A cryptosystem "à la" ElGamal on an elliptic curve over $\mathbb{F}_p[\varepsilon]$

Marie Virat
Laboratoire J.A. Dieudonné
Université de Nice Sophia-Antipolis, Nice, France
virat@math.unice.fr

Abstract: This paper introduces a new public key cryptosystem which is a variant of the ElGamal cryptosystem on an elliptic curve. To this end, we study the equations of type $y^2 = x^3 + ax + b$ with $a$ and $b$ in $\mathbb{F}_q[\varepsilon]$ where $\varepsilon^2 = 0$. When $4a^3 + 27b^2$ is invertible in $\mathbb{F}_q[\varepsilon]$, they allow us to define new groups which seem to be good candidates for the ElGamal public key cryptosystem. The variant we introduce has the advantage to present no plaintext encoding problem. Moreover, it reaches security levels which are similar to the ElGamal cryptosystem on an elliptic curve.

Keywords: ElGamal public key cryptosystem, elliptic curves, semantic security

1 Introduction

In this paper, we observe that the ElGamal public key cryptosystem on a finite group $G$ imposes a plaintext to belong to $G$. When considering the group of $\mathbb{F}_q$-rational points of an elliptic curve $E$, where $q$ is a power of a prime $p$, it is not so easy to encode a plaintext with an element of $E(\mathbb{F}_q)$. On the other hand, for a cryptosystem, the elliptic curves give the advantage to require shorter keys. There already exist various methods to solve the encoding problem. Our approach is to make things such that there is no problem at all. We achieve this goal by using equations of type $y^2 = x^3 + ax + b$ with $a$ and $b$ in $\mathbb{F}_q[\varepsilon]$ where $\varepsilon^2 = 0$. When $4a^3 + 27b^2$ is invertible in $\mathbb{F}_q[\varepsilon]$, they allow us to define new groups which seem to be good candidates for the ElGamal public key cryptosystem. The variant we introduce reaches security levels which are similar to the ElGamal cryptosystem on an elliptic curve.

This paper is organized as follows. In section 2, we recall the ElGamal public key cryptosystem on an abelian finite cyclic group and some problems related to its security. Then in section 3, we define the group of elements of a Weierstrass cubic curve on the ring $\mathbb{F}_q[\varepsilon]$ where $\varepsilon^2 = 0$. In section 4, we give a result on its group structure and we relate
the difficulty to solve the underlying problems of ElGamal encryption over a Weierstrass cubic curve on $\mathbb{F}_q[\epsilon]$ to the ones over an elliptic curve. In section 5, we present two methods to solve the encoding problem. Then we introduce our new cryptosystem which is a variant of ElGamal encryption. Finally, in section 6 we study security aspects of our cryptosystem.

2 ElGamal public key cryptosystem, underlying problems

Consider an abelian finite cyclic group $(G, +)$ of order $n$. The ElGamal public key cryptosystem is defined as follows:

Key generation algorithm $K \rightarrow (P_k, s_k)$
1. Choose an element $P$ generator of $G$.
2. Randomly choose $s_k$ an integer between 2 and $n - 1$.
3. Compute $P_k = s_kP$.

Encryption algorithm of $M$ in $G$: $E_{P_k}(M; r) \rightarrow (C_1, C_2)$
1. Randomly choose $r$ an integer between 2 and $n - 1$.
2. Compute $C_1 = rP$ and $C_2 = M + rP_k$ in $G$.

Decryption algorithm of $(C_1, C_2)$: $D_{s_k}(C_1, C_2) \rightarrow M$
1. Compute $C_2 - s_kC_1 = M$

Obviously, the security of this cryptosystem depends on the group $G$. In particular, it is related to the discrete logarithm problem. Its statement follows:

Discrete Logarithm problem over $(G, +)$ of base $P$
For $A$ in $\langle P \rangle$, find an integer $\alpha$ such that $A = \alpha P$.

