

# Cryptography over Sextic Extension with Cubic Subfield

A. Chillali, M. Sahmoudi

**Abstract**—In this paper, we will give a cryptographic application over the integral closure  $O_L$  of sextic extension  $L$ , namely  $L$  is an extension of  $Q$  of degree 6 in the form  $Q(a,b)$ , which is a rational quadratic and monogenic extension over a pure monogenic cubic subfield  $K$  generated by  $\alpha$  who is a root of monic irreducible polynomial of degree 2 and  $\beta$  is a root of irreducible polynomial of degree 3.

**Keywords**—Integral bases, Cryptography, Discrete logarithm problem.

## I. INTRODUCTION

PUBLICkey cryptographic is the fundamental technology in secure communications. It was devised by Diffie and Hellman [8], in 1976, to secret key distribution. In 1985, Cobitz [5] and Miller [7] independently proposed the implementation of a public key cryptosystem [3] using elliptic curve. The elliptic curve discrete logarithm problem appeared to be much more difficult than above discussed algorithms [6]. In this paper we present the cryptographic protocols based on a sextic extension with a cubic subfield of type  $L = Q(\alpha, \beta)$ , whose difficulty is based on discrete logarithm problem in  $O_L = \mathbb{Z}(\alpha, \beta)$ .

**Problem:** Let  $X, Y \in O_L$  and  $X$  non-invertible. Then there is a unique integer  $n$  such that  $X^n = Y$ , we call this unique integer  $n$ , the discrete logarithm of  $Y$  with base  $X$ .

## II. INTEGRAL BASES OF SEXTIC EXTENSION

This section introduces past work, we gave an integral basis of sextic field with a pure monogenic cubic subfield, namely,  $L = Q(\alpha, \beta)$ .

We denote by  $O_L$  the integral closure of  $\mathbb{Z}$  in  $L$ .

Let  $d$  be a square free rational integer and  $\alpha$  defined by:

$$\alpha = \begin{cases} \sqrt{d}; & d \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{d}}{2}; & d \equiv 1 \pmod{4} \end{cases}$$

**Theorem1.** Let  $d$  be a square free rational integer and  $\alpha$  is a root of  $Q(X) = X^2 - d$ . Let  $a$  be a rational square free integer,  $E$  be the field  $Q(\beta)$ , where  $\beta$  is a root of  $P(X) = X^3 - a$  and  $L = Q(\alpha, \beta)$ . Then  $\mathcal{B} = \{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}$  is an integral basis of  $O_L$  over  $\mathbb{Z}$ .

**Proof.** Indeed  $\mathcal{B} = \{1, \beta, \beta^2\}$  is an integral basis of  $E$  by [4,

Theorem 6.4.13, p. 346] or [1, Proposition 4.2.], therefore we use [2, Lemma 2.1] and [2, Theorem 1.1] to conclude. We define on  $O_L$ , the following structure, we set

$$\begin{cases} X = x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 \\ Y = y_0 + y_1\alpha + y_2\beta + y_3\beta^2 + y_4\alpha\beta + y_5\alpha\beta^2 \end{cases}$$

where  $(x_0, x_1, x_2, x_3, x_4, x_5, y_0, y_1, y_2, y_3, y_4, y_5) \in \mathbb{Z}^{12}$  by:

$$\begin{cases} X + Y = s_0 + s_1\alpha + s_2\beta + s_3\beta^2 + s_4\alpha\beta + s_5\alpha\beta^2 \\ X \cdot Y = p_0 + p_1\alpha + p_2\beta + p_3\beta^2 + p_4\alpha\beta + p_5\alpha\beta^2 \end{cases}$$

with,

$$\begin{aligned} s_i &= x_i + y_i, \forall i \in \{0, 1, 2, 3, 4, 5\} \\ p_0 &= x_0y_0 + ax_2y_3 + dax_5y_4 + dx_1y_1 + ax_3y_2 + dax_4y_5 \\ p_1 &= ax_4y_3 + ax_3y_4 + x_0y_1 + ax_5y_2 + x_1y_0 + ax_2y_5 \\ p_2 &= dx_0y_2 + dx_4y_1 + x_2y_0 + x_0y_2 + dax_5y_5 + ax_3y_3 \\ p_3 &= dx_5y_1 + x_3y_0 + dx_1y_5 + dx_4y_4 + x_0y_3 + x_2y_2 \\ p_4 &= x_2y_1 + x_4y_0 + x_0y_4 + ax_5y_3 + ax_3y_5 + x_1y_2 \\ p_5 &= x_4y_2 + x_0y_5 + x_5y_0 + x_2y_4 + x_1y_3 + x_3y_1 \end{aligned}$$

