Gulf Journal of Mathematics
Vol 8, Issue 2 (2020) 27-34

CRYPTOSYSTEM BASED ON LATTICE AND ELLIPTIC CURVE

MOHAMMED ELHASSANI[1], ABDELHAKIM CHILLALI[2*] AND ALI MOUHIB[3]

Abstract. In this work, we propose a new way to use lattice theory to build a public key cryptosystem and digital signature scheme. This cryptosystem based on the approximate closest vector problem and the problem of the discrete logarithm on an elliptic curve defined on a finite local ring. At first, we choose a point on the elliptic curve and we will make the exchange of keys to the Diffie-Hellman. We transform the coordinates of this point into a matrix which gives us the private key which will serve us for encryption and decryption.

1. Introduction and preliminaries

The standardized and currently used cryptography is essentially based on two mathematical problems: factorization and discrete logarithm. But researchers are interested in finding credible alternatives that, for example, could resist the advent of the quantum computer. One of these alternatives, based on the geometry of Lattices, has clearly stood out during this last decade of research, offering new perspectives such as so-called homomorphic encryption. [4, 8]
Lattices are used in several fields. First, there are hard computational problems on lattices that have been used as a building block for public key cryptosystems (e.g., the Goldreich-Goldwasser-Halevi GGH cryptosystem, the NTRU cryptosystem, the Ajtai work [1] cryptosystem and the LWE cryptosystem). Second, lattices are used as a fundamental tool for cryptanalysis of public key cryptosystems (e.g.lattice attacks on knapsack cryptosystem, Coppersmith's method for finding small solutions to polynomial equations, attacks on signatures and attacks on variants of RSA). Finally, lattices can be used to develop efficient and adaptable cryptographic tools. Among them, the most outstanding is the concept for fully homomorphic encryption, which allows an untrusted worker to manipulate encrypted data, in arbitrarily complex ways, without getting any knowledge for them.

Date: Received: May 21, 2020; Accepted: Aug 10, 2020.
* Corresponding author.
2010 *Mathematics Subject Classification.* Primary 46L55; Secondary 44B20.
Key words and phrases. lattice-based cryptography, elliptic curve over a ring, homomorphic encryption.

2. Lattice

Lattices are typically defined as a discrete subgroup of $(\mathbb{R}^n, +)$. Equivalently, a lattice is the $\mathbb{Z}$ -linear span of a set of linearly independent vectors $\{\mathbf{b}_1, ...\mathbf{b}_m\} \subset \mathbb{R}^n$. let:

$$\mathcal{L}(\mathbf{b}_1, ...\mathbf{b}_m) := \{\sum_{i=1}^{i=m} \lambda_i \mathbf{b}_i, \lambda_1 ...\lambda_m \in \mathbb{Z}\}$$

Lattice-based cryptography is the construction of cryptographic functions which are at least hard to break via the use of lattices as a source of computational hardness (see [6, 7]).

2.1. Computational problems in lattices.

There are several natural problems relating to lattices. We start by listing some problems that can be efficiently solved using linear algebra (in particular, the hermite normal form):

- Lattice membership: Given an $n \times m$ basis $\mathbf{B}$ for a lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ and a vector v $\in \mathbb{Z}^m$ determine wether v $\in \mathcal{L}$.
- Lattice basis: Given a set of vectors $\mathbf{b}_1, ...\mathbf{b}_m \in \mathbb{Z}^n$(possibly linearly dependant) find a basis for the lattice generated by them.
- Kernel lattice: Given an $n \times m$ integer matrix $\mathbf{A}$ compute a basis of the lattice $Ker\mathbf{A} = \{\mathbf{v} \in \mathbb{Z}^m / \mathbf{A}\mathbf{v} = 0\}$.

Now we list some computational problems that seem to be hard.

- (SVP): Find the shortest non-zero vector in $\mathcal{L}$, i.e. find $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\|$ is minimized
- (CVP): Given a target vector $\mathbf{t}$ (not necessarily in the lattice $\mathcal{L}$), Find vector $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$, i.e. find $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v} - \mathbf{t}\|$ is minimized.

