ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.1, 235–243
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.1.24

CRYPTOGRAPHY OVER TWISTED HESSIAN CURVES OF THE RING $\mathbb{F}_Q[\epsilon]$

Abdelâli Grini [1], Abdelhakim Chillali, and Hakima Mouanis

ABSTRACT. Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of a prime number p greater than or equal to 5. In this paper, we will present twisted Hessian curves cryptography over the local ring $\mathbb{F}_q[\epsilon]$, where $\epsilon^2 = 0$. The motivation for this work came from the observation that cryptography plays an important role in providing data security. In a first time, we describe these curves defined over this ring. Then, we give an application of twisted Hessian curve Diffie-Hellman key exchange. In other we give an example of encrypted and decrypted messages.

1. INTRODUCTION

In [4] Bernstein et al. have defined the twisted Hessian curves over a field, then in [1, 2] we studied these types of curves on a local ring $\mathbb{F}_q[\epsilon]$, $\epsilon^2 = 0$. In this work we will give applications of twisted Hessian curves cryptography over the local ring $\mathbb{F}_q[\epsilon]$, where $\epsilon^2 = 0$.

Let $\mathbb{F}_q$ be a finite field of order $q = p^m$, where $p \geq 5$ is a prime number and m is a positive integer, such that -3 is not a square in $\mathbb{F}_p$. We consider the quotient ring $R_2 = \mathbb{F}_q[X]/(X^2)$. Then the ring R_2 is identified to the ring $\mathbb{F}_q[\epsilon]$, $\epsilon^2 = 0$, i.e:

$$R_2 = \{a + b\epsilon / a, b \in \mathbb{F}_q\}.$$

[1] *corresponding author*

2020 *Mathematics Subject Classification.* 11T71, 14G50, 94A60.

Key words and phrases. Twisted Hessian curves, Finite Ring, Cryptography.

We consider the twisted Hessian curve over the ring R_2, which is given by the equation:

$$aX^3 + Y^3 + Z^3 = dXYZ,$$

where a, d are in R_2 and $a(27a - d^3)$ is invertible in R_2.

2. Notations

Lets a, $d \in R_2$ such that $a(a - 27d^3)$ is invertible in R_2.

We denote the twisted Hessian curve over the ring R_2 by $H_{a,d}(R_2)$ and we write:

$$H_{a,d}(R_2) = \{[X : Y : Z] \in P^2(R_2)\backslash \quad aX^3 + Y^3 + Z^3 = dXYZ\}.$$

We denote by π the canonical projection defined by

$$R_2 \mapsto \mathbb{F}_q$$

$$a + b\epsilon \mapsto a$$

Theorem 2.1. *Let* $P = [X_1 : Y_1 : Z_1]$ *and* $Q = [X_2 : Y_2 : Z_2]$ *two points in* $H_{a,d}(R_2)$.

(1) *Define:*

$$X_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1,$$
$$Y_3 = Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1,$$
$$Z_3 = Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1.$$

If $(\pi(X_3), \pi(Y_3), \pi(Z_3)) \neq (0,0,0)$ *then* $P + Q = [X_3 : Y_3 : Z_3]$.

(2) *Define:*

$$X_3' = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2,$$
$$Y_3' = Y_2^2 Y_1 Z_1 - aX_1^2 X_2 Z_2,$$
$$Z_3' = aX_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2.$$

If $(\pi(X_3'), \pi(Y_3'), \pi(Z_3')) \neq (0,0,0)$ *then* $P + Q = [X_3' : Y_3' : Z_3']$.

Proof. By using [[4], Theorem 3.2 and Theorem 4.2] we prove the theorem. □

Corollary 2.1. $(H_{a,d}(R_2), +)$ *is a group of unity* $[0 : -1 : 1]$.

3. Application twisted Hessian curve Cryptography

3.1. **Twisted Hessian curve Diffie-Hellman key exchange.**

Twisted Hessian curve Diffie-Hellman is a twisted Hessian curve variant of the standard Diffie Hellman algorithm [3]. It is a key agreement protocol that allows two parties, each having a twisted Hessian curve public/private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or to derive another key. The key, or the derived key, can then be used to encrypt subsequent communications using a symmetric-key cipher.

3.1.1. *Twisted Hessian curve Diffie-Hellman protocol.*

Suppose two people Alice and Bob, want to agree upon a key which will be later used for encrypted communication in conjunction with a private key cryptosystem.

