Cryptosystems with Rédei Rational Function *via* Pellconics

P. Anuradha Kameswari
Department Of Mathematics
Andhra University
Visakhapatnam-530003
Andhra Pradesh

R. Chaya Kumari
Department Of Mathematics
Andhra University
Visakhapatnam-530003
Andhra Pradesh

ABSTRACT

In this paper, two cryptosystems are constructed using the fact that Rédei rational functions are permutation polynomials and exploiting the multiplicative properties of Rédei rational functions and the inverse property of Dickson polynomial extended to Rédei rational functions. The encryptions are based on evaluating Rédei rational functions $Q_k(d,z) \in \not{C}_n$ with the values $z \in \not{C}_n$ connected to the solutions of the Pell's equation $x^2 - dy^2 = 1$ in $\not{C}_n$. The connection between these evaluations and the convergents of solutions of Pell's equation are used in the construction of the second cryptosystem.

KEYWORDS: Pell conics, Redei Rational function, Permutation Polynomial, Cryptosystem.

1. INTRODUCTION

The equation $x^2 - dy^2 = N$ with given integers d and N and unknowns x and y is called Pell's equation. If d is negative or perfect square the equation has only finitely many solutions and the most interesting case is when d is positive and non perfect square the equation has infinitely many solutions as in [7]. The study of solutions of Pell equation connected to Rédei rational functions is in [14]. There are various studies made on these solutions and the analysis of these solutions and their applications to cryptography has gained importance. In this paper, we construct a cryptosystem with Rédei rational functions [5] and Pell conics by evaluating Rédei rational functions $Q_k(d,z)$ in $\not{C}_n$ for z connected to (x,y), a solution of some Pell equation over $\not{C}_n$.

The set of all solutions of the Pell's equation in a domain R is denoted by $\mathrm{P}(\mathrm{R})$ and is given as

$$\mathrm{P}(\mathrm{R}) = \{(x,y) \in \mathrm{R} \times \mathrm{R} \ / x^2 - dy^2 = N \ \}$$

Let p be an odd prime and d be a non-square positive integer i.e. a non-zero quadratic residue element in F_p, and let $\mathrm{P}(\mathrm{F}_p)$ denote the set of all solutions of the Pell's equation in F_p, given as

$$\mathrm{P}(\mathrm{F}_p) = \{(x,y) \in \mathrm{F}_p \times \mathrm{F}_p \ / x^2 - dy^2 = 1\}.$$

The point $N = (1,0) \in \mathrm{P}(\mathrm{F}_p)$ is called the neutral point and the lines through neutral point N = (1, 0) will intersect the Pell conic in exactly two different points i.e., in N and in another point P_m depending on the slope m of the line. For the lines through (1, 0) with slope m, (except the line x = 1), the point of intersection P_m is

$$P_m = \left(\frac{dm^2+1}{dm^2-1}, \frac{2m}{dm^2-1}\right)$$

This is the parametrization of m on $\mathrm{P}(\mathrm{F}_p)$ and group laws on $\mathrm{P}(R)$, R an arbitrary ring in [8] are used for the construction of the cryptosystem with Rédei rational functions. In this context, basic concepts of Rédei rational functions and some of its properties are introduced in section 2. Using the theory on permutation polynomials by Müller and Nöbauer in [15], the description of Rédei rational functions as permutation polynomials is given in section 3. In section 4, the construction of the proposed cryptosystem is described.

