DE GRUYTER
OPEN

TATRA
MOUNTAINS
Mathematical Publications

DOI: 10.1515/tmmp-2017-0024
Tatra Mt. Math. Publ. **70** (2017), 151–162

KEY EXCHANGE OVER PARTICULAR ALGEBRAIC CLOSURE RING

Mohammed Sahmoudi — Abdelhakim Chillali

ABSTRACT. In this paper, we propose a new method of Diffie-Hellman key exchange based on a non-commutative integral closure ring. The key idea of our proposal is that for a given non-commutative ring, we can define the secret key and take it as a common key to encrypt and decrypt the transmitted messages. By doing, we define a new non-commutative structure over the integral closure O_L of sextic extension L, namely L is an extension of $\mathbb{Q}$ of degree 6 in the form $\mathbb{Q}(\alpha, \beta)$, which is a rational quadratic and monogenic extension over a non-pure and monogenic cubic subfield $K = \mathbb{Q}(\beta)$.

1. Introduction

The purpose of homomorphic encryption is to allow calculation on encrypted data. Thus, data can remain confidential during treatment, allowing performing useful tasks with data residing in untrusted environments. Finding a general method for computing on encrypted data have been a goal in cryptography since it was proposed in 1978 by Rivest, Adleman and Dertouzos [6]. Principally, fully homomorphic cryptosystems allow for arbitrary computations on encrypted data. Computing on encrypted data means that if a user has a function f and wants to obtain $f(t_1, t_2, \ldots, t_n)$ for some $t_1, t_2, \ldots, t_n$ inputs, it is possible to compute on encryptions of these inputs $c_1, c_2, \ldots, c_n$, obtaining a result, which decrypts to $f(t_1, t_2, \ldots, _n)$. In some cryptosystems, the input messages (plaintexts) lie within some algebraic structure, often a group or a ring as in our work, where the cryptosystem is a homomorphic encryption and decryption scheme. In other terms an encryption function Enc() such that both Enc(x+y) and Enc(x.y) are easy to compute from Enc(x) and Enc(y). If a user could take a problem defined in one algebraic system and encode it into a problem in a different algebraic system in a way that decoding back to the original

2010 Mathematics Subject Classification: Primary 11T71; Secondary 11Rxx.
Keywords: integral basis, key exchange, fully homomorphic cryptosystems, cryptography.
LAGA Laboratory, Faculty of Sciences Dhar El Mahraz Fèz and FPT in Taza. USMBA.

algebraic system is hard, then the user could encode expensive computations and send them to the untrusted party. This untrusted party then performs the corresponding computation in the second algebraic system, returning the result to the user. Upon receiving the result, the user can decode it into a solution in the original algebraic system, while the untrusted party learns nothing of which computation is actually performed. Let L be a sextic number field, namely, L is an extension of $\mathbb{Q}$ of degree 6 in the form $\mathbb{Q}(\alpha, \beta)$, which is a rational quadratic and monogenic extension over non-pure cubic subfield $K = \mathbb{Q}(\beta)$ see [1], [7]. Let O_L be the ring of integers of L, Theorem 1 gives a basis of the ring of integer; namely:

$$O_L = \left\{ a_0 + a_1\alpha + a_2\beta + a_3\beta^2 + a_4\alpha\beta + a_5\alpha\beta^2 \,/\, (a_i)_{0\leq i\leq 5} \in \mathbb{Z}^6 \right\}.$$

The work presented in this paper comes within the framework of making cryptography on the integral closure of a sextic number field. In [2], we have defined a new multiplicative and commutative structure on O_L. Here, we define another structure on O_L, which is not commutative and on which the discrete logarithm problem appears to be much more difficult than in the case discussed in [2].

2. Integral bases of sextic extension

In this section, we give an integral basis of sextic field with a non-pure and monogenic cubic subfield, namely $\mathbb{Q}(\alpha, \beta)$, we denote by O_L the integral closure of $\mathbb{Z}$ in L.