One way to establish a secret key using twisted Hessian curve Diffie-Hellman's method is the following:

- Alice and Bob agree on a finite local ring R_2, a twisted Hessian curve $H_{a,d}$ defined over it and a point $P \in H_{a,d}$ such that the discrete logarithm problem (DLP) to the base of P is exponentially hard (P is the generator point for the curve).
- Alice chooses a secret random integer s_A, computes $K_A = (s_A \ mod \ n)P$ (n is the order of the curve) and sends K_A to Bob.
- Bob chooses a secret random integer s_B, computes $K_B = (s_B \ mod \ n)P$ and sends K_B to Alice.
- Alice computes $Q = (s_A \ mod \ n)K_B = (s_A \ s_B \ mod \ n)P$.
- Bob computes $Q = (s_B \ s_A \ mod \ n)P$.
- Their secret common key is then $Q = (s_B \ s_A \ mod \ n)P$.

Since it is practically impossible to find the private key s_A or s_B from the public key Q. Indeed, if Oscar were able to solve the DLP for the given twisted Hessian curve, than she would be able to extract the integer s_A from $K_A = (s_A \ mod \ n)P$ and simply compute $Q = (s_A \ mod \ n)K_B$. However, there is no known way of solving the Diffie-Hellman problem without solving a discrete logarithm problem in this twisted Hessian curve.

3.1.2. *Implementation Example.*

We consider the twisted Hessian curve over the ring R_2, which is given by the equation:

$$(1+\epsilon)X^3 + Y^3 + Z^3 = (1+\epsilon)XYZ.$$

The twisted Hessian curve $H_{a,d}(\mathbb{F}_5[\epsilon])$ has 45 elements:
$H_{1+\epsilon,1+\epsilon}(\mathbb{F}_5[\epsilon]) = \{[0:4:1], [1:0:4+3\epsilon], [1:2:3], [1:2:3\epsilon], [1:2:3+2\epsilon], [1:2:3+3\epsilon], [1:2:3+4\epsilon], [1:2:4+2\epsilon], [1:3:2], [1:4:4\epsilon], [1:4:2+4\epsilon], [1:4:3+2\epsilon], [1:\epsilon:4\epsilon], [1:2\epsilon:4+4\epsilon], [1:3\epsilon:4+2\epsilon], [1:4\epsilon:4], [1:2\epsilon:4+4\epsilon], [1:2+2\epsilon:4\epsilon], [1:2+3\epsilon:4+3\epsilon], [1:2+4\epsilon:4], [1:3\epsilon:2], [1:3+2\epsilon:2], [1:3+2\epsilon:4], [1:3+2\epsilon:4\epsilon], [1:3+2\epsilon:4+2\epsilon], [1:3+2\epsilon:4+3\epsilon], [1:3+2\epsilon:4+4\epsilon], [1:3+3\epsilon:2], [1:3+4\epsilon:2], [1:4\epsilon:\epsilon], [1:4\epsilon:2+2\epsilon], [1:4\epsilon:3+2\epsilon], [1:4+2\epsilon:2], [1:4+2\epsilon:3\epsilon], [1:4+2\epsilon:3+2\epsilon], [1:4+3\epsilon:0], [1:4+3\epsilon:2+3\epsilon], [1:4+3\epsilon:3+2\epsilon], [1:4+4\epsilon:2\epsilon], [1:4+4\epsilon:2\epsilon], [1:4+4\epsilon:3+2\epsilon], [\epsilon:4+3\epsilon:1], [2\epsilon:4\epsilon:1], [3\epsilon:4+4\epsilon:1], [4\epsilon:4+2\epsilon:1]\}$.

Let $P = [1,2,3+\epsilon] \in H_{1+\epsilon,1+\epsilon}(\mathbb{F}_5[\epsilon])$, P is of order 45, so P is a generator of $H_{1+\epsilon,1+\epsilon}(\mathbb{F}_5[\epsilon])$. Thus $H_{1+\epsilon,1+\epsilon}(\mathbb{F}_5[\epsilon]) =< P >$.

By using the Theorem 2.1 we obtain:

$$4P = [1,4,3+2\epsilon],\ 5P = [1,3+2\epsilon,4+3\epsilon], \text{ and } 35P = [1,3,2].$$

Suppose two people Alice and Bob want to exchange a secret key in order to communicate:

Alice and Bob each choose an integer modulo $n = 45$ (the order of the curve $H_{1+\epsilon,1+\epsilon}(\mathbb{F}_5[\epsilon])$) for example; $s_A = 49$ for Alice and $s_B = 80$ for Bob.