In general,these computational problems are known to be hard when the rank is sufficiently large. It is known that CVP is NP hard also, SVP is NP hard under randomised reductions and non-uniform reduction.
Even in large dimension, the CVP and SVP problems are easy if one has an orthogonal basis for a lattice. When we give a non-orthogonal basis, it is quite hard to find a vector of the lattice of minimal norm.

3. The ring $\mathbf{A}_n$

In this section, we follow the approach of [3, 9]. Let p a prim number ($p \geq 5$), we consider the quotient ring $\mathbf{A}_n = \mathbb{F}_{p^d}[\mathbf{X}]/(\mathbf{X}^n)$ where $\mathbb{F}_{p^d}$ is the finite field of order p^d and $n \geq 1$. Then the ring $\mathbf{A}_n$ is identified to the ring:

$$\mathbf{A}_n = \{\sum_{i=0}^{n-1} x_i \epsilon^i / (x_i)_{0 \leq i \leq n-1} \in \mathbb{F}_{p^d}^n, \epsilon^n = 0\}.$$

The arithmetic operations in $\mathbf{A}_n$:
Let X $= \sum_{i=0}^{n-1} x_i \epsilon^i$, Y $= \sum_{i=0}^{n-1} y_i \epsilon^i$.

- Addition law:

$$\mathrm{X}+\mathrm{Y}=\sum_{i=0}^{n-1}(x_i+y_i)\epsilon^i$$

- Product laws:

$$\lambda\sum_{i=0}^{n-1}x_i\epsilon^i=\sum_{i=0}^{n-1}\lambda x_i\epsilon^i$$

$$\mathrm{XY}=\sum_{i=0}^{n-1}t_i\epsilon^i, t_i=\sum_{j=0}^{i}x_jy_{i-j}$$

We have the following lemmas.

Lemma 3.1. *Let* $\mathrm{X}=\sum_{i=0}^{n-1}x_i\epsilon^i$. X *is invertible in* $\mathbf{A}_n$ *if and only if* $x_0\neq 0$.

Lemma 3.2. $\mathbf{A}_n$ *is local ring, its maximal ideal is* $\epsilon\mathbf{A}_n$.

Lemma 3.3. $\mathbf{A}_n$ *is a vector space over* $\mathbb{F}_{p^d}$ *and have* $(1,\epsilon,\epsilon^2...\epsilon^{n-1})$ *as basis.*

4. Matrix representation of an elliptic curve on the ring $\mathbf{A}_n$

We define an elliptic curve over $\mathbf{A}_n$, noted $\mathbf{E}_{a,b}^n(\mathbf{A}_n)$ as a curve that is given by such Weiestrass equation:

$$Y^2Z=X^3+aXZ^2+bZ^3,$$

where $a,b\in\mathbf{A}_n$ and $4a^3+27b^2$ is invertible in $\mathbf{A}_n$.
So we have:

$$\mathbf{E}_{a,b}^n(\mathbf{A}_n)=\{[X:Y:Z]\in\mathbb{P}_n(\mathbf{A}_n)/Y^2Z=X^3+aXZ^2+bZ^3\}.$$

The set $\mathbf{E}_{a,b}^n(\mathbf{A}_n)$ together with special point $\mathcal{O}$ (called the point infinity) has a commutative binary operation denote by $+$. It is well known that the binary operation $+$ endows the set $\mathbf{E}_{a,b}^n(\mathbf{A}_n)$ with an abelian group with $\mathcal{O}$ as identity element. For more results on these curves has different characteristics, we can see the following references: [2, 5, 10].