Theorem 1. *Let d be a square free rational integer and α defined by*

$$\alpha = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \bmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \bmod 4. \end{cases} \tag{1}$$

Let $K = \mathbb{Q}(\beta)$ be a non-pure and monogenic cubic field, where β is a root of a monic irreducible polynomial $T(X) = X^3 - aX + b \in \mathbb{Z}[X]$. Let $L = \mathbb{Q}(\alpha, \beta)$ be a pure quadratic extension of K, where α is a root of a monic irreducible polynomial $P(X) = X^2 - d \in O_K$. Suppose that the p-adic valuation υ_p of b equals to 1 ($\upsilon_p(b) = 1$), for all prime integer p in $\mathbb{Z}$. Then the sextic field $L = \mathbb{Q}(\alpha, \beta)$ has an integral basis given by

$$\mathfrak{B} = \left\{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\right\}.$$

Proof. Indeed $B = \{1, \beta, \beta^2\}$ is an integral basis of K by [1, Theorem 5.1.], therefore we use [7, Lemma 3.2] and [1, Theorem 1.1]. □

3. Structure on the ring L

Let d be a square free rational integer and β is a root of a monic polynomial $Q(X) = X^2 - d$. Let a be a rational square free integer, K be the field $\mathbb{Q}(\beta)$, where β is a root of $P(X) = X^3 - aX + b$ and putting $L = \mathbb{Q}(\alpha, \beta)$. By 1, $\mathfrak{B} = \{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}$ is a basis of L over $\mathbb{Q}$. Let $X, Y \in L$ given by:

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

where $(x_0, x_1, x_2, x_3, x_4, x_5, y_0, y_1, y_2, y_3, y_4, y_5) \in \mathbb{Q}^{12}$. We define over L the following structure:

$$\begin{aligned} X + Y &= s_0 + s_1\alpha + s_2\beta + s_3\beta^2 + s_4\alpha\beta + s_5\alpha\beta^2, \\ X \,.\, Y &= p_0 + p_1\alpha + p_2\beta + p_3\beta^2 + p_4\alpha\beta + p_5\alpha\beta^2, \end{aligned} \tag{3}$$

where

$$\begin{aligned} s_i &= x_i + y_i, \quad \text{for all } \ i \in \{0, 1, 2, 3, 4, 5\}, \\ p_0 &= x_0y_0\,, \\ p_1 &= x_0y_1 + x_1y_3\,, \\ p_2 &= x_0y_2 + x_1y_4 + x_2y_5\,, \\ p_3 &= x_3y_3\,, \\ p_4 &= x_3y_4 + x_4y_5\,, \\ p_5 &= x_5y_5\,. \end{aligned} \tag{4}$$

Theorem 2. *The product* $(\,.\,)$ *is an internal composition law on* L*. Moreover* $(L, +, .)$ *is a non-commutative and associative ring.*

P r o o f. The product is non-commutative, comes from $p_1 = x_0y_1 + x_1y_3$, which is clearly not symmetric. For the second statement we put $Z := z_0 + z_1\alpha + z_2\beta + z_3\beta^2 + z_4\alpha\beta + z_5\alpha\beta^2$. Then

$$(X \,.\, Y) \,.\, Z = t_0 + t_1\alpha + t_2\beta + t_3\beta^2 + t_4\alpha\beta + t_5\alpha\beta^2,$$

where

$$\begin{aligned} t_0 &= x_0y_0z_0\,, \\ t_1 &= x_0y_0z_1 + x_0y_1z_3 + x_1y_3z_3\,, \\ t_2 &= x_0y_0z_2 + x_0y_1z_4 + x_1y_3z_4 + x_0y_2z_5 + x_1y_4z_5 + x_2y_5z_5\,, \\ t_3 &= x_3y_3z_3\,, \\ t_4 &= x_3y_3z_4 + x_3y_4z_5 + x_4y_5z_5\,, \\ t_5 &= x_5y_5z_5\,. \end{aligned} \tag{5}$$

