \mathbb{F}$ be a non–cubic element.

Let us consider

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

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

$\forall n \geq 0$, for $z_1, z_2 \in \mathbb{F} \setminus \{0\}$

Generalized Rédei functions and powers

The functions

$$\frac{A_n}{C_n}, \quad \frac{B_n}{C_n}$$

are the Rédei functions generalized to the cubic case.

Generalized Rédei functions and powers

The functions

$$\frac{A_n}{C_n}, \quad \frac{B_n}{C_n}$$

are the Rédei functions generalized to the cubic case. We have

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

Proposition 2

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,*

Proposition 2

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*

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

Future work

There exists an algorithm of complexity $O(log_2(n))$ with respect to addition, subtraction and multiplication to evaluate Rédei rational functions over a ring.

Future work

There exists 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.

We conjecture that $(B, \odot) \simeq (\mathcal{C}, \bullet)$.

We conjecture that $(B, \odot) \simeq (\mathcal{C}, \bullet)$.

- the isomorphism could be exploited in order to improve our scheme following the ideas of RSA–like schemes.

We conjecture that $(B, \odot) \simeq (\mathcal{C}, \bullet)$.

- the isomorphism could be exploited in order to improve our scheme following the ideas of RSA–like schemes.
- a method for generating the solutions of the cubic Pell equation could be found (note that such a method is still missing).

We conjecture that $(B, \odot) \simeq (\mathcal{C}, \bullet)$.

- the isomorphism could be exploited in order to improve our scheme following the ideas of RSA–like schemes.
- a method for generating the solutions of the cubic Pell equation could be found (note that such a method is still missing).
- we state that the number of solutions of the cubic Pell equation in $\mathbb{Z}_p$ is $p^2 + p + 1$.

Bibliography

- E. J. Barbeau, Pell's equation, Springer, New York, 2003.
- E. Bellini, N. Murru, *An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics*, Finite Fields and their Applications, Vol. **39**, 179–194, 2016.

K. Koyama, Fast RSA–type schemes based on singular cubic curves $y^2 + axy \equiv \pmod{n}$, Advances in Cryptology, EUROCRYPT95, Springer, 329–340, 1995.

R. Lidl, G. L. Mullen, G. Turnwald, Dickson polynomials, Pitman Monogr. Surveys Pure Appl. Math. 65, Longman, 1993.

S. Padhye, A public key cryptosystem based on Pell equation, IACR Cryptol. ePrint Arch., 191, 2006.

Conclusion


I NEVER REALIZED HOW GOOD IT FEELS TO STRETCH OUT AND NOT THINK ABOUT ANYTHING!
CP 8 (C) DISNEY