International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:5, No:6, 2011

Cryptography Over Elliptic Curve Of The Ring $\mathbf{F_q}[\epsilon], \epsilon^4 = 0$

CHILLALI ABDELHAKIM
FST DE FEZ
Department of Mathematics
FEZ
MOROCCO
chil2015@yahoo.fr

Abstract—Groups where the discrete logarithm problem (DLP) is believed to be intractable have proved to be inestimable building blocks for cryptographic applications. They are at the heart of numerous protocols such as key agreements, public-key cryptosystems, digital signatures, identification schemes, publicly verifiable secret sharings, hash functions and bit commitments. The search for new groups with intractable DLP is therefore of great importance.The goal of this article is to study elliptic curves over the ring $F_q[\epsilon]$, with F_q a finite field of order q and with the relation $\epsilon^n = 0$, $n \geq 3$. The motivation for this work came from the observation that several practical discrete logarithm-based cryptosystems, such as ElGamal, the Elliptic Curve Cryptosystems . In a first time, we describe these curves defined over a ring. Then, we study the algorithmic properties by proposing effective implementations for representing the elements and the group law. In anther article we study their cryptographic properties, an attack of the elliptic discrete logarithm problem, a new cryptosystem over these curves.

Keywords—Elliptic Curve Over Ring, Discrete Logarithm Problem.

I. INTRODUCTION

LET p be an odd prime number and n be an integer such that $n \geq 2$. Consider the quotient ring $A = F_q[X](X^n)$ where F_q is the finite field of characteristic p and q elements. Then the ring A may be identified to the ring $F_q[\epsilon]$ where $\epsilon^n = 0$. In other word [1, 4]

$$A = \left\{ \sum_{i=0}^{n-1} a_i \epsilon^i | \ (a_i)_{0 \leq i \leq n-1} \in F_q^{n-1} \right\}.$$

The following result is easy to prove:

Lemma 1: Let $X = \sum_{i=0}^{n-1} X_i \epsilon^i$ and $Y = \sum_{i=0}^{n-1} Y_i \epsilon^i$ be two elements of A. Then

$$XY = \sum_{i=0}^{n-1} Z_i \epsilon^i \ \texttt{where} \ Z_j = \sum_{i=0}^{j} X_i Y_{j-i}.$$

The following result

Lemma 2: The non-invertible elements of A are those elements of the form:

$$\sum_{i=1}^{n-1} X_i \epsilon^i.$$

A. Chillali, Department of Mathematic and Computer , FST, Fez, 30000 Morocco e-mail: (chil2015@yahoo.fr).

Manuscript received Mai 30, 2011

Proof 3: Indeed the ring A is a local ring with the maximal ideal ϵA.

Remark 4: Let $Y = \sum_{i=0}^{n-1} Y_i \epsilon^i$ be the inverse of the element $X = \sum_{i=0}^{n-1} X_i \epsilon^i$. Then

$$\begin{cases} Y_0 = X_0^{-1} \\ Y_j = -X_0^{-1} \sum_{i=0}^{j-1} Y_i X_{j-i}, \quad \forall j > 0 \end{cases}$$

II. ELLIPTIC CURVE OVER A

In this section we suppose $n = 4$. An elliptic curve over ring A is curve that is given by such Weierstrass equation:[1, 2, 3, 4, 5]

$$(\star) : Y^2 Z = X^3 + aXZ^2 + bZ^3$$

where $a, \ b \in \ A$ and $4a^3 + 27b^2$ is invertible in A. We denote by $E_{a,b}$ the elliptic curve over A. The set $E_{a,b}$ together with a special point $\mathcal{O}$ -called the point infinity-, a commutative binary operation denoted by $+$. It is well known that the binary operation $+$ endows the set $E_{a,b}$ with an abelian group with $\mathcal{O}$ as identity element.

Defining the curve over A with characteristic 2 or 3 is possible, but it is indifferent for our purposes.

Lemma 5: The mapping

$$\pi_{a,b} : \left| \begin{array}{ccc} E_{a,b} & \longrightarrow & E_{\pi(a),\pi(b)} \\ [X:Y:Z] & \longmapsto & [\pi(X):\pi(Y):\pi(Z)] \end{array} \right.$$

is a surjective homomorphism of groups.