With the same way we compute $X\,.\,(Y.\,Z)$, we find the same coefficients as in $(X\,.\,Y)\,.\,Z$. To conclude this proof, we show the distributivity on the left and on the right. X, Y and Z are as above. Using a computing package, such as (Maple), we check that:

$$\begin{aligned}(Y+Z)\,.\,X &= h_0+h_1\alpha+h_2\beta+h_3\beta^2+h_4\alpha\beta+h_5\alpha\beta^2,\\ Y.\,X+Z.\,X &= g_0+g_1\alpha+g_2\beta+g_3\beta^2+g_4\alpha\beta+g_5\alpha\beta^2\end{aligned} \tag{6}$$

with

$$\begin{aligned}h_0 &= x_0(y_0+z_0)\,,\\ h_1 &= (y_1+z_1)x_0+(y_3+z_3)x_1\,,\\ h_2 &= x_0(y_2+z_2)+x_1(y_4+z_4)+x_2(y_5+z_5)\,,\\ h_3 &= x_3(y_3+z_3)\,,\\ h_4 &= x_3(y_4+z_4)+x_4(y_5+z_5)\,,\\ h_5 &= x_5(y_5+z_5)\,,\end{aligned} \tag{7}$$

and

$$\begin{aligned}g_0 &= x_0y_0+x_0z_0\,,\\ g_1 &= x_0y_1+x_1y_3+x_0z_1+x_1z_3\,,\\ g_2 &= x_0y_2+x_1y_4+x_2y_5+x_0z_2+x_1z_4+x_2z_5\,,\\ g_3 &= x_3y_3+x_3z_3\,,\\ g_4 &= x_3y_4+x_4y_5+x_3z_4+x_4z_5\,,\\ g_5 &= x_5y_5+x_5z_5\,.\end{aligned} \tag{8}$$

It's clear that for all i in $\{0,\ldots,5\}$; $h_i=g_i$. □

Proposition 1. *Let $X\in L$ given by: $X=x_0+x_1\alpha+x_2\beta+x_3\beta^2+x_4\alpha\beta+x_5\alpha\beta^2$. The neutral element for the group law $(L,\,.\,)$ is the point e equal to $1+\beta^2+\alpha\beta^2$. On the other hand, X is invertible in L if and only if $x_0x_3x_5\neq 0$. Indeed, the inverse Y is*

$$Y=i_0+i_1\alpha+i_2\beta+i_3\beta^2+i_4\alpha\beta+i_5\alpha\beta^2\,,$$

where

$$\begin{aligned}i_0 &= \frac{1}{x_0}; & i_1 &= -\frac{x_1}{x_0x_3};\\ i_2 &= \frac{x_1x_4-x_2x_3}{x_0x_3x_5}; & i_3 &= \frac{1}{x_3};\\ i_4 &= \frac{-x_4}{x_5x_3}; & i_5 &= \frac{1}{x_5}.\end{aligned} \tag{9}$$

P r o o f. It is simple, but less natural, to check directly with the given formulas of unit element e that for all $X \in L$, $X.e = e.X = X$. Using the product law defined one finds immediately that the inverse of X is equal to Y. □

Theorem 3. *Let p be a positive integer. Then if X is any element of L: $X = x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2$. We give the $p-$power of X by: $X^n = p_0 + p_1\alpha + p_2\beta + p_3\beta^2 + p_4\alpha\beta + p_5\alpha\beta^2$, where*

$$\begin{aligned}
p_0 &= x_0^n\,,\\
p_1 &= x_1 \sum_{i+j=n-1} x_0^i x_3^j\,,\\
p_2 &= x_2 \sum_{i+j=n-1} x_0^i x_5^j + x_1 x_4 \sum_{i+j+k=n-2} x_0^i x_5^j x_3^k\,,\\
p_3 &= x_3^n\,,\\
p_4 &= x_4 \sum_{0\le i\le n-1} x_3^i x_5^{n-1-i},\\
p_5 &= x_5^n\,.
\end{aligned} \tag{10}$$

P r o o f. By induction on n. For $n = 1$: the right-hand side in 10 holds since the set $S = \{(i, j, k) \in \mathbb{N}^3; i + j + k = -1\}$ is empty.