2. RÉDEI RATIONAL FUNCTIONS

DEFINITION 1: Let $d \neq 0$ be a non-square positive integer. The Rédei rational functions are developed from $(z + \sqrt{d})^n$ for the non perfect square positive integer d by taking the expression

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

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

and

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

Then the Rédei rational functions denoted by $Q_n(d,z)$ are defined as

$$Q_n(d,z)=\frac{N_n(d,z)}{D_n(d,z)} \ \forall n\geq 1, n\in \not\subset$$

DEFINITION 2: For any positive real number d, define the transform $\rho_d : ¡^{\infty} \to ¡^{\infty}$ given as $\rho_d(x)=\frac{x+1}{x-1}\sqrt{d}$ and ρ_d is such that $\rho_d(1)=\infty, \rho_d(0)=-\sqrt{d}, \rho_d(\infty)=\sqrt{d}$ with inverse given as $\rho_d^{-1}(x)=\frac{x+\sqrt{d}}{x-\sqrt{d}}$ and ρ_d induces the product e_d, over $¡^{\infty}$ is given as:

$$x \, e_d \, y=\rho_d(\rho_d^{-1}(x)\rho_d^{-1}(y))=\frac{d+xy}{x+y}$$

Remark 1: Comparing e_d with the usual product over ¡, $\sqrt{d}$ plays the role of ∞ and $-\sqrt{d}$ plays the role of 0, by using the relations for all $x \in ¡^{\infty}$.

From the following proposition, the product e_d on Rédei rational functions satisfy commutative property.

PROPOSITION 1: The product e_d on Rédei rational function satisfies $Q_n(d,z) \, e_d \, Q_m(d,z)=Q_{n+m}(d,z)$ $\forall m,n\geq 1; m,n\in \not\subset$.

PROOF: By definition of the product e_d on Rédei rational functions we have

$$Q_n(d,z) \, e_d \, Q_m(d,z) = \frac{d+Q_nQ_m}{Q_n+Q_m}$$

$$=\frac{d+\frac{N_n}{D_n}\frac{N_m}{D_m}}{\frac{N_n}{D_n}+\frac{N_m}{D_m}}$$

$$=\frac{N_nN_m+dD_nD_m}{N_nD_m+N_mD_n}$$

$$=\frac{N_{n+m}}{D_{n+m}}$$

$$=Q_{n+m}$$

LEMMA 1: If $z^n \, e_d = z \, e_d \, z \, e_d \ldots z \, e_d$ is the n^{th} power of z with respect to the product e_d then $z^n \, e_d = Q_n(d,z).$

Proof: We have for n = 1

$$(z+\sqrt{d})^1 = N_1(d,z)+D_1(d,z)\sqrt{d}$$

$$Q_1(d,z)=\frac{N_1(d,z)}{D_1(d,z)}=z$$

$$\Rightarrow z^n \, e_d = z \, e_d \, z \, e_d \ldots z$$

$$= Q_1(d,z) \, e_d \, Q_1(d,z) \, e_d \ldots Q_1(d,z)$$

$$= Q_{1+\ldots+1}(d,z) \quad \text{(by the proposition)}$$

$$= Q_n(d,z).$$

THEOREM 1: Rédei Rational functions satisfy the multiplicative property $Q_{nm}(d,z)=Q_n(d,Q_m(d,z))$ *for* $m,n\in \not\subset$.