Let $\mathrm{X}\in\mathbf{A}_n$, $\mathrm{Y}\in\mathbf{A}_n$, $\mathrm{Z}\in\mathbf{A}_n$, They exist $x_i\in\mathbb{F}_{p^d}$, $y_i\in\mathbb{F}_{p^d}$, $z_i\in\mathbb{F}_{p^d}$ such that:

$$\mathrm{X}=x_0+x_2\epsilon+....+x_{n-1}\epsilon^{n-1}$$

$$\mathrm{Y}=y_0+y_2\epsilon+....+y_{n-1}\epsilon^{n-1}$$

$$\mathrm{Z}=z_0+z_2\epsilon+....+z_n\epsilon^{n-1}$$

Our Matrix representation:
In [9]; the author's has classifies the points of the elliptic curve over $\mathbf{A}_n$ as follow:
Let $[\mathrm{X}:\mathrm{Y}:\mathrm{Z}]\in\mathbf{E}_{a,b}(\mathbb{F}_{p^d}[\epsilon]); d=1$
If Z is invertible then $[\mathrm{X}:\mathrm{Y}:\mathrm{Z}]\rightsquigarrow[\mathrm{X}:\mathrm{Y}:1]$, else $[\mathrm{X}:\mathrm{Y}:\mathrm{Z}]\rightsquigarrow[\mathrm{X}:1:\mathrm{Z}]$.
We will see how to represent a point $\mathcal{P}[\mathrm{X}:\mathrm{Y}:\mathrm{Z}]$ of an elliptic curve with a matrix, we denote the matrix by $\mathbf{L}$.

We use the coordinates of X, Y, Z to build a type $3 \times n$ matrix :

$$\begin{pmatrix} x_0 & x_1 & ... & x_{n-1} \\ y_0 & y_1 & ... & y_{n-1} \\ z_0 & z_1 & ... & z_{n-1} \end{pmatrix}$$

Which one multiplies by its transpose one obtains then a square matrix of order n, that is the matrix representation of the point$\mathcal{P}$[X : Y : Z] :

$$\mathbf{L} = \begin{pmatrix} x_0^2 + y_0^2 + z_0^2 & ... & x_0x_i + y_0y_i + z_0z_i & ... & x_0x_n + y_0y_n + z_0z_n \\ ... & ... & ... & ... & ... \\ x_ix_0 + y_iy_0 + z_iz_0 & ... & x_i^2 + y_i^2 + z_i^2 & ... & x_ix_n + y_iy_n + z_iz_n \\ ... & ... & ... & ... & ... \\ x_{n-1}x_0 + y_{n-1}y_0 + z_{n-1}z_0 & ... & x_{n-1}x_i + y_{n-1}y_i + z_{n-1}z_i & ... & x_{n-1}^2 + y_{n-1}^2 + z_{n-1}^2 \end{pmatrix}$$

5. Hybrid Cryptosystem

In this section we introduce an hybrid Cryptosystem based on two difficult problems namely: Discrete logarithm problem on $\mathbf{E}_{a,b}^n(\mathbf{A}_n)$ and the conjugate problem on square matrix. The encryption of message is done with a bad basis of the lattice.

5.1. **Key exchange protocol.** Alice and Bob have agreed on an elliptic curve over $\mathbf{E}_{a,b}^n(\mathbf{A}_n)$, n is the dimension of the Lattice and a "base point" $\mathcal{P}$ on the curve of order m.
1- Alice chooses secret large random $0 \leq c \leq m-1$ and compute $\mathbf{K}_A = c\mathcal{P}$
2- Alice sends $\mathbf{K}_A$ to Bob.
3- Bob chooses secret large random number $0 \leq e \leq m-1$ and compute $\mathbf{K}_B = e\mathcal{P}$
4- Bob sends $\mathbf{K}_A$ to Alice.
5- Alice and Bob compute their secret key $\mathbf{Q} = ce\mathcal{P} = ec\mathcal{P}$
6- Alice and Bob transform the point $\mathbf{Q}$ of the curve into a square matrix $\mathbf{K}$.
If $\mathbf{K}$ is not invertible then return to (1). Else the secret key of Alice and Bob is the matrix $\mathbf{K}$.