Assume that the formula holds for $n = p$; we will prove it for $n = p + 1$. Let $n = p$. Then

$$\begin{aligned}
p_0 &= x_0^p\,,\\
p_1 &= x_1 \sum_{i+j=p-1} x_0^i x_3^j\,,\\
p_2 &= x_2 \sum_{i+j=p-1} x_0^i x_5^j + x_1 x_4 \sum_{i+j+k=p-2} x_0^i x_5^j x_3^k\,,\\
p_3 &= x_3^p\,,\\
p_4 &= x_4 \sum_{0\le i\le p-1} x_3^i x_5^{p-1-i},\\
p_5 &= x_5^p\,.
\end{aligned} \tag{11}$$

Show that 11 holds for $n = p + 1$, we start with

$$X^{p+1} = X^p.X = q_0 + q_1\alpha + q_2\beta + q_3\beta^2 + q_4\alpha\beta + q_5\alpha\beta^2.$$

Then by the formula 4:

$$
\begin{aligned}
q_0 &= x_0^p x_0 = x_0^{p+1},\\
q_1 &= p_0 x_1 + p_1 x_3 = x_0^p x_1 + x_1 x_3 \sum_{i+j=p-1} x_0^i x_3^j\,,\\
q_2 &= p_0 x_2 + p_1 x_4 + p_2 x_5 = x_0^p x_2 + x_4 x_1 \sum_{i+j=p-1} x_0^i x_3^j\\
&\quad + \left[x_2 \sum_{i+j=p-1} x_0^i x_5^j + x_1 x_4 \sum_{i+j+k=p-2} x_0^i x_5^j x_3^k \right] x_5\,,\\
q_3 &= x_3^p x_3 = x_3^{p+1},\\
q_4 &= p_3 x_4 + p_4 x_5 = x_3^p x_4 + x_5 x_4 \sum_{0\le i\le p-1} x_3^i x_5^{p-i},\\
q_5 &= x_5^p x_5 = x_5^{p+1}.
\end{aligned}
$$

By reindexation, we find:

$$
\begin{aligned}
q_0 &= x_0^p x_0 = x_0^{p+1},\\
q_1 &= x_1 \left(x_0^p + \sum_{i+j=p-1} x_0^i x_3^{j+1} \right) = x_1 \sum_{i+j'=p} x_0^i x_3^{j'} \ (j' = j-1),\\
q_2 &= x_0^p x_2 + x_4 x_1 \sum_{i+j=p-1} x_0^i x_3^j + x_2 \sum_{i+j=p-1} x_0^i x_5^j + x_1 x_4 \sum_{i+j+k=p-2} x_0^i x_5^{j+1} x_3^k\\
&= x_0^p x_2 + x_2 \sum_{i+j=p-1} x_0^i x_5^j + x_4 x_1 \sum_{i+j+k=p-1, j=0} x_0^i x_5^j x_3^k\\
&\quad + x_4 x_1 \sum_{i+j+k=p-1, j\ge 1} x_0^i x_5^j x_3^k\\
&= x_0^p x_2 + x_2 \sum_{i+(j+1)=p} x_0^i x_5^j + x_4 x_1 \sum_{i+j+k=p-1, j=0} x_0^i x_5^j x_3^k\\
&\quad + x_4 x_1 \sum_{i+j'+k=p-2, j\ge 1} x_0^i x_5^{j'} x_3^k\\
&= x_0^p x_2 + x_2 \sum_{i+j''=p} x_0^i x_5^{j''} + x_4 x_1 \sum_{i+j+k=p-1} x_0^i x_5^j x_3^k \ (j'' = j+1)\\
&= x_2 \sum_{i+j''=p} x_0^i x_5^{j''} + x_4 x_1 \sum_{i+j+k=p-1} x_0^i x_5^j x_3^k\,,
\end{aligned}
$$

$$q_3 = x_3^p x_3 = x_3^{p+1},$$

$$q_4 = p_3 x_4 + p_4 x_5 = x_4 \left(x_3^p + x_5 \sum_{0 \le i \le p-1} x_3^i x_5^{p-1-i} \right)$$

$$= x_4 \left(x_3^p + \sum_{0 \le i \le p-1} x_3^i x_5^{p-i} \right) = x_4 \sum_{0 \le i \le p} x_3^i x_5^{p-i},$$

$$q_5 = x_5^p x_5 = x_5^{p+1}.$$ □

4. Key exchange on O_L

4.1. Key exchange

Key exchange is a method of securely exchanging cryptographic keys over a public channel [4], [8]. The Diffie-Hellman key exchange is the following protocol:

- Alice and Bob choose a common element $(x_0, x_3, x_5) \in \mathbb{Z}^3$.
- Alice chooses an element $X = x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 \in O_L$.
- Bob chooses an element $Y = x_0 + y_1\alpha + y_2\beta + x_3\beta^2 + y_4\alpha\beta + x_5\alpha\beta^2 \in O_L$.
- Alice chooses an integer n. First, she computes $X^n = f_0 + f_1\alpha + f_2\beta + f_3\beta^2 + f_4\alpha\beta + f_5\alpha\beta^2$. After, she transmits the new element denoted by X_a to Bob, namely, $X_a = t_0 + t_1\alpha + t_2\beta + t_3\beta^2 + t_4\alpha\beta + t_5\alpha\beta^2$ with $t_0 = x_0,\ t_3 = x_3,\ t_5 = x_5\,.\ t_1 = f_1,\ t_2 = f_2,\ t_4 = f_4$.
- Similarly, Bob chooses an integer m and computes $Y^m = g_0 + g_1\alpha + g_2\beta + g_3\beta^2 + g_4\alpha\beta + g_5\alpha\beta^2$. Once calculated, Bob transmits the new element Y_b to Alice where $Y_b = \delta_0 + \delta_1\alpha + \delta_2\beta + \delta_3\beta^2 + \delta_4\alpha\beta + \delta_5\alpha\beta^2$ with $\delta_0 = x_0$, $\delta_3 = x_3,\ \delta_5 = x_5\,.\ \delta_1 = g_1,\ \delta_2 = g_2,\ \delta_4 = g_4$.
- Alice computes $Y_b^n = d_0 + d_1\alpha + d_2\beta + d_3\beta^2 + d_4\alpha\beta + d_5\alpha\beta^2$.
- Bob computes $X_a^m = r_0 + r_1\alpha + r_2\beta + r_3\beta^2 + r_4\alpha\beta + r_5\alpha\beta^2$.

Now to give the secret key, we need to create links between d_i and r_i.

Lemma 1. *We have $x_1d_1 = y_1r_1$ and $x_4d_4 = y_4r_4$, which will be denoted k_1 and k_2, respectively.*

Proof. According to the power formulas, we have:

$$d_1 = y_1 \sum_{i+j=n-1} x_0^i x_3^j, \quad r_1 = x_1 \sum_{i+j=n-1} x_0^i x_3^j.$$

Then, $x_1d_1 = y_1r_1$.

Of the same one finds,

$$d_4 = y_4 \sum_{i+j=n-1} x_0^i x_3^j, \quad r_4 = x_4 \sum_{i+j=n-1} x_0^i x_3^j.$$

which shows $x_4 d_4 = y_4 r_4$. The common secret key

$$k = 1 + k_1\alpha + k_2\beta + \beta^2 + k_4\alpha\beta + \alpha\beta^2$$

with

$$k_1 = x_1 d_1, \quad k_2 = x_4 d_4, \quad \text{and} \quad k_4 = \text{ next prime } (k_1 \,.\, k_2).$$

□

Problem(*). Let X and X_a in O_L, find the integer n such that

$$\begin{cases} t_1 = x_1 \displaystyle\sum_{i+j=n-1} x_0^i x_3^j, \\ t_2 = x_2 \displaystyle\sum_{i+j=n-1} x_0^i x_5^j + x_1 x_4 \sum_{i+j+k=n-2} x_0^i x_5^j x_3^k, \\ t_4 = x_4 \displaystyle\sum_{0\le i\le n-1} x_3^i x_5^{n-i}. \end{cases} \tag{12}$$

Assumption. There is no polynomial or sub-exponential algorithm that can calculate the integer n in the previous problem.

4.2. Function of encryption — function of decryption

Before defining the functions of encryption and decryption, we will introduce some spaces, which will be useful to us later:

- Space of lights: $M = O_L$.
- Space of quantified: $C = O_L$.
- Space of the keys: $K = U(O_L)$; unit of O_L.

4.2.1. Function of encryption

For all k in K, the function of encryption is defined by:

$$\begin{aligned} e_k : M &\to C, \\ m &\mapsto k \,.\, m \,.\, k^{-1}. \end{aligned} \tag{13}$$

4.2.2. Function of decryption

For all k in K, the function of decryption is defined by:

$$\begin{aligned} d_k : C &\to M, \\ c &\mapsto k^{-1} \,.\, c \,.\, k. \end{aligned} \tag{14}$$

Remark 1. The functions e_k and d_k are well defined since k admits an inverse in K, consequently, we can check immediately that: $d_k \circ e_k(m) = m$, for all $m \in M$.