Proof: By above lemma as each z^n equals $Q_n(d,z)$ we have

$$Q_n(d,Q_m(d,z)) = Q_m(d,z)^n \, e \, d$$

$$= (z^m \, e_d)^n \, e_d$$

$$= z^{nm} \, e_d$$

$$= z^n \, e_d \, z^n \, e_d \ldots z^n \, e_d$$

$$= Q_{nm}(d,z)$$

Therefore $Q_n(d,Q_m(d,z)) = Q_{nm}(d,z).$

3 RÉDEI RATIONAL FUNCTIONS AS PERMUTATION POLYNOMIALS

For encryptions of a message m in $\not\subset_n$ we need bijections of

$\not{c}_n$ that are trapdoor functions. Trapdoor functions may be obtained by using permutation polynomials modulo n, where permutation polynomials are the polynomials $P(x)$ which induce a permutation Π of $\not{c}_n$ on substitution of elements of $\not{c}_n$ in $P(x)$ i.e., $\Pi : \not{c}_n \to \not{c}_n$ given as $\Pi(\alpha) = P(\alpha)$ is a permutation on $\not{c}_n$. For the polynomial $P_k(x) = x^k$, a polynomial in one variable $\Pi_k : \not{c}_n \to \not{c}_n$ given as $\Pi_k(\alpha) = P_k(\alpha) = \alpha^k$ is a permutation whenever $gcd(k, \varphi(n)) = 1$. The study of necessary and sufficient conditions for other polynomials to be permutation polynomials and the classification of permutation polynomials [5] was generated with the initiation made by Nöbauer and Müller for Dickson polynomials. RSA cryptosystem is based on the permutations on $\not{c}_n$ induced by the polynomials x^k for gcd(k, $\varphi(n)$) = 1. Müller and Lidl [12] suggested the replacement of polynomial $P_k(x) = x^k$ by the Dickson polynomials $g_k(a, x)$ in constructing the RSA type cryptosystem. The Dickson polynomials are the polynomials defined as

$$g_k(a,x) = \sum_{i=0}^{[k/2]} \frac{k}{k-i} \binom{k-i}{i} (-a)^i x^{k-2i}$$

for $a = \pm 1$ with some properties given as:

- The polynomials $g_k(a, x)$ also satisfies $g_k(a,x) \circ g_n(a,x) = g_{kn}(a,x)$
- For $a = 1$, there is a simple recurrence relation, for generating these polynomials $g_{k+2} - xg_{k+1} + g_k = 0; g_0 = 2; g_1 = x$

In [12] Müller and Lidl established that Dickson polynomials are permutation polynomials if and only if gcd($k, \nu(n)$) = 1, where $\nu(n) = (p^2 - 1q^2 - 1)$. In particular, for $m = pq$, p and q are prime that is a Dickson polynomial $g_k(a, x)$ induces a permutation if and only if $(k, (p^2 - 1)(q^2 - 1))$ = 1. Also, $g_n(a, x)$ is the inverse of $g_k(a, x)$ if and only if $kn \equiv 1 mod((p^2 - 1)(q^2 - 1))$. Now consider the two theorems by Nöbauer in [11], [6] as follows:

THEOREM 2: If $n = ab$, $\frac{g(x)}{h(x)}$ is a permutation function modulo n if and only if $\frac{g(x)}{h(x)}$ is a permutation function modulo a and $\frac{g(x)}{h(x)}$ is a permutation function modulo b.

THEORE M 3: $\frac{g(x)}{h(x)}$ is a permutation function modulo p^e whenever $\frac{g(x)}{h(x)}$ is a permutation function modulo p $h(r)g'(r) - g(r)h'(r) \not\equiv 0 \mod p$. In particular, $g(x)$ is a permutation polynomial modulo p^e whenever $g'(r) \not\equiv 0 \mod p.$

REMARK 2: Let $R_k(x) = \frac{g_k(x)}{h_k(x)}$ be a quotient of polynomials over $\not{c}$ where $g_k(x)$ and $h_k(x)$ are relatively prime in $\not{c}[x]$.

It is assumed that $\infty = \frac{1}{0}; \Rightarrow 0 = \frac{1}{\infty}$

$\infty + b = \infty; for b \in \not{c}_m$; $b\infty = \infty; for b \neq 0$.

If the quantities $R_k(b)$ are distinct for all $b \in \not{c}_n \cup \{\infty\}$. Then $R_k(x)$ is called a permutation function for $\not{c}_n \cup \{\infty\}$.

REMARK 3: Moreover, a rational function $R_k(x)$ is a permutation function for $\not{c}_n \cup \{\infty\}$ and for $\not{c}_n$ if and only if the degree of the numerator is greater than the degree of the denominator of $R_k(x)$.

In [12] Müller and Lidl also established that Rédei rational functions are permutation polynomials by the fact that the quotients of Rédei rational functions are Dickson polynomials. Applying the above theorems and remark 3 it is observed that $Q_k(x)$, a Rédei rational function is a permutation polynomial with necessary and sufficient conditions as that of Dickson polynomial $g_k(x)$. In particular we exploit the inverse property of Dickson extended

to Rédei rational functions in construction of cryptosystems in the following section.