**Remark 1.** With this structure,  $(O_L, +, \cdot)$  is an abelian ring.

## III. THE GROUP $R_{a,d}$

This section introduces the finite set  $R_{a,d}$ , constructed from the ring  $O_L$  (which is infinite), its usefulness will come in Section V. Let  $d$  and  $a$  are two square free rational integer. Let  $p_0, p_1, p_2, p_3, p_4$  and  $p_5$  sex prime number.

We define over a set

$$R_{a,d} = \mathbb{Z}_{p_0} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3} \times \mathbb{Z}_{p_4} \times \mathbb{Z}_{p_5}.$$

the following structure:

Let  $P = [x_0, x_1, x_2, x_3, x_4, x_5]$  and  $Q = [y_0, y_1, y_2, y_3, y_4, y_5]$

$$\begin{cases} P + Q = [s_0, s_1, s_2, s_3, s_4, s_5] \\ P \cdot Q = [f_0, f_1, f_2, f_3, f_4, f_5] \end{cases}$$

with,

$$\begin{aligned} s_i &= x_i + y_i \pmod{p_i}, \forall i \in \{0, 1, 2, 3, 4, 5\} \\ f_0 &= x_0y_0 + ax_2y_3 + dax_5y_4 + dx_1y_1 + ax_3y_2 + dax_4y_5 \pmod{p_0} \\ f_1 &= ax_4y_3 + ax_3y_4 + x_0y_1 + ax_5y_2 + x_1y_0 + ax_2y_5 \pmod{p_1} \\ f_2 &= dx_0y_2 + dx_4y_1 + x_2y_0 + x_0y_2 + dax_5y_5 + ax_3y_3 \pmod{p_2} \\ f_3 &= dx_5y_1 + x_3y_0 + dx_1y_5 + dx_4y_4 + x_0y_3 + x_2y_2 \pmod{p_3} \\ f_4 &= x_2y_1 + x_4y_0 + x_0y_4 + ax_5y_3 + ax_3y_5 + x_1y_2 \pmod{p_4} \\ f_5 &= x_4y_2 + x_0y_5 + x_5y_0 + x_2y_4 + x_1y_3 + x_3y_1 \pmod{p_5} \end{aligned}$$

**Remark 2.** The product  $(\cdot)$  is an internal composition law on

A. Chillali and M. Sahmoudi are with Fez University, USMBA, LSI, FPT, Taza, Morocco (e-mail: abdelhakim.chillali@usmba.ac.ma, sahmoudi@usmba.ac.ma).

$R_{a,d}$  commutative with unit elemente' = [1,0,0,0,0,0].

**Theorem 2.** The set  $(R_{a,d}, +)$  is a commutative group with unit elemente = [0,0,0,0,0,0].

#### IV. CRYPTOGRAPHIC APPLICATION OVER $O_L$

Let  $L = \mathbb{Q}(\alpha, \beta)$ .

##### A. Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel[7], [8].The Diffie-Hellman key exchange is the following protocol:

1. Alice and Bob choose a common element  $X \in O_L$ .
2. Alice chooses an integer  $n$ , computes  $X^n$  and transmits it to Bob.
3. Similarly, Bob chooses an integer  $m$ , computes  $X^m$  and transmits it to Alice.
4. The common secret key:

$$K = (X^n)^m = (X^m)^n$$

**Problem (\*):** Given  $X$  and  $Y$  in  $L$ , find  $n \in \mathbb{N}$  such that  $X^n = Y$ .

**Assumption:** Given a field  $L = \mathbb{Q}(\alpha, \beta)$  and  $X, Y$  in  $L$ , there is no polynomial algorithm or sub-exponential can calculate the integer  $n$  such that  $X^n = Y$ .