We have $[s_A] = 4 \ mod\ 45$ and $[s_B] = 35\ mod\ 45$, so:

- Alice calculates $[s_A]P = 4P = [1,4,3+2\epsilon]$ and sends it to Bob.
- Bob calculates $[s_B]P = 35P = [1,3,2]$ and sends it to Alice.
- Their secret key is then:

$$K = ([s_A s_B])P = [3920]P = 5P = [1,3+2\epsilon,4+3\epsilon].$$

3.2. **Encryption and decryption of a message in $H_{a,d}(R_2)$.**

Let $H_{a,d}(R_2)$ be the twisted Hessian curve over the ring R_2 such that $a = 1+2\epsilon$ and $d = 2+\epsilon$.

The twisted Hessian curve $H_{a,d}(\mathbb{F}_{11}[\epsilon])$ has 99 elements:

$H_{a,d}(\mathbb{F}_{11}[\epsilon]) = \{[0 : 10 : 1], [1 : 0 : 10 + 3\epsilon], [1 : 3 : 10 + 9\epsilon], [1 : 4 : 7 + 10\epsilon], [1 : 7 : 4+4\epsilon], [1 : 8 : 10+5\epsilon], [1 : 10 : 10\epsilon], [1 : 10 : 3+4\epsilon], [1 : 10 : 8+8\epsilon], [1 : \epsilon : 10+6\epsilon], [1 : 2\epsilon : 10 + 9\epsilon], [1 : 3\epsilon : 10 + \epsilon], [1 : 4\epsilon : 10 + 4\epsilon], [1 : 5\epsilon : 10 + 7\epsilon], [1 : 6\epsilon : 10 + 10\epsilon], [1 : 7\epsilon : 10 + 2\epsilon], [1 : 8\epsilon : 10 + 5\epsilon], [1 : 9\epsilon : 10 + 8\epsilon], [1 : 10\epsilon : 10], [1 : 3 + \epsilon : 10 + 4\epsilon], [1 : 3+2\epsilon : 10+10\epsilon], [1 : 3+3\epsilon : 10+5\epsilon], [1 : 3+4\epsilon : 10], [1 : 3+5\epsilon : 10+6\epsilon], [1 : 3+6\epsilon : 10 + \epsilon], [1 : 3 + 7\epsilon : 10 + 7\epsilon], [1 : 3 + 8\epsilon : 10 + 2\epsilon], [1 : 3 + 9\epsilon : 10 + 8\epsilon], [1 : 3 + 10\epsilon : 10 + 3\epsilon], [1 : 4 + \epsilon : 7 + 2\epsilon], [1 : 4 + 2\epsilon : 7 + 5\epsilon], [1 : 4 + 3\epsilon : 7 + 8\epsilon], [1 : 4 + 4\epsilon : 7], [1 : 4 + 5\epsilon : 7 + 3\epsilon], [1 : 4 + 6\epsilon : 7 + 6\epsilon], [1 : 4 + 7\epsilon : 7 + 9\epsilon], [1 : 4 + 8\epsilon : 7 + \epsilon], [1 : 4 + 9\epsilon : 7+4\epsilon], [1 : 4+10\epsilon : 7+7\epsilon], [1 : 7+\epsilon : 4+8\epsilon], [1 : 7+2\epsilon : 4+\epsilon], [1 : 7+3\epsilon : 4+5\epsilon], [1 : 7+4\epsilon : 