Proof 6: Consider $[X1 : Y1 : Z1]$ and $[X2 : Y2 : Z2]$ in $E_{a,b}$. We have

$(1) : \pi_{a,b}([X1 : Y1 : Z1] + [X2 : Y2 : Z2]) = \pi_{a,b}([X1 : Y1 : Z1]) + \pi_{a,b}([X2 : Y2 : Z2])$.

We now quickly show how one can also obtain results (1) using maple procedure " some and proj2". So, $\pi_{a,b}$ is a homomorphism of groups.

Let $[x_0 : y_0 : z_0]$ in $E_{\pi(a),\pi(b)}$, then

$$a = a_0 + a_1\epsilon + a_2\epsilon^2 + a_3\epsilon^3$$

$$b = b_0 + b_1\epsilon + b_2\epsilon^2 + b_3\epsilon^3$$

$$X = x_0 + x_1\epsilon + x_2\epsilon^2 + x_3\epsilon^3$$

$$Y = y_0 + y_1\epsilon + y_2\epsilon^2 + y_3\epsilon^3$$

$$Z = z_0 + z_1\epsilon + z_2\epsilon^2 + z_3\epsilon^3$$

If $[X : Y : Z]$ in $E_{a,b}$, then

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

In order to simplify this last expression, we have

$$(2) : f_0 + f_1\epsilon + f_2\epsilon^2 = 0 + f_3\epsilon^3 = 0$$

where

$$f_0 = -y_0^2z_0 + b_0z_0^3 + a_0x_0z_0^2 + x_0^3$$

$f_1 = (z_0^2a_0 + 3x_0^2)x_1 - 2y_0z_0y_1 + (-y_0^2 + 3b_0z_0^2 + 2a_0x_0z_0)z_1 + b_1z_0^3 + z_0^2a_1x_0$
$f_2 = (z_0^2a_0 + 3x_0^2)x_2 - 2z_0y_0y_2 + (-y_0^2 + 3b_0z_0^2 + 2a_0x_0z_0)z_2 + z_0^2a_1x_1 - 2y_0y_1z_1 - z_0y_1^2 + 3x_1^2x_0 + 3b_0z_1^2z_0 + 3b_1z_0^2z_1 + b_2z_0^3 + a_0x_0z_1^2 + 2z_0z_1a_0x_1 + 2z_0z_1a_1x_0 + z_0^2a_2x_0.$

$$(2) \Leftrightarrow f_0 = 0, f_1 = 0, f_2 = 0, f_3 = 0$$

$$f_0 = 0 \Leftrightarrow [x_0 : y_0 : z_0] \in E_{\pi(a),\pi(b)}$$

Coefficients $z_0^2a_0 + 3x_0^2$, $2z_0y_0$ and $-y_0^2 + 3b_0z_0^2 + 2a_0x_0z_0$ are partial derivative of a function $F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$ at the point (x_0, y_0, z_0), can not be all three null. We can then at last conclude that $[x_1 : y_1 : z_1]$, $[x_2 : y_2 : z_2]$ and $[x_3 : y_3 : z_3]$. Finally, $\pi_{a,b}$ is a surjective homomorphism of groups.

Lemma 7: The mapping

$$\theta_4 : \left| \begin{array}{ccc} F_q^3 & \longrightarrow & E_{a,b} \\ (l, k, h) & \longmapsto & [l\epsilon + k\epsilon^2 + h\epsilon^3 : 1 : l^3\epsilon^3] \end{array} \right.$$

is a injective homomorphism of groups.

Proof 8: Evidently, θ_4 is injective.
Every $[l\epsilon + k\epsilon^2 + h\epsilon^3 : 1 : l^3\epsilon^3]$ satisfies the equation of $(\star)$, we calls its points points at infinity of the curve $E_{a,b}$. We have: $[l\epsilon + k\epsilon^2 + h\epsilon^3 : 1 : l^3\epsilon^3] + [l^{'}\epsilon + k'\epsilon^2 + h'\epsilon^3 : 1 : l^{'3}\epsilon^3] = [(l + l^{'})\epsilon + (k + k')\epsilon^2 + (h + h')\epsilon^3 : 1 : (l + l^{'})^3\epsilon^3]$
Finally $\theta_4((l, k, h) + (l^{'}, k', h')) = \theta_4(l, k, h) + \theta_4(l^{'}, k', h')$, and we concluded θ_4 is injective homomorphism of groups.

Definition 9: We definite G_4 by $G_4 = Ker(\pi_{a,b})$.

Proposition 10: $G_4 = \theta_4(F_q^3)$.