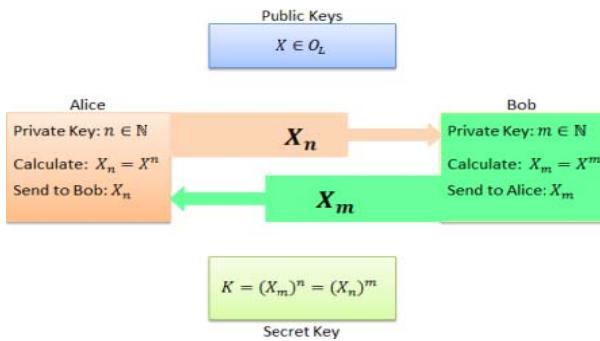


Fig. 1 Diffie-Hellman key exchange

##### B. $CSO_L$ Cryptosystem

The  $CSO_L$  cryptosystem was based on the field  $L = \mathbb{Q}(\alpha, \beta)$ .

Description of the  $CSO_L$  cryptosystem:

1. Space of Lights:  $Li = O_L$ .
2. Space of quantified :  $C = O_L$ .
3. Space of the keys :  $K = O_L \setminus \mathbb{Z}$ .
4. Function of encryption:  $\forall K \in K, e_K: Li \rightarrow C$   
 $M \mapsto K.M$
5. Function of decryption:  $\forall K \in K, d_K: C \rightarrow Li$   
 $c \mapsto K^{-1}.c$

**Remark 3.** The function  $d_K$  is well defined because the  $d_K$  function is related to  $e_K$  function by the key  $K$ .

- $d_K \circ e_K(M) = M$ .
- Secret key:  $K$ .
- Public key:  $C, Li, X, e_K$  and  $d_K$ .

**Remark 4.**  $e_K(M)$  is a public and can be known by others persons, but it is necessary to solve the problem (\*) to obtain the secret key  $K$ .

##### C. Numerical Example of $CSO_L$

In this section we will try to give a numerical example of the cryptosystem  $CSO_L$ . For that we give  $(a, d) \in \mathbb{Z}^2$  and  $X \in O_L$ . Let  $a = 7, d = 2$  and the public key:  $X = 3 + 2\alpha - 4\beta - \alpha\beta + 7\beta^2 - \alpha\beta^2$ .

- Key Exchange:

1. Alice takes a private key  $= 4$ , Computes  $X^4$  and send it to Bob.
2. Similarly, Bob takes a private key  $n = 5$ , Computes  $X^5$  and send it to Alice.
3. Secret key:  $K = (X^4)^5 = (X^5)^4$ .
4. The message example is:  $M = 20 + 12\alpha + 5\beta - \alpha\beta + 3\beta^2 - 8\alpha\beta^2$ .
5. The Encryption and Decryption message are successively:  $c = e_K(M)$  and  $M = d_K(c)$ .

- The Sent Messages:

$$\begin{aligned} X_4 &= (3)(17)(5059) + (2)^3(3)(5)(11)(53)\alpha \\ &\quad + (3)(23)(1373)\beta - (2)(3)^2(17)(587)\alpha\beta \\ &\quad + (2)^2(3)(5)(1427)\beta^2 - (2)^2(3)(5)(1699)\alpha.\beta^2 \end{aligned}$$

and

$$\begin{aligned} X_5 &= -(3)(3390589) + (3)^2(929977)\alpha \\ &\quad + (3)(1009)(1553)\beta - (2)^2(3)^3(29)(2011)\alpha\beta \\ &\quad - (3)^3(1759)\alpha\beta^2 + (2)(3)(348307)\beta^2 \end{aligned}$$

- The Secret Key:

$$\begin{aligned} K &= 52262641034876535629685607809 \\ &\quad - 23845486442998289091752693700. \alpha \\ &\quad - 478241616443579417352112157169. \beta \\ &\quad + 33871436167196700909482549400. \alpha\beta \\ &\quad + 23847785222441218172938077766. \beta^2 \\ &\quad - 172497356888128335004227387300. \alpha\beta^2 \end{aligned}$$

- The Encryption Message:

$$\begin{aligned} c &= -3674433482290661683032737181959 + \\ &\quad 26338021622868726956170062658710. \alpha + \\ &\quad 23201055397457638229782438479351. \beta - \\ &\quad 1900700620235484549245121701898. \beta^2 - \\ &\quad 16113306456240884060097451462533. \alpha\beta + \\ &\quad 1093962926102135228527491147789. \alpha\beta^2 \end{aligned}$$

- Decryption Message:

Using Maple we calculate the inverse of  $K$ . So,

$$M = 20 + 12\alpha + 5\beta - \alpha\beta + 3\beta^2 - 8\alpha\beta^2.$$

#### V. GENERIC SET OF $R_{a,d}$

##### A. Coding over $O_L$

Let  $R_{a,d}$  be a set defined as above and  $P$  an element of  $R_{a,d}$ .

$$P = [x_0, x_1, x_2, x_3, x_4, x_5]$$

We codePas follows:

1) We convert  $x_i$  to binary  $s_i = (x_i)_2, \forall i \in \{0,1,2,3,4,5\}$

2)  $P$  is coding by:  $s_P = s_0s_1s_2s_3s_4s_5$ .

