International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:9, No:4, 2015

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_Lof 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 a who is a root of monic irreducible polynomial of degree 2 andb is a root of irreducible polynomial of degree 3.

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

I. Introduction

PUPLICkey 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 whit 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:

$$\alpha = \begin{cases} \sqrt{d}\ ;\ d \equiv\ 2\ ,3 \text{ modulo } 4 \\ \dfrac{1+\sqrt{d}}{2}\ ;\ d \equiv 1 \text{ modulo } 4 \end{cases}$$

Theorem1. 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:

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

with,

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

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

III. The Group $R_{a,d}$

This sectionintroduces 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 tow 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$Q = [y_0, y_1, y_2, y_3, y_4, y_5]$

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

with,

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

Remark 2. The product (.) 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 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 OverO_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 $L = \mathbb{Q}(\alpha, \beta)andX, Y$ in L, there is no polynomial algorithm or sub-exponential can calculate the integer n such that $X^n = Y$.

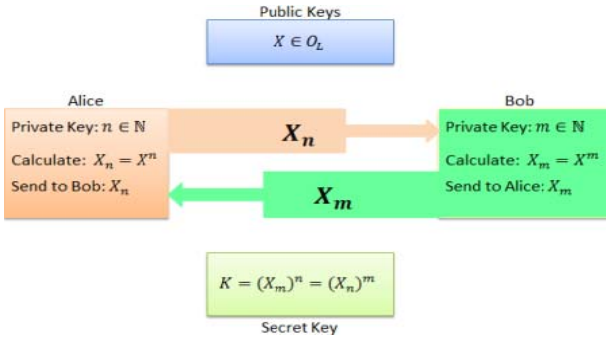

Fig. 1 Diffie-Hellman key exchange

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: $\forall K \in \mathbb{K}$, $e_K: Li \to C$, $M \mapsto K.M$
5. Function of decryption: $\forall K \in \mathbb{K}$, $d_K: C \to Li$, $c \mapsto K^{-1}.c$

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.

Remark4.$e_K(M)$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 ofCSO_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:

$$K = 52262641034876535629685607809 - 2384548644299828909175269370 0.\alpha - 4782416164435794173521121571 69.\beta + 3387143616719670090994825494 00.\alpha\beta + 2384778522224412181729380777 66.\beta^2 - 1724973568881283350042273873 00.\alpha\beta^2$$

- The EncryptionMessage:

$$c = -3674443348229066168303273718195 9 + 2633802162286872695617006265871 0.\alpha + 2320105539745763822978243847935 1.\beta - 1900700620235484549245121701898.\beta^2 - 1611330645624088406009745146253 3.\alpha\beta + 1093962926102135228527491147789.\alpha\beta^2$$

- Decryption Message:

Using Maple we calculatethe 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:$s_P = s_0 s_1 s_2 s_3 s_4 s_5$.

Remark5. Through this process, the infinite ring O_L will be transformed into a finite set noted byS_{O_L}whose elements are s_X for all Xin O_L.

$$x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2$$
$$\Downarrow$$
$$[x_0 mod p_0, x_1 mod p_1, x_2 mod p_2, x_3 mod p_3, x_4 mod p_4, x_5 mod p_5]$$
$$\Downarrow$$
$$s_0 s_1 s_2 s_3 s_4 s_5$$

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

$$s_P + s_Q = s_{P+Q}$$
$$s_P . s_Q = s_{P.Q}$$

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

Remark 6.

- Number of elements of $S_{O_L}$is $p_0 p_1 p_2 p_3 p_4 p_5$.
- 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 ofO_L generated bys_P.

B. Cryptosystem overG_P

Definition 2. Let$s_P = x_0 x_1 \ldots x_t$and$s_Q = y_0 y_1 \ldots y_t$. We define$s_P \oplus s_Q$ by:

$$s_P \oplus s_Q = z_0 z_1 \ldots z_t,$$

where

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

Let P in $R_{a,d}$whose G_P has a maximal cardinal. The cryptosystem o*verG_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: $\forall K \in \mathbb{K}$, $e_K: Li \to C$, $M \mapsto K \oplus M$
5. Function of decryption: $\forall K \in \mathbb{K}$, $d_K: C \to Li$, $c \mapsto K \oplus c$

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) Let$s_P = 10010110001001011000$, the generic set is $G_P = \{s_P{}^l / l \in \{1, .., 44\}\}$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(sp)*
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_P	$K \oplus s_P$
R	0001010000000000000	1001000000000000000
E	0010000100001000000	1010010100001000000
G	0001000100000011000	1001010100000011000
I	1010000000100100100	0010010000100100100
S	1001000100100100010	0001010100100100010
T	0001011000001000000	1001001000001000000
A	1001011000100101100	0001001000100101100
O	0001010000000001000	1001000000000001000
N	1001001000100100010	0001011000100100010
F	0001001000000000100	1001011000000000100
Sp	0001010000000101100	1001000000000101100
C	0010010000000100100	1010000000000100100
Y	0000001000001000100	1000011000001000100
P	1001010000100000000	0001000000100000000
H	0001011000000101100	1001001000000101100
4	1010010000101001100	0010000000101001100
5	1000000000100100010	0000010000100100010
0	1010011000101001100	0010001000101001100
€	1010011000101000010	0010001000101000010
.	0010000000000100100	1010010000000100100

6) Encryption message:

The encryption message is:

"1001000000000000000001010010100001000000010010101000000
1100000100100001001001000000101010010010001001001001000
0100000001001000000000000000000010010001001011000100100
1000001000000000010010000100100100010010000000000001000000
1011000100100010010010000000000101100010010110000000000100
0101001010000010000000101001010000100000000000101010010010
0010010010000000000101100000100100001001001000000010110001
0010001001001000000000101100000001001000100101100010010000
0000001011000101000000000001001000100100000000000000000100
0011000000100010000000100000001000000000100100100000010000000
0100100000000000010000100101010000000110001001000000000000
0000000010010001001011000000010000000100000000010010010000
0010110001000011000000100010001001000000000010110001010000
0000001001000100100000000000010000000101100010010001001000
1011000000000010001010010100001000000010010000000000000000
0101001010000010000000000101100010010001001010000000000010
0100010100101000010000000100100000000010110000001001000001
0010010000000101010010010001001001000000000010110000010000
0001010011000000000100001001000100001000100010100110000001
00010001010000100101001000000001001000"

- *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 ringO_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 $\mathbb{F}_q[\varepsilon], \varepsilon^4 = 0$ 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", Mathematies 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.