An adversary who solves this problem can compute the secret key given only the public one within the same time. In particular, the groups chosen for the construction of an ElGamal cryptosystem must resist the Discrete Logarithm problem. Some groups do not resist, as, obviously, $(\mathbb{F}_p, +)$ for a prime $p$. Some others are prone to specific attacks like for a power $q$ of a prime, $(\mathbb{F}_q^*, \times)$ [BW98] or the group of $\mathbb{F}_q$-rational points of an hyperelliptic
curve of genus strictly higher than four [Gau00].

Some groups always resist the Discrete Logarithm problem, and are not (yet) prone to specific attacks. This is the case for the group of the \( \mathbb{F}_q \)-rational points of certain elliptic curves \( (E(\mathbb{F}_q), +) \). Nevertheless, some elliptic curves do not resist the Discrete Logarithm problem, for instance, when the number of \( \mathbb{F}_q \)-rational points of the curve is divisible by the characteristic \( p \) of \( \mathbb{F}_q \) [[Sma99],[Sem98],[AS98]].

We list some other problems related to the study of ElGamal public key cryptosystem security we will use:

**Computational Diffie Hellman problem over \((G, +)\) of base \(P\):**
Given \( A = \alpha P \) and \( B = \beta P \) in \( G \), compute \( \alpha \beta P \).

**Decisional Diffie Hellman problem over \((G, +)\) of base \(P\):**
Given \( A = \alpha P \), \( B = \beta P \) and \( C \) over \( G \), decide whether \( C = \alpha \beta P \).

Of course, an algorithm for solving the Discrete Logarithm problem over \( G \) of base \( P \) necessarily solves the corresponding Computational Diffie Hellman problem, and in turn the corresponding Decisional Diffie Hellman problem in the same time.

Moreover, if there exists an isomorphism \( \phi \) from a group \( G \) to a group \( G' \) computable in a time polynomial in \( \log(|G|) \), then each computational problem over \( G \) of base \( P \) is equivalent to the corresponding problem over \( G' \) of base \( \phi(P) \), in the sense that polynomial transformations in \( \log(|G|) \) from one to the other can be constructed [GJ79].

In the next section, we focus on a specific abelian finite group.

## 3 Weierstrass cubic curve over \( \mathbb{F}_q[\varepsilon] \) and its group structure

Consider a finite field \( \mathbb{F}_q \) of characteristic \( p \) different from 2 and 3 and the ring \( \mathbb{F}_q[\varepsilon] \) where \( \varepsilon^2 = 0 \). Its elements are written in the form \( x_0 + x_1 \varepsilon \) with \( x_0 \) and \( x_1 \) in \( \mathbb{F}_q \). We call \( x_1 \) the infinitesimal part and \( x_0 \) the constant one. Its non invertible elements are of type \( k \varepsilon \) with \( k \) in \( \mathbb{F}_q \).

Moreover, this ring projects canonically on \( \mathbb{F}_q \). We denote this projection by \( \pi \):

\[
\pi(a_0 + a_1 \varepsilon) = a_0.
\]

In this section, we will give some definitions useful for implementations. They are linked to algebraic geometry notions and schemes theory.

**Definition 3.1** A Weierstrass equation over \( \mathbb{F}_q[\varepsilon] \) is an equation of type \( y^2 = x^3 + ax + b \) with \( a \) and \( b \) in \( \mathbb{F}_q[\varepsilon] \). Then the reduction on \( \mathbb{F}_q \) of such an equation is \( y^2 = x^3 + \pi(a)x + \pi(b) \).
Consider a Weierstrass equation over \( \mathbb{F}_q[e] \). It defines a Weierstrass cubic curve over \( \mathbb{F}_q[e] \), if and only if \( 4a^3 + 27b^2 \) is invertible in \( \mathbb{F}_q[e] \).

**Lemma 3.2** A Weierstrass equation over \( \mathbb{F}_q[e] \) defines a Weierstrass cubic curve if and only if its reduction on \( \mathbb{F}_q \) defines an elliptic curve.

**Proof.** \( 4a^3 + 27b^2 \) is invertible in \( \mathbb{F}_q[e] \) if and only if \( \pi(4a^3 + 27b^2) \neq 0 \) if and only if \( 4\pi(a)^3 + 27\pi(b)^2 \neq 0 \) if and only if \( y^2 = x^3 + \pi(a)x + \pi(b) \) defines an elliptic curve on \( \mathbb{F}_q \).