**Remark 5.** Through this process, the infinite ring  $O_L$  will be transformed into a finite set noted by  $S_{O_L}$  whose elements are  $s_X$  for all  $X$  in  $O_L$ .

$$\begin{aligned} & x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 \\ & \quad \Downarrow \\ & [x_0 \text{mod} p_0, x_1 \text{mod} p_1, x_2 \text{mod} p_2, x_3 \text{mod} p_3, x_4 \text{mod} p_4, x_5 \text{mod} p_5] \\ & \quad \Downarrow \\ & s_0s_1s_2s_3s_4s_5 \end{aligned}$$

We define on the set  $S_{O_L}$  the sum and product by:

$$\begin{aligned} s_P + s_Q &= s_{P+Q} \\ s_P \cdot s_Q &= s_{P \cdot Q} \end{aligned}$$

**Theorem 3.** The set  $(S_{O_L}, +)$  is a commutative group with unit elements  $s_e = 000 \dots 0$ .

**Remark 6.**

- Number of elements of  $S_{O_L}$  is  $p_0p_1p_2p_3p_4p_5$ .
- The length of every  $s_P$  is

$$l(S_{O_L}) = p_0 + p_1 + p_2 + p_3 + p_4 + p_5.$$

**Definition 1.** Let  $s_P$  an element of  $S_{O_L}$ . The set  $G_P$  of power of  $s_P$  will be called generic set of  $O_L$  generated by  $s_P$ .

#### B. Cryptosystem over $G_P$

**Definition 2.** Let  $s_P = x_0x_1 \dots x_t$  and  $s_Q = y_0y_1 \dots y_t$ . We define  $s_P \oplus s_Q$  by:

$$s_P \oplus s_Q = z_0z_1 \dots z_t,$$

where

$$z_i = x_i + y_i \bmod 2, \forall i \in \{0, \dots, t\}.$$

Let  $P$  in  $R_{a,d}$  whose  $G_P$  has a maximal cardinal. The cryptosystem over  $G_P$  is based on the ring  $O_L$ .

**Description:**

- Space of Lights:  $L = G_P$ .
- Space of quantified :  $\forall K \in \mathbb{K}, C = K \oplus G_P$ .
- Space of the keys :  $\mathbb{K} = S_{O_L}$ .
- Function of encryption:  $\forall K \in \mathbb{K}, e_K: L \rightarrow C$   
 $M \mapsto K \oplus M$
- Function of decryption:  $\forall K \in \mathbb{K}, d_K: C \rightarrow L$   
 $c \mapsto K \oplus c$

**Remark 7.**

- Secret key:  $K$  and  $C$ .
- Public key:  $L$ ,  $\mathbb{K}$ ,  $e_K$  and  $d_K$ .

#### C. Example of Encryption and Decryption

We take  $p_0 = p_3 = 2, p_1 = p_4 = 3, p_2 = p_5 = 5, a = 7$  and  $d = 2$ . Then we have:

1) Number of elements of  $S_{O_L}$  is 900.

2) The length of every  $s_P$  is  $l(S_{O_L}) = 20$ .

3) Lets  $P = 10010110001001011000$ , the generic set is

$G_P = \{s_P^l / l \in \{1, \dots, 44\}\}$  of order 44.