Proof 11: Let $[l\epsilon + k\epsilon^2 + h\epsilon^3 : 1 : l^3\epsilon^3] \in \theta_4(F_q^3)$, then $\pi_{a,b}([l\epsilon + k\epsilon^2 + h\epsilon^3 : 1 : l^3\epsilon^3]) = [0 : 1 : 0]$, we concluded $[l\epsilon + k\epsilon^2 + h\epsilon^3 : 1 : l^3\epsilon^3] \in ker(\pi_{a,b})$.
Let $P = [X : Y : Z] \in ker(\pi_{a,b})$, then $\pi_{a,b}(P) = [0 : 1 : 0]$.
We set $X = x_1\epsilon + x_2\epsilon^2 + x_3\epsilon^3$, $Y = 1 + y_1\epsilon + y_2\epsilon^2 + y_3\epsilon^3$, $Z = z_1\epsilon + z_2\epsilon^2 + z_3\epsilon^3$, and $Y^{-1} = 1 + s_1\epsilon + s_2\epsilon^2 + s_3\epsilon^3$.
So, $P = [Y^{-1}X : 1 : Y^{-1}Z] = [x_1\epsilon + x_2'\epsilon^2 + x_3'\epsilon^3 : 1 : z_1\epsilon + z_2'\epsilon^2 + z_3'\epsilon^3]$.
We have $P \in E_{a,b}$, thus $z_1 = 0, z_2' = 0, z_3' = x_1^3$ and $P \in \theta_4(F_q^3)$.
Finally, $G_4 = \theta_4(F_q^3)$.
We deduce easily the following corollaries.

Corollary 12: The group G_4 is an elementary abelian p-group, called group at infinity of $E_{a,b}$.

Corollary 13: The sequence

$$0 \to G_4 \overset{j}{\to} E_{a,b} \overset{\pi_{a,b}}{\to} E_{\pi(a),\pi(b)} \to 0$$

be a short exact sequence defining the group extension $E_{a,b}$ of $E_{\pi(a),\pi(b)}$ by G_4.

III. A strongly collision resistant function on $E_{a,b}$

Let m be a prime number such that $s = \frac{m-1}{2}$ is also prime. Let P and Q be two elements of order m. Assume that is difficult to calculate $r = log_PQ$. We define the function h by:

$$h: \left| \begin{array}{ccc} \{0, 1, 2, ..., s-1\}^2 & \longrightarrow & E_{a,b} \\ (x, y) & \longmapsto & xP + yQ \end{array} \right.$$

Theorem 14: All collision in the function h allow to calculate r.

Proof 15: Suppose we have a collision i.e, there are two distinct pairs (x, y) and $(x^{'}, y^{'})$ such as

$$xP + yQ = x^{'}P + y^{'}Q.$$

This gives

$$(x - x^{'})P = (y^{'} - y)Q.$$

Therefore

$$(x - x^{'})P = r(y^{'} - y)P.$$

i.e

$$(x - x^{'}) = r(y^{'} - y)[m].$$

Let $d = gcd(2s, y^{'} - y)$.
Since s is prime and $y^{'} - y < s$, then $d = 1$ or $d = 2$.
If $d = 1$ then, we calculate z the inverse of $y^{'} - y$ mod $m-1$, therefore $r = (x - x^{'})z[m - 1]$.
If $d = 2$ then we calculate $z^{'}$ the inverse of $y^{'} - y$ mod s, therefore $r = (x - x^{'})z^{'}[m - 1]$ or $r = (x - x^{'})z^{'} + s[m - 1]$.

Remark 16: The function h is strongly collision resistant.

IV. Identification methods on $E_{a,b}$

Let m be a prime number such that $s = \frac{m-1}{2}$ is also prime. Let P and Q be two elements of order m. An Authority form a pair (x_A, y_A) from the identity of Alice. It chooses a random number $0 \leq d \leq m - 1$, compute $P_A = dh(x_A, y_A)$ and sends it to Alice.

1) Alice chooses a random number $0 \leq a \leq m - 1$ and compute $K = aP_A$.
2) Alice sends K to Bob.
3) Bob chooses a random number $0 \leq b \leq m-1$, computes $B = bh(x_A, y_A)$ and sends it to Alice.
4) Alice computes $C = ah(x_A, y_A) + aB$ and sends it to Bob.
5) Bob computes $D = b^{-1}C$ and sends it to authority.
6) The authority calculate $E = dD$ and sends it to Bob.
7) Bob verifies that $K = b(E - K)$.