5.2. **Parameters.** The system relies on several parameters:
- The lattice dimension n
- The public key consists of a public matrix $\mathbf{B}$ which is a bad basis of the lattice in the sense that is not reduced, the elliptic curve over $\mathbf{E}_{a,b}^n(\mathbf{A}_n)$, and a "base point" $\mathcal{P}$ on the curve of order m.
The private key consists of secret matrix $\mathbf{K}$. $\mathbf{KB} \neq \mathbf{BK}$

5.3. **Encryption and Decryption.** One transform a point of the curve into a matrix that gives the private key; $\mathbf{K}$. In this case we do not need to look for the vector error and we do not need to add the vector error to the message, which minimizes time and space.

5.3.1. *Encryption Message.* To encrypt a message, encode it as an integral $\mathbf{m} \in \mathbb{Z}^n$, we compute $\mathbf{B}' = \mathbf{K}^{-1}\mathbf{B}\mathbf{K}$ and the ciphertext $\mathbf{c} = \mathbf{B}'\mathbf{m}$ is not a vector of lattice.

5.3.2. *Decryption Message.* To decrypt a ciphertext $\mathbf{c}$, we compute :$\mathbf{B}^{'-1}\mathbf{c} = \mathbf{B}^{'-1}\mathbf{B}^{'}\mathbf{m} = \mathbf{m}$ and we retrieve the message $\mathbf{m}$.

5.3.3. *Parameters and comparison.* In this section we will make a comparison between our cryptosystem and the GGH cryptosystem:In the GGH public key cryptosystem one chooses a nice basis $\mathbf{B}$ for a lattice $\mathcal{L}$ and publishes a disguised basis $\mathbf{B}^{'} = \mathbf{UB}$ for $\mathcal{L}$ where $\mathbf{U}$ is a random unimodular matrix. A message $\mathbf{m}$ is encrypted as $\mathbf{c} = \mathbf{B}^{'}\mathbf{m} + \mathbf{e}$, where $\mathbf{e}$ is a randomly chosen short error vector. To decrypt one solves the closest vector problem using the nice basis $\mathbf{B}$, to obtain the lattice point $\mathbf{B}^{'}\mathbf{m}$ close to $\mathbf{c}$, on can then obtain $\mathbf{m}$. GGH relies on two parameters, the lattice dimension n and the security parameter σ where the error vector is taken randomly from $\{-\sigma, \sigma\}^n$. In our contribution we do not need The error vector.

Parameter	Parameters of GGH	Parameters of our contribution
n	Public Dimension	Public Dimension
σ	Public security parameter	We do not need The error vector
$\mathbf{K}$	Square private Matrix	Square private Matrix
$\mathbf{B}$	Square public Matrix	Square public Matrix

Table 3.1: Parameters and comparison

5.3.4. *Cryptanalysis of our Encryption.* We now discuss the one-way encryption security of the GGH cryptosystem under passive attacks and the security of our cryptosystem: There are three natural ways to attack the GGH cryptosystem:
1- Try to obtain the private key $\mathbf{K}$ from the public key $\mathbf{B}$, however our encryption method has indistinguishability security under this attack.
2- Try to obtain information about the massage from the ciphertext, we use the attack of Nguyen's based on two flaws in the GGH system. The first is that the error vectors are always very short when compared with the lattice vectors. The second flaws is based on the choice of the error vector. However our method is efficient system because it does not depend on error vector. So we could avoid the Nguyen's attack.
3- Try to solve the CVP of the encryption message $\mathbf{c}$ with respect to the lattice $\mathcal{L}$ defined by $\mathbf{B}$. So, our encryption is secure against this attack because the security of this method is based on two hard problem: The problem of the discrete logarithm on an elliptic curve defined on a finite local ring and the conjugate problem on square matrices.