4) Symbol table:

TABLE I  
TABLE OF SYMBOL

$l$	$s_P^l$	Symbol
1	10010110001001011000	A
2	10010000001010001000	B
3	00100100000001001000	C
4	10000010001000010000	D
5	00100001000010000000	E
6	00010010000000001000	F
7	000100010000000011000	G
8	000101100000001011000	H
9	10100000001001001000	I
10	00100100000000000100	J
11	10100110001000001000	K
12	10010100001010000100	L
13	101001000010000010000	M
14	10010010001001000100	N
15	000101000000000010000	O
16	100101000010000000000	P
17	10000001001010000100	Q
18	0001010000000000000000	R
19	10010001001001000100	S
20	00010110000010000000	T
21	10000000001010010000	U
22	0001010000001000000000	V
23	10000100001010010000	W
24	100100100010000010000	X
25	00000010000010000000	Y
26	0010000000001000000000	Z
27	00010100000001011000	SPACE( $s_P$ )
28	10100110001010011000	0
29	10000010001000011000	1
30	00100110000000001000	2
31	10100100001001000100	3
32	10100100001010011000	4
33	10000000001001000100	5
34	00000100000001000000	6
35	10010001001010011000	7
36	0010000100000001010000	8
37	00000100000001000000	9
38	10100001001001000100	,
39	00100000000001000000	.
40	00000100000001000000	!
41	10100110001010000100	€

• Diffie-Hellman Key Exchange

We keep the algorithm of Diffie-Hellman in IV. B. We will get the secret key

$$K = S_K = 10000100000000000000.$$

• Encryption Message:

In this example, we encrypt the following message:

# REGISTRATION FEES IN A CRYPTOGRAPHY CONFERENCE IS 450€

### 5) Encryption Message table:

In table II, we will encode the characters of the message, which will be thereafter encrypted.

**TABLE II**  
**ENCRYPTION MESSAGE**

Symbol	Coding symbols $p$	$K \oplus S_p$
$R$	000101000000000000000000	100100000000000000000000
$E$	00100001000010000000	10100101000010000000
$G$	00010001000000011000	10010101000000011000
$I$	10100000001001001000	00100100001001001000
$S$	10010001001001000100	00010101001001000100
$T$	00010110000010000000	10010010000010000000
$A$	100101100001001011000	000100100001001011000
$O$	000101000000000010000	100100000000000010000
$N$	100100100001001000100	000101100001001000100
$F$	000100100000000001000	100101100000000001000
$Sp$	00010100000001011000	10010000000001011000
$C$	00100100000001001000	10100000000001001000
$Y$	000000100000010001000	100001100000010001000
$P$	100101000001000000000	000100000001000000000
$H$	00010110000001011000	10010010000001011000
$4$	101001000001010011000	001000000001010011000
$5$	100000000001001000100	000000100001001000100
$0$	101001100001010011000	001000100001010011000
$\epsilon$	101001100001010000100	001000100001010000100
.	001000000000010010000	101001000000010010000

#### *6) Encryption message:*

The encryption message is:

- *Decryption Message*

Through the same process using the decryption function we get the message being sent.

problem.

To give an example of cryptography, we had built a set called a generic finite set over  $O_L$  on which the cryptosystem whose secret key  $K$  has raised from Diffie-Hellman Key Exchange on  $O_L$ .

## ACKNOWLEDGMENT

The authors would like to thank USMBA, LSI, FSDMFES in Fez and FPT in Taza and FSDMFES in Fez, MOROCCO for its valued support.

## REFERENCES

- [1] M. E. Charkani and M. Sahmoudi, Sextic Extension With Cubic subfield, JP journal of algebra, Number theory and applications, vol. 34, No. 2, p. 139-150, 2014.
  - [2] M. E. Charkani and O. Lahlou, On Dedekind's criterion and monogeneity over Dedekind rings, Int. J. of Math. and Math. Sci. 2003 (7) (2003) 4455-4464.
  - [3] A. Chillali, Cryptography over elliptic curve of the ring  $\mathbb{F}_q[\epsilon], \epsilon^4 = 0$  World Academy of science Engineering and Technology,78 (2011),pp.848-850.
  - [4] H. Cohen, A Course in Computational Algebraic Number theory, GTM vol. 138 (Springer Verlag, Berlin, 1996).
  - [5] K. Koblitz, "Elliptic curve cryptosystem", Mathematics of computation., 48: 203-209, 1987.
  - [6] A. J. Menezes, Elliptic curve public key cryptosystems., Kluwer Academic Publishers, 1993.
  - [7] V. S. Miller, "Use of elliptic curves in cryptography", In Crypto'85, p: 417-426, 1986.
  - [8] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on information theory, vol. it-22, No. 6, November 1976.

## VI. CONCLUSION

In conclusion, it has highlighted a key exchange on the infinity ring  $O_1$ , which is based on the discrete logarithm