4+9\epsilon], [1 : 7+5\epsilon : 4+2\epsilon], [1 : 7+6\epsilon : 4+6\epsilon], [1 : 7+7\epsilon : 4+10\epsilon], [1 : 7+8\epsilon : 4+3\epsilon], [1 : 7+9\epsilon : 4+7\epsilon], [1 : 7+10\epsilon : 4], [1 : 8+\epsilon : 10+3\epsilon], [1 : 8+2\epsilon : 10+\epsilon], [1 : 8 + 3\epsilon : 10 + 10\epsilon], [1 : 8 + 4\epsilon : 10 + 8\epsilon], [1 : 8 + 5\epsilon : 10 + 6\epsilon], [1 : 8 + 6\epsilon : 10 + 4\epsilon], [1 : 8 + 7\epsilon : 10 + 2\epsilon], [1 : 8 + 8\epsilon : 10], [1 : 8 + 9\epsilon : 10 + 9\epsilon], [1 : 8 + 10\epsilon : 10 + 7\epsilon], [1 : 10 + \epsilon : 3\epsilon], [1 : 10 + \epsilon : 3 + 6\epsilon], [1 : 10 + \epsilon : 8 + 2\epsilon], [1 : 10 + 2\epsilon : 7\epsilon], [1 : 10 + 2\epsilon : 3 + 8\epsilon], [1 : 10 + 2\epsilon : 8 + 7\epsilon], [1 : 10 + 3\epsilon : 0], [1 : 10 + 3\epsilon : 3 + 10\epsilon], [1 : 10 + 3\epsilon : 8 + \epsilon], [1 : 10 + 4\epsilon : 4\epsilon], [1 : 10 + 4\epsilon : 3 + \epsilon], [1 : 10 + 4\epsilon : 8 + 6\epsilon], [1 : 10 + 5\epsilon : 8], [1 : 10 + 5\epsilon : 8\epsilon], [1 : 10 + 5\epsilon : 3 + 3\epsilon], [1 : 10 + 6\epsilon : \epsilon], [1 : 10 + 6\epsilon : 3 + 5\epsilon], [1 : 10 + 6\epsilon : 8 + 5\epsilon], [1 : 10 + 7\epsilon : 5\epsilon], [1 : 10 + 7\epsilon : 3 + 7\epsilon], [1 : 10 + 7\epsilon : 8 + 10\epsilon], [1 : 10 + 8\epsilon : 9\epsilon], [1 : 10 + 8\epsilon : 3 + 9\epsilon], [1 : 10 + 8\epsilon : 8 + 4\epsilon], [1 : 10 + 9\epsilon : 3], [1 : 10 + 9\epsilon : 2\epsilon], [1 : 10 + 9\epsilon : 8 + 9\epsilon], [1 : 10 + 10\epsilon : 6\epsilon], [1 : 10 + 10\epsilon : 3 + 2\epsilon], [1 : 10 + 10\epsilon : 8 + 3\epsilon], [\epsilon : 10+7\epsilon : 1], [2\epsilon : 10+3\epsilon : 1], [3\epsilon : 10+10\epsilon : 1], [4\epsilon : 10+6\epsilon : 1], [5\epsilon : 10+2\epsilon : 1], [6\epsilon : 10 + 9\epsilon : 1], [7\epsilon : 10 + 5\epsilon : 1], [8\epsilon : 10 + \epsilon : 1], [9\epsilon : 10 + 8\epsilon : 1], [10\epsilon : 10 + 4\epsilon : 1]\}$.

