

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 \mathbb{Q} of degree 6 in the form $\mathbb{Q}(a,b)$, which is a rational quadratic and monogenic extension over a pure monogenic cubic subfield K generated by a who is a root of monic irreducible polynomial of degree 2 and b is a root of irreducible polynomial of degree 3.

Keywords—Integral bases, Cryptography, Discrete logarithm problem.

I. INTRODUCTION

Public key cryptographic is the fundamental technology in secure communications. It was devised by Diffie and Hellman [8], in 1976, to secret key distribution. In 1985, Coblitz [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 $L = \mathbb{Q}(\alpha, \beta)$, 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, $L = \mathbb{Q}(\alpha, \beta)$.

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

Let d be a square free rational integer and α defined by:

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

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

Proof. Indeed $\mathfrak{B} = \{1, \beta, \beta^2\}$ 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 six 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

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

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

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 $X^n = Y$.

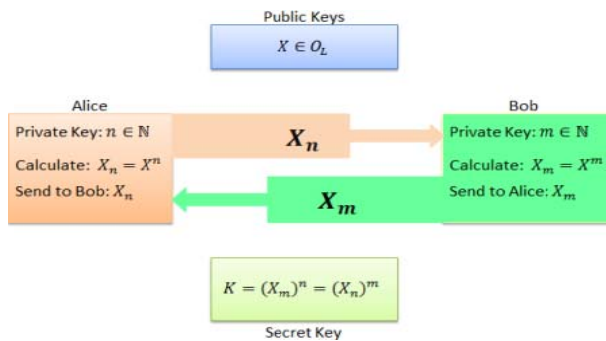


Fig. 1 Diffie-Hellman key exchange

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: $\mathbb{K} = O_L \setminus \mathbb{Z}$.
4. Function of encryption: $\forall K \in \mathbb{K}, \begin{matrix} e_K: Li \rightarrow C \\ M \mapsto K.M \end{matrix}$
5. Function of decryption: $\forall K \in \mathbb{K}, \begin{matrix} d_K: C \rightarrow Li \\ c \mapsto K^{-1}.c \end{matrix}$

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 $m = 4$, 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:

$$X_4 = (3)(17)(5059) + (2)^3(3)(5)(11)(53)\alpha + (3)(23)(1373)\beta - (2)(3)^2(17)(587)\alpha\beta + (2)^2(3)(5)(1427)\beta^2 - (2)^2(3)(5)(1699)\alpha.\beta^2$$

and

$$X_5 = -(3)(3390589) + (3)^2(929977)\alpha + (3)(1009)(1553)\beta - (2)^2(3)^3(29)(2011)\alpha\beta - (3)^3(1759)\alpha\beta^2 + (2)(3)(348307)\beta^2$$

• The Secret Key:

$$K = 52262641034876535629685607809 - 23845486442998289091752693700.\alpha - 478241616443579417352112157169.\beta + 338714361671967009099482549400.\alpha\beta + 23847785222441218172938077766.\beta^2 - 172497356888128335004227387300.\alpha\beta^2$$

• The Encryption Message:

$$c = -36744433482290661683032737181959 + 26338021622868726956170062658710.\alpha + 23201055397457638229782438479351.\beta - 1900700620235484549245121701898.\beta^2 - 16113306456240884060097451462533.\alpha\beta + 1093962926102135228527491147789.\alpha\beta^2$$

• 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) Pis 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 .

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

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 $e = 000 \dots 0$.

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. Lets $s_p = x_0x_1 \dots x_t$ and $s_q = y_0y_1 \dots y_t$. We defines $s_p \oplus s_q$ 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:

1. Space of Lights: $Li = G_p$.
2. Space of quantified : $\forall K \in \mathbb{K}, C = K \oplus G_p$.
3. Space of the keys : $\mathbb{K} = S_{O_L}$.
4. Function of encryption: $\forall K \in \mathbb{K}, \begin{matrix} e_K: Li \rightarrow C \\ M \mapsto K \oplus M \end{matrix}$
5. Function of decryption: $\forall K \in \mathbb{K}, \begin{matrix} d_K: C \rightarrow Li \\ c \mapsto K \oplus c \end{matrix}$

Remark 7.

- Secret key: K and C .
- Public key: Li, \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 $s_p = 10010110001001011000$, 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	00010001000000011000	G
8	00010110000001011000	H
9	10100000001001001000	I
10	00100100000000000100	J
11	10100110001000001000	K
12	10010100001010000100	L
13	10100100001000010000	M
14	10010010001001000100	N
15	00010100000000010000	O
16	10010100001000000000	P
17	10000001001010000100	Q
18	00010100000000000000	R
19	10010001001001000100	S
20	00010110000010000000	T
21	10000000001010010000	U
22	00010100000010000100	V
23	10000100001010010000	W
24	10010010001000010000	X
25	00000010000010001000	Y
26	00100000000010000100	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	00100010000001010000	8
37	00000100000010001000	9
38	10100001001001001000	.
39	00100000000001001000	.
40	00000100000010000100	!
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 s_p	$K \oplus s_p$
R	00010100000000000000	10010000000000000000
E	00100001000010000000	10100101000010000000
G	00010001000000011000	10010101000000011000
I	10100000001001001000	00100100001001001000
S	10010001001001000100	00010101001001000100
T	00010110000010000000	10010010000010000000
A	10010110001001011000	00010010001001011000
O	00010100000000100000	10010000000000100000
N	10010010001001000100	00010110001001000100
F	00010010000000001000	10010110000000001000
Sp	00010100000001011000	10010000000001011000
C	00100100000001001000	10100000000001001000
Y	00000010000010001000	10000110000010001000
P	10010100001000000000	00010000001000000000
H	00010110000001011000	10010010000001011000
4	10100100001010011000	00100000001010011000
5	10000000001001000100	00000100001001000100
0	10100110001010011000	00100010001010011000
€	10100110001010000100	00100010001010000100
.	00100000000001001000	10100100000001001000

6) Encryption message:

The encryption message is:

"1001000000000000000010100101000010000000100101010000000
11000001001000010010010000001010100100100010010010010000
010000000100100000000000000000000100100010010110001001001
00000100000000010010000100100010001000000000010000000
1011000100100010001001001000000001011000100101100000000100
01010010100001000000010100101000010000000000101010010010
00100100100000000010110000010010000100100100000010110001
00100010010010000000001011000000100100010010110001001000
00000010110001010000000001001000100100000000000000100
00110000010001000000100000010000000001001001000001000000
010010000000000100001001010100000001100010010000000000
00000000100100010010110000001000000100000000010010010000
00101100010000110000010001000100100000000010110001010000
0000001001000100100000000001000000010110001001000100100
10110000000001000101001010000100000000100100000000000000
0101001010000100000000001011000100100010010100000000010
01000101001010000100000001001000000000101100000100100001
00100100000010101001001000100100100000000010110000010000
000101001100000001000010010001000010001000100010001000001
00010001010000100101001000100010000000100100010001000001

• Decryption Message

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

VI. CONCLUSION

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

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 monogenicity 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.