5.4. **Homomorphic encryption.** Cloud computing provides accesses to many on-line services, and remote computing resources as needed, the major problem that keeps many companies, including banks to migrate to the cloud is the security of sensitive data hosted in the cloud, encrypt data before sending it to the cloud server is mandatory, but to respond to a client request, it is necessary that the cloud server has access to the clear data (so the client must provide the decryption key). A method to perform operations on encrypted without having any

information about it(without decryption) is the Homomorphic encryption witch allows certain types of operations to be carried out on the encrypted data, without the need to decrypt them. Many schemas are partially homomorphic. In 2009 Gentry presented the first fully homomorphic encryption scheme: totally impracticable. If $(G_1, *)$ and $(G_2, \otimes)$ are two groups, then a function $f : G_1 \longrightarrow G_2$ is a group homomorphism if:

$$f(x * y) = f(x) \otimes f(y), \forall x, y \in G_1$$

Partially homomorphic encryption:
- Additively homomorphic: $Enc(x + y) = Enc(x) + Enc(y)$
- Multiplicatively homomorphic: $Enc(x \times y) = Enc(x) \times Enc(y)$

Fully homomorphic encryption (FHE):
Fully homomorphic encryption allows to do arbitrary computations on encrypted data without decrypting it. It is homomorphic with respect to both multiplication and addition.
Our cryptosystem is additively homomorphic:
Let $\mathbf{m}_1$ and $\mathbf{m}_2$ are two messages, we have:

$$Enc(\mathbf{m}_1 + \mathbf{m}_2) = Enc(\mathbf{m}_1) + Enc(\mathbf{m}_2)$$

6. Digital signature

Hash function or hash algorithm creates a unique digital fingerprint of data. The digital fingerprint of data is called digest or message digest or simply hash. Hash algorithm is primarily used for comparison purpose, not for encryption. Many secure hash algorithms have three characteristics.
1- Secure: Non reversible function (on way function).
2- Fixed size: short or long data will produce the fixed-size data.
3- Unique: two different data sets cannot produce the same digest.
Hash function is commonly used for passwords and for digital signature. The concept of digital signatures was first described by Diffie and Hellman as one of the possible application of asymmetric cryptography. It can be described as the dual of public-key cryptography. In a public-key encryption scheme messages are encrypted using a public key and decrypted using the corresponding public key. In a digital signature scheme this is reversed: a message is signed using a private key and this signature can be verified using the corresponding public key.
A digital signature serves three purposes:
1- Authentication: A digital signature gives the receiver reason to believe the message was created and sent by the claimed sender.
2- Non-repudiation: With digital signature, the sender cannot deny having sent the message later on.
3- Integrity: A digital signature ensures that the message was not alerted in transit.
How it works:
Digital signature uses asymmetric cryptography. First the sender generate two keys public and private key, and after creating a memo he generate a digest by hashing his memo using some hash algorithm. He encrypt the digest with his

private key, this encrypting digest is the digital signature for the memo. Then he sends both the memo and the digital signature to the receiver. Notice the memo is not encrypted.
When the receiver receives them she will do two thing: He decrypt the digital signature using the public key and he get the digest and he hashes the memo by the same hash algorithm, if it equal to the digest the memo was signed by the holder the private key.

6.1. **GGH digital signature scheme.** Let $\mathbf{B}$ a GGH public key corresponding to a lattice $\mathcal{L}$ in $\mathbb{Z}^n$. The natural signature scheme is as follows: Given a message $\mathbf{m}$ hash it to a random element $H(\mathbf{m}) \in \mathbb{Z}^n$. Then, using the private key, compute a lattice vector $\mathbf{s}$ close to $H(\mathbf{m})$. The signature on message $\mathbf{m}$ is then $\mathbf{s}$. To verify the signature one checks that $\mathbf{s}$ lies in the lattice $\mathbf{B}^{-1}(\mathbf{s}) \in \mathbb{Z}^n$ and that $\|\mathbf{s}-H(\mathbf{m})\|$ is smaller.
To analyse the security of such a signature is required to use lattices for large dimensions $n \geq 200$. Furthermore, as usual for signature, on must also consider the fact that an adversary could obtain signatures on messages and that leak information about the private key. For the GGH signature scheme on see that $\mathbf{s}-H(\mathbf{m})$ is a short vector in $\mathbb{R}^n$ and always lies in the parallelepiped which called a fundamental domain for the lattice, whose sides are determined by the basis vectors in the private bases.
Nguyen and Regev have explored this idea and shown that such an approach can be used to cryptanalyses signatures.
Adding a perturbation to the signature seems to prevent the attack of Nguyen and Regev. Gentry, Peikert and Vainkuntanathan give a method to sample from a lattice such that the output is statistically close to a Gaussian distribution. Hence their paper gives a secure implementation of the GGH signature concept.