Let $P = [1, 7 + 6\epsilon, 4 + 6\epsilon] \in H_{a,d}(\mathbb{F}_{11}[\epsilon])$, P is of order 99, so P is a generator of $H_{a,d}(\mathbb{F}_{11}[\epsilon])$. Thus $H_{a,d}(\mathbb{F}_{11}[\epsilon]) =< P >$.

We will use the group $H_{a,d}(\mathbb{F}_{11}[\epsilon])$ to encrypt and decrypt messages, and we denote $G = H_{a,d}(\mathbb{F}_{11}[\epsilon])$.

3.3. **Coding of elements of G.**

We will code each number $a \in \{0, 1, \dots, 9\}$ by $0a$ and the number 10 by 10.

We will give a code to each element $Q = mP \in G$, where $m \in 1, \dots, 99$ defined as it follows:

- If $Q = [1, y_0+y_1\epsilon, z_0+z_1\epsilon]$, where y_0, y_1, z_0, $z_1 \in \mathbb{F}_{11}$, then $Q = 01y_0y_1z_0z_1$.
- If $Q = [x\epsilon, y_0 + y_1\epsilon, 1]$, where y_0, y_1, $x \in \mathbb{F}_{11}$, then $Q = 00xy_0y_101$.

We also attach any element $Q \in G$ with a letter of the alphabet or a punctuation sign and we assemble the results in the following table:

TABLE 1. Table of codes

m	mP	Code mP	Symbol	m	mP	Code mP	Symbol
1	$[1, 7+6\epsilon, 4+6\epsilon]$	0107060406	a	2	$[1, 10+4\epsilon, 3+\epsilon]$	0110040301	b
3	$[1, 10+4\epsilon, 4\epsilon]$	0110040004	c	4	$[1, 10+9\epsilon, 8+9\epsilon]$	0110090809	d
5	$[1, 8+6\epsilon, 10+4\epsilon]$	0108061004	e	6	$[1, 3\epsilon, 10+\epsilon]$	0100031001	f
7	$[1, 3+2\epsilon, 10+10\epsilon]$	0103021010	g	8	$[1, 4, 7+10\epsilon]$	0104000710	h
9	$[10\epsilon, 10+8\epsilon, 1]$	0010100801	i	10	$[1, 7+2\epsilon, 4+\epsilon]$	0107020401	j
11	$[1, 10+9\epsilon, 3]$	0110090300	k	12	$[1, 10+7\epsilon, 5\epsilon]$	0110070005	l
13	$[1, 10+3\epsilon, 8+\epsilon]$	0110030801	m	14	$[1, 8+3\epsilon, 10+10\epsilon]$	0108031010	n
15	$[1, 2\epsilon, 10+9\epsilon]$	0100021009	o	16	$[1, 3+3\epsilon, 10+5\epsilon]$	0103031005	p
17	$[1, 4+5\epsilon, 7+3\epsilon]$	0104050703	q	18	$[9\epsilon, 10+5\epsilon, 1]$	0009100501	r
19	$[1, 7+9\epsilon, 4+7\epsilon]$	0107090407	s	20	$[1, 10+3\epsilon, 3+10\epsilon]$	0110030310	t
21	$[1, 10+10\epsilon, 6\epsilon]$	0110100006	u	22	$[1, 10+8\epsilon, 8+4\epsilon]$	0110080804	v
23	$[1, 8, 10+5\epsilon]$	0108001005	w	24	$[1, \epsilon, 10+6\epsilon]$	0100011006	x
25	$[1, 3+4\epsilon, 10]$	0103041000	y	26	$[1, 4+10\epsilon, 7+7\epsilon]$	0104100707	z
27	$[8\epsilon, 10+2\epsilon, 1]$	0008100201	0	28	$[1, 7+5\epsilon, 4+2\epsilon]$	0107050402	1
29	$[1, 10+8\epsilon, 3+9\epsilon]$	0110080309	2	30	$[1, 10+2\epsilon, 7\epsilon]$	0110020007	3
31	$[1, 10+2\epsilon, 8+7\epsilon]$	0110020807	4	32	$[1, 8+8\epsilon, 10]$	0108081000	5
33	$[1, 0, 10+3\epsilon]$	0100001003	6	34	$[1, 3+5\epsilon, 10+6\epsilon]$	0103051006	7
35	$[1, 4+4\epsilon, 7]$	0104040700	8	36	$[7\epsilon, 10+10\epsilon, 1]$	0007101001	9
37	$[1, 7+\epsilon, 4+8\epsilon]$	0107010408	space	38	$[1, 10+2\epsilon, 3+8\epsilon]$	0110020308	A
39	$[1, 10+5\epsilon, 8\epsilon]$	0110050008	B	40	$[1, 10+7\epsilon, 8+10\epsilon]$	0110070810	C
41	$[1, 8+5\epsilon, 10+6\epsilon]$	0108051006	D	42	$[1, 10\epsilon, 10]$	0100101000	E
43	$[1, 3+6\epsilon, 10+\epsilon]$	0103061001	F	44	$[1, 4+9\epsilon, 7+4\epsilon]$	0104090704	G
45	$[6\epsilon, 10+7\epsilon, 1]$	0006100701	H	46	$[1, 7+8\epsilon, 4+3\epsilon]$	0107080403	I
47	$[1, 10+7\epsilon, 3+7\epsilon]$	0110070307	J	48	$[1, 10+8\epsilon, 9\epsilon]$	0110080009	K
49	$[1, 10+\epsilon, 8+2\epsilon]$	0110010802	L	50	$[1, 8+2\epsilon, 10+\epsilon]$	0108021001	M
51	$[1, 9\epsilon, 10+8\epsilon]$	0100091008	N	52	$[1, 3+7\epsilon, 10+7\epsilon]$	0103071007	O
53	$[1, 4+3\epsilon, 7+8\epsilon]$	0104030708	P	54	$[5\epsilon, 10+4\epsilon, 1]$	0005100401	Q
55	$[1, 7+4\epsilon, 4+9\epsilon]$	0107040409	R	56	$[1, 10+\epsilon, 3+6\epsilon]$	0110010306	S