4. CRYPTOSYSTEMS WITH RÉDEI RATIONAL FUNCTIONS *VIA* PELLCONICS

In this section, two public key cryptosystems are constructed that are based on Rédei rational functions on elements in a finite ring that are connected to the solutions of Pell's equation. The properties of Rédei rational functions given as in section 2 and the inverse property of Dickson polynomial extended to Rédei rational functions are exploited in the constructions of following crypto-systems.

ENCRYPTION:

- Let m be the plain text message in $\not\subset_n$ and $n = pq$ with $gcd(m,n) = 1$.
- Choose the Pell's equation $x^2 - dy^2 = 1(modn)$ with d, a non perfect square modulo n and make it public.
- Compute $\nu(n) = (p^2 - 1q^2 - 1)$ and choose an integer k such that $1 \le k \le \nu(n)$, with gcd $(k, \nu(n)) = 1$ and t be the integer such that $kt \equiv 1 mod(\nu(n))$, then k is an encryption key which is made public and t is the decryption key that is kept secret.
- Compute the point $P_m = (x_m, y_m)(modn)$, the parametrization of m which is a solution of Pell's equation $x^2 - dy^2 = 1(modn)$
- Choose a function $f : \mathrm{P}(\not\subset_n) \to \not\subset_n$ and evaluate $f(x_m, y_m)(modn).$
- Compute $C_m = Q_k(d, f(P_m))$, the Rédei rational functions evaluated at f for d.
- Send the cipher text message C_m to the receiver R.
- $(n, d, f(x,y), C_m)$ is the public key.

DECRYPTION:

- Evaluate $f(P_m) = f(x_m, y_m)$ from the cipher text message C_m as follows:
- For the secret key t with $kt \equiv 1(mod\nu(n)),$

$$Q_t(d, C_m) = Q_t(d, Q_k(d, f(P_m)))$$

$$= Q_{kt}(d, f(P_m))$$

$$= Q_1(d, f(P_m)) \text{ by inverse property}$$

$$Q_n \equiv Q_m \text{ iff } n \equiv m \bmod \nu(n)$$

$$\equiv f(P_m)$$

$$\equiv f(x_m, y_m)(modn)$$

- Evaluate $P_m = (x_m, y_m)$ by solving the equations

$$x_m^2 - dy_m^2 = 1(\text{mod } n) \text{ and}$$
$$f(x_m, y_m) = f(P_m)(\text{mod } n)$$

- Retrieve the message m from P_m, the parametrization of m on the Pell conic $x^2 - dy^2 = 1(modn)$ by solving $(x_m, y_m) = P_m = (\frac{dm^2+1}{dm^2-1}, \frac{2m}{dm^2-1}).$

EXAMPLE 1:

Take $p = 5$ and $q = 7$, $n = pq = 35$ and $m = 13$ and for $d = 17$ take the Pell's equation $x^2 - 17y^2 = 1(mod35)$. Now for $\nu(n) = \nu(35) = 1152$ we may choose k = 5, as the encryption key for which t = 461, is the decryption key. By the parametrization of m on the Pell conic we have $(x_m, y_m) = P_m = (2,13)$ and for the function $f(x,y) = \frac{1+x}{y}$ we have $f(P_m) = f(2,13) = 11(mod35)$ then the cipher text $C_m = Q_k(d, f(P_m))$ is evaluated as:

$$Q_k(d, f(P_m)) = Q_5(17,11)$$
$$= Q_1(17,11) \, e_d \, Q_1(17,11) \, e_d \, Q_1(17,11)$$
$$e_d \, Q_1(17,11) \, e_d \, Q_1(17,11)$$
$$= 34.$$

Now for the decryption of the cipher text, with the public key and the decryption key t = 461, $f(P_m)$ mod n is evaluated as:

$$f(P_m) \equiv Q_{461}(17,34) mod 35 \equiv 11 mod 35.$$

Now solving the equations

$$x_m^2 - 17y_m^2 = 1(mod35) and f(x_m, y_m) = 11(mod35).$$

We have $P_m = (x_m, y_m) = (2,13)$, then the parametrization of m on the Pell conic gives

$(2,13) = P_m = (\frac{17m^2+1}{17m^2-1}, \frac{2m}{17m^2-1})$ from which we retrieve the message m as m = 13.