Under this protocol, Bob identifies Alice without disclosure information.

International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:5, No:6, 2011

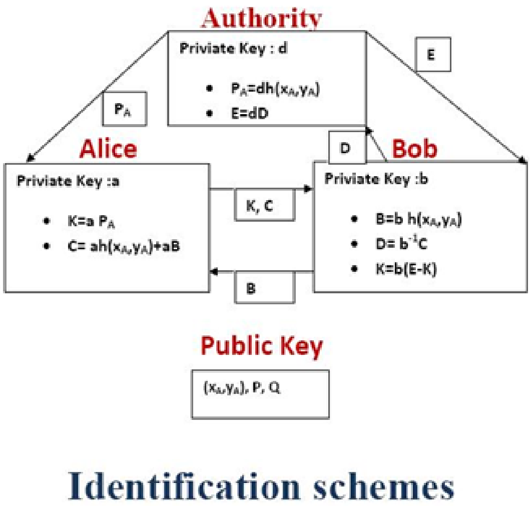

Fig. 1 Protocole D'identification

VI. Key distribution protocols

Let m be a prime number such that $s = \frac{m-1}{2}$ is also prime. Let P and Q be two elements of order m.
An Authority distributes a random number $0 \leq k \leq m-1$, sends it to Alice and to Bob.

1) Alice take a private key t such that $0 \leq t \leq m-1$, compute $P_A = h(t, kt)$, and he transmits P_A to Bob.
2) Similar, Bob takes a private key l such that $0 \leq l \leq m-1$, computes $P_B = h(l, kl)$, and transmits P_B to Alice.
3) Then Alice and Bob computes tP_B and lP_A respectively.

The secret key is

$$K = tP_B = lP_A$$

VII. Description of Cryptosystem Based on $E_{a,b}$

Let m be a prime number such that $s = \frac{m-1}{2}$ is also prime. Let P and Q be two elements of order m.

1) Space of lights: $P = E_{a,b}$.
2) Space of quantified: $C = E_{a,b}$.
3) Space of the keys: $K = E_{a,b}$.
4) Function of encryption: $\forall K \in K$,

$$e_K: \left| \begin{array}{ccc} P & \longrightarrow & C \\ X & \longmapsto & X+K \end{array} \right.$$

5) Function of decryption: $\forall K \in K$,

$$d_K: \left| \begin{array}{ccc} C & \longrightarrow & P \\ X & \longmapsto & X-K \end{array} \right.$$

Remark 17:

$$d_K o e_K(X) = X$$

Secret key :

$$K$$

Public keys:

Espace of lights P

Espace of quantified C

Espace of the keys K

P a generator of the group P

Q

Fonction of encryption e_K

Fonction of deciphering d_K

Remark 18: P and Q are public and can known by another person, but to obtain the private key K, it is necessary to solve the problem of the discrete logarithm in $E_{a,b}$, what returns the discovery of the difficult key K.

VIII. Conclusion

The conclusion in this work we study the elliptic curve over the artinian principal ideal ring $A = F_q[\epsilon], \epsilon^4 = 0$. More precisely, we establish a group homomorphism betweens $(F_q^3, +)$ and the abelian group $E_{a,b}$ of elliptic curve. For cryptography applications, we give a strongly collision resistant function on $E_{a,b}$ and identification methods on $E_{a,b}$.

Acknowledgment

I would thank Professor M. E. Charkani and H. Benaza for his helpful comments and suggestions.

References

[1] A. Chillali, *Ellipic cuvre over ring*, International Mathematical Forum, Vol. 6, no . 31, 1501-1505, 2011.
[2] T. El Gamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*,In IEEE Transactions on Information Theory, volume IT-31, no. 4, pages 469-472, july 1985.
[3] S. Vanstone and R. Zuccherato, *Elliptic Curve Cryptosystem Using Curves of Smooth Order Over the Ring Zn*, IEEE Transaction on Information Theory, IT-43, 1997.
[4] M. Virat,*Courbe elliptique sur un anneau et applications cryptographiques*, Thse Docteur en Sciences, Nice-Sophia Antipolis 2009.
[5] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, In Studies in Advenced Mathematics, pages 21-76. American mathematical society and international press edition, Based on a talk given at the conference in honor of A.O.L. Atkin, 1998.

A. Chillali , Department of Mathematic and Computer , FST, Fez, 30000 Morocco,
E-mail:chil2015@yahoo.fr.