m	mP	Code mP	Symbol	m	mP	Code mP	Symbol
57	$[1, 10, 10\epsilon]$	0110000010	T	58	$[1, 10 + 6\epsilon, 8 + 5\epsilon]$	0110060805	U
59	$[1, 8 + 10\epsilon, 10 + 7\epsilon]$	0108101007	V	60	$[1, 8\epsilon, 10 + 5\epsilon]$	0100081005	W
61	$[1, 3 + 8\epsilon, 10 + 2\epsilon]$	0103081002	X	62	$[1, 4 + 8\epsilon, 7 + \epsilon]$	0104080701	Y
63	$[4\epsilon, 10 + \epsilon, 1]$	0004100101	Z	64	$[1, 7, 4 + 4\epsilon]$	0107000404	.
65	$[1, 10 + 6\epsilon, 3 + 5\epsilon]$	0110060305	:	66	$[1, 10 + 3\epsilon, 0]$	0110030000	;
67	$[1, 10, 8 + 8\epsilon]$	0110000808	,	68	$[1, 8 + 7\epsilon, 10 + 2\epsilon]$	0108071002	?
69	$[1, 7\epsilon, 10 + 2\epsilon]$	0100071002	$+$	70	$[1, 3 + 9\epsilon, 10 + 8\epsilon]$	0103091008	-
71	$[1, 4 + 2\epsilon, 7 + 5\epsilon]$	0104020705	$\times$	72	$[3\epsilon, 10 + 9\epsilon, 1]$	0003100901	$\div$
73	$[1, 7 + 7\epsilon, 4 + 10\epsilon]$	0107070410	$=$	74	$[1, 10, 3 + 4\epsilon]$	0110000304	$*$
75	$[1, 10 + 6\epsilon, \epsilon]$	0110060001	α	76	$[1, 10 + 5\epsilon, 8]$	0110050800	β
77	$[1, 8 + 4\epsilon, 10 + 8\epsilon]$	0108041008	γ	78	$[1, 6\epsilon, 10 + 10\epsilon]$	0100061010	δ
79	$[1, 3 + 10\epsilon, 10 + 3\epsilon]$	0103101003	ϵ	80	$[1, 4 + 7\epsilon, 7 + 9\epsilon]$	0104070709	ε
81	$[2\epsilon, 10 + 6\epsilon, 1]$	0002100601	ζ	82	$[1, 7 + 3\epsilon, 4 + 5\epsilon]$	0107030405	η
83	$[1, 10 + 5\epsilon, 3 + 3\epsilon]$	0110050303	θ	84	$[1, 10 + 9\epsilon, 2\epsilon]$	0110090002	λ
85	$[1, 10 + 10\epsilon, 8 + 3\epsilon]$	0110100803	μ	86	$[1, 8 + \epsilon, 10 + 3\epsilon]$	0108011003	(
87	$[1, 5\epsilon, 10 + 7\epsilon]$	0100051007	)	88	$[1, 3, 10 + 9\epsilon]$	0103001009	π
89	$[1, 4 + \epsilon, 7 + 2\epsilon]$	0104010702	τ	90	$[\epsilon, 10 + 3\epsilon, 1]$	0001100301	ϕ
91	$[1, 7 + 10\epsilon, 4]$	0107100400	φ	92	$[1, 10 + 10\epsilon, 3 + 2\epsilon]$	0110100302	ψ
93	$[1, 10 + \epsilon, 3\epsilon]$	0110010003	ω	94	$[1, 10 + 4\epsilon, 8 + 6\epsilon]$	0110040806	[
95	$[1, 8 + 9\epsilon, 10 + 9\epsilon]$	0108091009	]	96	$[1, 4\epsilon, 10 + 4\epsilon]$	0100041004	$\vert$
97	$[1, 3 + \epsilon, 10 + 4\epsilon]$	0103011004	{	98	$[1, 4 + 6\epsilon, 7 + 6\epsilon]$	0104060706	}
99	$[0, 10, 1]$	0000100001	/				

3.3.1. *Encryption of a message.*

Let the following message:

"Twisted Hessian curves are well suited to public key cryptography. They replace calculations on integers, or in Z/nZ groups, with calculations in groups associated with a twisted Hessian curve."