In this section, the relations between Rédei rational functions and solutions of Pell's equation are studied in [14] to construct another public key cryptosystem by exploiting the properties of Rédei rational functions on $\not\subset_n$ by using the following lemma.

LEMMA 2: For any solution (x_1, y_1) of Pell's equation satisfying $x_1^2 - dy_1^2 = 1$ we have

$$Q_{2n}\left(d, \frac{x_1+1}{y_1}\right) = \frac{x_n}{y_n}$$

ENCRYPTION:

- Let m be the plain text message in $\not\subset_n$ and $n = pq$ with $gcd(m,n) = 1$.
- Let e be an integer such that $1 \le e \le \varphi(n)$ with $gcd(e, \varphi(n)) = 1$ and e is made public.
- Consider the Pell's equation $x^2 - dy^2 = 1(modn)$ with d, such that $ed \equiv 1 mod(\varphi(n))$ e is chosen such that d is a non perfect square modulo n.
- Compute $\nu(n) = (p^2 - 1q^2 - 1)$ and choose an integer k such that $1 \le k \le \nu(n)$, with gcd $(k, \nu(n)) = 1$ and t be the integer such that $kt \equiv 1 mod(\nu(n))$, then k is an encryption key which is made public and t is the decryption key that is kept secret.
- Compute the point $P_m = (x_m, y_m)(modn)$, the parametrization of m which is a solution of Pell's equation $x^2 - dy^2 = 1(modn)$
- Compute $C_m = Q_{2k}(d, \frac{1+x_m}{y_m})$, the Rédei rational function evaluated at $\frac{1+x_m}{y_m}$ for d.
- Send the cipher text message C_m to the receiver R.
- (n, e, C_m) is the public key.

DECRYPTION:

- Evaluate (x_m, y_m) from the cipher text message C_m as follows:
  First find the value

$$u_m = Q_t(d, c_m)$$

Next note

$$Q_t(d, C_m) = Q_t(d, Q_{2k}(d, \frac{1+x_m}{y_m}))$$

$$= Q_{2kt}(d, \frac{1+x_m}{y_m})$$

$$= Q_2(d, \frac{1+x_m}{y_m})$$

$$= \frac{x_m}{y_m}(modn) by [14]$$

by the inverse property $Q_n \equiv Q_m$ iff $n \equiv m mod\, \nu(n)$

Therefore we have

$$\frac{x_m}{y_m} = u_m(modn)$$

- Evaluate $P_m = (x_m, y_m)$ by solving the equations

$$x_m^2 - dy_m^2 = 1(modn)$$

$$x_m y_m^{-1} = u_m(modn).$$

retrieve the message m from P_m, the parametrization of m on the Pell conic $x^2 - dy^2 = 1(modn)$ by solving

$$(x_m, y_m) = P_m = (\frac{dm^2+1}{dm^2-1}, \frac{2m}{dm^2-1}).$$

EXAMPLE 2:

Take $p = 5$ and $q = 7$, $n = pq = 35$ and $m = 13$ and take $e = 17$ be an integer such that $1 \le 17 \le 24)$ with $gcd(17, 24) = 1$ and $e = 17$ is made public. Take

$d = 17$ such that $17.17 \equiv 1 mod(24)$ and consider the Pell's equation $x^2 - 17y^2 = 1 mod 35)$.