Remark 2. The algebraic integer $e_k(m)$ is public and is known to other persons, but it is necessary to solve the problem (*) to obtain the secret key k.

Lemma 2. *Let* $(m_1, m_2) \in M^2$. *Then*:

- $e_k(m_1 + m_2) = e_k(m_1) + e_k(m_2)$,
- $e_k(m_1 \,.\, m_2) = e_k(m_1) \,.\, e_k(m_2)$.

P r o o f.
On one hand:

- $e_k(m_1 + m_2) = k \,.\, (m_1 + m_2) \,.\, k^{-1} = k \,.\, m_1 \,.\, k^{-1} + k \,.\, m_2 \,.\, k^{-1}$
  $= e_k(m_1) + e_k(m_2)$.

On the other hand:

- $e_k(m_1 \,.\, m_2) = k \,.\, (m_1 \,.\, m_2) \,.\, k^{-1} = (k \,.\, m_1 \,.\, k^{-1}) \,.\, (k \,.\, m_2 \,.\, k^{-1})$
  $= e_k(m_1) \,.\, e_k(m_2)$.

□

Remark 3. This cryptosystem is a homomorphic encryption and decryption scheme.

5. Numerical example

In this section, we will try to give a numerical example of the cryptosystem thus constructed. For that, we put, $n = 461$, $m = 562$ and we give a prime number $p = 46613216676546898945626221516$. Alice and Bob choose two algebraic integers X, Y transformed as a list:

$X = [5464162646131664323565555555555555555556514123232355,$
$554655442166569898984579899565646562199898798597995 9, 2545499621$
$5465512115454462124545, 515454544555454121245451515451511 51, 6$
$5144599898888888888888888888888865656, 6544656746989897797997 9$
$71299999999991]$ mod p.

$Y = [54641626461316643235655555555555555555556514123232355, 55446$
$554421656219989879859799 59, 254554996215465588787458488787871$
$2115454462124545, 515454544555454121245451515451511 51, 65888889$
$989415518944651615454888888888888865656, 654465746 98898977979$
$97971299999999991] \bmod p.$

$X_a = 54641626461316643235655555555555555555556514123232355,$
$124211420031641734355653731845 9, 27589404339774676327788 75714860,$
$515454544555454121245451515451511 51, 135335885375569939208413732 3774,$
$654465674698898977979979971299999999991 \bmod p.$

$Y_b = 54641626461316643235655555555555555555556514123232355, 18437$
$040170169847279776344748 12, 42228475390237554607627137 9645, 515$
$454544555454121245451515451511 51, 88187601322927067925949779 64$
$76, 654465674698898977979979971299999999991 \bmod p.$

$Y_b^n = [21694976138476603341997115494 28, 1506827088352661952016$
$372541470, 28610394118776546481577280239 78, 3132620795697456678$
$692624481121, 96770361090150204090063295 8300, 18403999185170136$
$76297144748199] \bmod p.$

$X_a^m = [21694976138476603341997115494 28, 5658005008936889441365$
$62778407, 27227038411780320921877692003 83, 3132620795697456678 6$
$92624481121, 34155519585882336750815764 26158, 18403999185170136$
$76297144748199] \bmod p.$

The common secret key:

$$k = 1 + k_1\alpha + k_2\beta + \beta^2 + k_4\alpha\beta + \alpha\beta^2$$

with

- $k_1 = 27332831617715368998357436 22228,$
- $k_2 = 22207521903476683484033260 22796,$
- $k_4 = 38106587654220653146146197 43114.$

The inverse of the common secret key:

$$k^{-1} = 1 + k_{11}\alpha + k_{21}\beta + \beta^2 + k_{41}\alpha\beta + \alpha\beta^2$$

with

- $k_{11} = 19280385058831529947268785 29419,$
- $k_{21} = 33990365513965731302206735 17652,$
- $k_{41} = 85066290223262457994800240 8533.$