Its encryption is:

"011000001001080010050010100801010709040701100303100108061004011009080901070104
08000610070101080610040107090407010709040700101008010107060406010803101001070104
08011004000401101000060009100501011008080401080610040107090407010701040801070604
06000910050101080610040107010408010800100501080610040110070005011007000501070104

080107090407011010000600101008010110030310010806100401100908090107010408011003031001000210090107010408010303100501101000060110040301011007000500101008010110040004010701040801100903000108061004010304100001070104080110040004000910050101030410000103031005011003031001000210090103021010000910050101070604060103031005010400071001030410000107000404010701040801100000100104000710010806100401030410000107010408000910050101080610040103031005011007000501070604060110040004010806100401070104080110040004010706040601100700050110040004011010000601100700050107060406011003031000101008010100021009010803101001070904070107010408010002100901080310100107010408000101008010108031010011003031001080610040103021010010806100400091005010107090407011000080801070104080100021009000910050101070104080010100801010803101001070104080004100101000010000101080310100004100101010701040801030210100009100501010002100901101000060103031005010709040701100008080107010408010800100500101008010110030310010400071001070104080110040004010706040601100700050110040004011010000601100700050107060406011003031000101008010100021009010803101001070904070107010408001010080101080310100107010408010302101000091005010100021009011010000601030310050107090407010701040801070604060107090407010709040701000210090110040004001010080101070604060110030310010806100401100908090107010408010800100500101008010110030310010400071001070104080107060406010701040801100303100108001005001010080101070904070110030310010806100401100908090107010408000610070101080610040107090407010709040700101008010107060406010803101001070104080110040004011010000600091005010110080804010806100401070000404”

3.3.2. *Decryption of a message.*

Let the following message:

”010708040301080310100107010408011003031001040007100010100801010709040701070104080103031005010706040601030310050108061004000910050101100008080107010408010800100501080610040107010408010302101000101008010110080804010806100401070104080107060406010803101001070104080108061004010001100601070604060110030801010303100501100700050108061004010701040801000210090100031001010701040801070604060103031005010303100501100700050010100801011004000401070604060110030310001010080101000210090108031010010701040801100303100104000710010806100401070104080110030310010800100500101008010107090407011003031001080610040110090809010701040800061007010108061004010709040701070904070010100801010706040601080310100107010408011004000401101000060009100501011008080401080610040107090407010701040801000210090110080804010806100400091005010107010408010706040601070104080110070005010002100901100400040107060406011007000

0501070104080009100501001010080101080310100103021010010701040800101008010108031010010701040801100400040009100501010304100001030310050110030310010002100901030210100009100501010706040601030310050104000710010304100001070004 04”

Its decryption is:

"In this paper, we give an example of application the twisted Hessian curves over a local ring in cryptography."

4. Conclusion

With this example, we can encrypt and decrypt any message of any length. This application is implemented by Maple.

References

[1] A. Grini, A. Chillali, L. ElFadil, H. Mouanis: *Twisted Hessian curves over the ring $F_q[e]$, $e^2 = 0$*, International Journal of Computer Aided Engineering and Technology, to appear.

[2] A. Grini, A. Chillali, H. Mouanis: *The Binary Operations Calculus in $H^2_{a,d}$*, Boletim da Sociedade Paranaense de Matemàtica, , to appear.

[3] W. Diffie, M. E. Hellman: *New Directions in Cryptography*, NSF Grant ENG10173, 1976.

[4] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, T. Lange: *Twisted Hessian Curves*, In LATINCRYPT 2015, pages 269-294, 2015. http://cr.yp.to/papers.html#hessian.

Department of Mathematics, Faculty of Science Dhar El Mahraz-Fez
University of S. M.Ben Abdellah Fez, Morocco
P.O. Box 1796 Atlas-Fez Morocco
Email address: abdelali.grini@usmba.ac.ma

Department of Mathematics, FP, LSI, Taza
University of S. M.Ben Abdellah Fez, Morocco
P.O. Box 1796 Atlas-Fez Morocco
Email address: abdelhakim.chillali@usmba.ac.ma

Department of Mathematics, Faculty of Science Dhar El Mahraz-Fez
University of S. M.Ben Abdellah Fez, Morocco
P.O. Box 1796 Atlas-Fez Morocco
Email address: hmouanis@yahoo.fr