6.2. **Our digital signature scheme.** Our digital signature is as follow:
Given a message $\mathbf{m}$ hash it to a random element $H(\mathbf{m}) \in \mathbb{Z}^n$, we compute $\mathbf{s} = \mathbf{B}^{'}H(\mathbf{m})$ and send $(\mathbf{m}, \mathbf{s})$ where $\mathbf{K}$ and $\mathbf{B}^{'} = \mathbf{K}^{-1}\mathbf{B}\mathbf{K}$ are the secret keys.
To check the signature, we calculate $H(\mathbf{m})$, $\mathbf{B}^{'-1}\mathbf{s}$ and compare them if they are equal, the message is well signed, otherwise we reject it.

References

1. M. Ajtai, *Gererating Hard instances of lattice problems,* In proceedings of the 28^{th} ACM symposium on theory of computing, New York, USA,(2015).
2. A. Boulbot, A. Chillali, A. Mouhib, *Elliptic curves over a ring*$Fq[e]; e^3 = e^2$, Gulf Journal of Mathematics, Vol 4, Issue 4, pp 123-129, (2016).
3. A. Chillali, *Elliptic Curves of the Ring* $F_q[\epsilon]$, $\epsilon^n = 0$, International Mathematical Forum. (2011).
4. O. Goldreich, S. Goldwasser, S. Halevi, *Public-key cryptosystems from lattice reduction problems,* In B. Kaliski editor, Advences in cryptology-CRYPTO'97, volume 1294 of lecture notes in computer science, pages 112-131 Springer Berlin/ Heidelberg, (1997).

5. MH. Hassib, A. Chillali, MA. Elomary, *Elliptic curves over a chain ring of characteristic 3,* Journal of Taibah University for Science, Vol(9), 3, pp. 276-287, (2015).
6. D. Micciancio, *Lattice -based cryptography,* University of California, San diego, (2003).
7. D. Miccinco, O. Regev, *Lattice- based cryptography,* In Proceedings of cryptography 2009, Springer, page 577-594,(2008).
8. T. Plantard, M. Rose, S. Willy, *Improvement of Lattice based cryptography using CRT,* School of computer and software Engineering. University of Wollongong NSW Australia, (2009).
9. A. Tadmori, A. Chillali, M. Ziane, *Elliptic Curve over Ring A_4,* Applied Mathematical Sciences Vol(9), 33, pp. 1721-1733,(2015).
10. A. Tadmori, A. Chillali, M. Ziane, *Cryptography over the elliptic curve $E_{a,b}(A_3)$,* Journal of Taibah University for Science, Vol(9), 3, pp. 326-331, (2015).

[1] Department of Mathematics, Physical and Computer Sciences, Sidi Mohamed ben Abdellah University, FP, LSI, Taza, Morocco
Email address: abouaminem@gmail.com

[2] Department of Mathematics, Physical and Computer Sciences, Sidi Mohamed ben Abdellah University, FP, LSI, Taza, Morocco
Email address: abdelhakim.chillali@usmba.ac.ma

[3] Department of Mathematics, Physical and Computer Sciences, Sidi Mohamed ben Abdellah University, FP, LSI, Taza, Morocco
Email address: mouhibali@yahoo.fr