The encryption message:

$$\begin{aligned} c &= e_k(X \bmod p) = k \,.\, m \,.\, k^{-1} \\ &= 48385458079557240049145558524 + 284643977367852885483899 \\ &\quad 0945055 \,.\, \alpha + 6327312132721509807082406545 1 \,.\, \beta - 59454 \\ &\quad 619851270471675792238625 \,.\, \beta^2 - 16204005879189078877631 \\ &\quad 34802282 \,.\, \alpha\beta + 3100042710810325132186233801776 \,.\, \alpha\beta^2 \end{aligned} \tag{15}$$

The decryption message:

$$\begin{aligned} m &= d_k(c) \\ &= [5464162646131664323565555555555555556514123232355, \\ &\quad 554655442166569898984579899565646562199898 7985979959, \\ &\quad 254549962154655121154544621245 45, 51545454455545412124 \\ &\quad 545151545151151, 651445998988888888888888888888865656, \\ &\quad 654465674698898977979979712999999999991] \bmod p. \end{aligned} \tag{16}$$

Conclusion 1. In conclusion, we have presented a key exchange on the infinity ring O_L, which is based on the discrete logarithm problem. To give an example of cryptography, we can build a set called generic set over O_L on which the cryptosystem whose secret key K has stemmed from Diffie-Hellman Key Exchange on O_L. This idea is the object of a next paper.

6. Open problem

Let X and X_a in O_L as defined above in the beginning of the fourth section. Is it easy to find the integer n such that

$$\begin{cases} t_1 = x_1 \displaystyle\sum_{i+j=n-1} x_0^i x_3^j \,, \\ t_2 = x_2 \displaystyle\sum_{i+j=n-1} x_0^i x_5^j + x_1 x_4 \sum_{i+j+k=n-2} x_0^i x_5^j x_3^k \,, \\ t_4 = x_4 \displaystyle\sum_{0\le i\le n-1} x_3^i x_5^{n-i}. \end{cases} \tag{17}$$

Can we generalize this work in an upper degree for the extension L, knowing that the difficulty of the problem becomes more difficult every time the degree of the extension becomes bigger?

Acknowledgements. The authors would like to thank LAGA Laboratory, Faculty of Sciences Dhar El Mahraz Fez and FPT in Taza. USMBA, MOROCCO for its valued support.

REFERENCES

[1] CHARKANI, M. E.—SAHMOUDI, M.: *Sextic extension with cubic subfield*, JP J. Algebra, Number Theory Appl. **34** (2014), 139–150.

[2] CHILLALI, A.—SAHMOUDI, M.: *Cryptography over sextic extension with cubic subfield*, World Academy Sci. Engrg. Technol. **9** (2015), 246–249.

[3] COHEN, H.: *A Course in Computational Algebraic Number theory*. GTM Springer-Verlag, Berlin, 1996.

[4] DIFFIE, W.—HELLMAN, M. E.: *New directions in cryptography*, IEEE Trans. Inf. Theory **22** (1976), 644–654.

[5] MENEZES, A. J.: *Elliptic Curve Public key Cryptosystems. Foreword by Neal Koblitz*. In: Kluwer Internat. Ser. Engrg. Comput. Sci., Vol. 234, Kluwer Acad. Publ., Boston, MA, 1993.

[6] RIVEST, R. L.—ADLEMAN, L.—DERTOUZOS, M. L.: *On data banks and privacy homomorphisms*. Foundations of Secure Computation **11**, (1978) no. 4, 169–180.

[7] SAHMOUDI, M.: *Explicit integral basis for a family of sextic field*, Gulf J. Math. **4** (2016), 217–222.

[8] MILLER, V. S.: *Use of elliptic curves in cryptography*. In: Advances in Cryptology––CRYPTO '85 (H. C. Williams, ed.), Proc. Conf., Santa Barbara/Calif. 1985, Lect. Notes Comput. Sci., Vol. 218, Springer, Berlin, 1986, pp. 417–426.

Received March, 25, 2017

Mohammed Sahmoudi
LAGA Laboratory
Faculty of Sciences Dhar El Mahraz
P. 0. Box 1796, Atlas-Fez
MOROCCO
E-mail: mohamed-sahmoudi@usmba.ac.ma

Abdelhakim Chillali
Sidi Mohamed Ben Abdellah University
FP, LSI, Taza,
MOROCCO
E-mail: abdelhakim.chillali@usmba.ac.ma