Now for $\nu(n) = \nu(35) = 1152$, we may choose k = 5, as the encryption key for which t = 461, is the decryption key. By the parametrization of m on the pell conic we have $(x_m, y_m) = P_m = (2,13)$. Then the cipher text $C_m = Q_{2k}(d, \frac{1+x_m}{y_m})$ is evaluated as:

$$Q_{2k}(d, \frac{1+x_m}{y_m}) = Q_{10}(17,11)$$

= 26

Now for the decryption of the cipher text, with the public key and the decryption key t = 461, $\frac{x_m}{y_m}$ mod n is evaluated as:

$$\frac{x_m}{y_m} \equiv Q_{461}(17,26) mod 35$$

$$\equiv 19 mod 35$$

Now solving the equations

$$x_m^2 - 17y_m^2 = 1 mod 35$$

$$\frac{x_m}{y_m} \equiv 19 mod 35$$

We have $P_m = (x_m, y_m) = (2,13)$, then the parametrization of m on the Pell conic gives

$(2,13) = P_m = (\frac{17m^2+1}{17m^2-1}, \frac{2m}{17m^2-1})$ from which we retrieve the message m as m = 13.

5. CONCLUSION

The cryptosystem constructed is based on super enciphering, the encryptions by pell conics with Rédei rational functions over finite ring that induce permutations. i.e. The encryptions of the proposed cryptosystems are based on evaluating Rédei rational functions $Q_k(d,z) \in \not\subset_n$ with the values $z \in \not\subset_n$ connected to the solutions of the Pell's equation $x^2 - dy^2 = 1$ in $\not\subset_n$. The connection between these evaluations and the convergents of solutions of Pell's equation are used in the construction of the second cryptosystem. The security of the system depends on difficulty of factoring n and the role of $\varphi(n)$ as in RSA is replaced by $\nu(n)$. This makes the proposed cryptosystem more secure than RSA cryptosystem from the classical attacks with time algorithm $O(ld(\exp\lg(d)))$. This idea may be extended to other cryptosystems involving permutation polynomials.

REFERENCES

[1] A. K. Bhandari, *The public key cryptography. Proceedings of the advanced instructional workshop on Algebraic number theory, HBA (2003)287-301.*

[2] J. Buchmann, *Introduction to cryptography , Springer-Verlag 2001.*

[3] W.S.Chou, *The factorization Dickson polynomials over finite fields, Finite fields Appl.3,1997.*

[4] S.D.Cohen, *Dickson permutations in Number-theoritic and Algebraic methods in computer science. Moscow, 1993.*

[5] M.Fried-R.Lidl, *On Dickson Polynomials And Rédei Function, Contributions to general algebra 5, Proceedings of the Salzburg conferene, Mai29-june1,1986.*

[6] Hans Lausch and Wilfried Nobauer, *Algebra of Polynomials, North Holland publishing company-1973.*

[7] M.jacobson, W.Hugh, *Solving the pell equation, CMS Books in mathematics, canadian mathematical society, 2009.*

[8] F.Lemmermeyer, *Higher descent on Pellconics. III. The first 2-descent, available on http://arxiv.org/abs/math/0311310v1,2003.*

[9] Lenstra H.W Jr. *Solving the pell equation. Notice of AMS v.49 no.2 186-192 (2002).*

[10] Neal Koblitz, *A course in number theory and cryptography. ISBN 3-578071-8,SPIN 10893308 .*

[11] Nobauer Wilfried, *Uber Permutationspolynome und Permutationsfunktionen fur Primzahlpotenzen.*

[12] Rudolf Lidl and Winfried B. Muller, *Permutation polynomials in RSA cryptosystems, Springer-Verlag(1998).*

[13] Sahadeo Padhye, *A Public key cryptosystem based on pell equation.*

[14] Stefano Barbero, Umberto Cerruti and Nadir Murru, *Solving the Pell Equation via Rédei rational functions.*

[15] [Wilfried B.Muller and Rupert Nobauer, *Cryptanalysis of the dickson scheme.*