**Definition 3.3** Let \( E_{a,b} \) the Weierstrass cubic curve defined by the equation \( y^2 = x^3 + ax + b \) in \( \mathbb{F}_q[e] \). Then we define the set \( \mathcal{E}_{a,b}(\mathbb{F}_q[e]) \) of elements of the Weierstrass cubic curve by the union of two disjoined sets. The elements of these sets are :

- for the first one : the elements at infinity \( \Theta_k \) for all \( k \) in \( \mathbb{F}_q \).
- for the second one : the elements of type \( P = (x_0 + x_1 e, y_0 + y_1 e) \) which satisfy the following system of equations in \( \mathbb{F}_q \)

\[
\begin{align*}
\left\{ \\
y_0^2 &= x_0^3 + a_0x_0 + b_0 \\
(2y_0)y_1 &= (3x_0^2 + a_0)x_1 + a_1x_0 + b_1 \\
\end{align*}
\]

where \( a = a_0 + a_1 e \) and \( b = b_0 + b_1 e \) with \( a_0, a_1, b_0, b_1 \in \mathbb{F}_q \).

Then, an element at finite distance is an element \( (x_0 + x_1 e, y_0 + y_1 e) \) such that \( (x_0, y_0) \) is in \( E_{\pi(a), \pi(b)}(\mathbb{F}_q) \) and \( (x_1, y_1) \) is on the line given by the equation

\( (2y_0)y_1 = (3x_0^2 + a_0)x_1 + a_1x_0 + b_1 \) with coefficients in \( \mathbb{F}_q \).

The set \( \mathcal{E}_{a,b}(\mathbb{F}_q[e]) \) of the elements of the Weierstrass cubic curve naturally projects on the set of the \( \mathbb{F}_q \)-rational points of the underlying elliptic curve as follows :

\[
\begin{align*}
\pi_{E_{a,b}} : \mathcal{E}_{a,b}(\mathbb{F}_q[e]) & \rightarrow E_{\pi(a), \pi(b)}(\mathbb{F}_q) \\
\Theta_k & \mapsto \Theta \\
(x, y) & \mapsto (\pi(x), \pi(y))
\end{align*}
\]

where \( \Theta \) denotes the infinity point in \( E_{\pi(a), \pi(b)}(\mathbb{F}_q) \).

The usual cord and tangent operations on a set like \( \mathcal{E}_{a,b}(\mathbb{F}_q[e]) \) provide a group law with identity element \( \Theta_0 \) [Gal02]. It allows us to define explicitly a group law for which \( \pi_{E_{a,b}} \) is a group morphism. In the sequel of this paper, we will denote \( \pi_{E_{a,b}} \) and \( \pi \) similarly by \( \pi \).

In the next section, we focus on the equivalence between computational problem on the set of elements of Weierstrass cubic curve on \( \mathbb{F}_q[e] \) and on the set of \( \mathbb{F}_q \)-rational points of its reduction.
4 Equivalent problems

**Lemma 4.1** Let $\mathbb{F}_q$ be a finite field of characteristic $p$ different of 2 and 3, $a$ and $b$ in $\mathbb{F}_q[e]$ such that the equation $y^2 = x^3 + ax + b$ defines a Weierstrass cubic curve on $\mathbb{F}_q[e]$. We denote by $\mathbb{N}$ the cardinal of the set $E_{\pi(a), \pi(b)}(\mathbb{F}_q)$. If $p$ does not divide $\mathbb{N}$, then there exists a group isomorphism between $E_{\pi(a), \pi(b)}(\mathbb{F}_q[e])$ and $E_{\pi(a), \pi(b)}(\mathbb{F}_q \times \mathbb{F}_q)$ which is computable in polynomial time in $\log(q)$.

**Proof.** We denote by $\pi$ the residue class of an integer $u$ in $\mathbb{F}_p$. The characteristic $p$ does not divide $\mathbb{N}$, so we denote by $[\mathbb{N}^{-1}]$ the unique integer $u$ in $[1, p-1]$ such that $\pi = \mathbb{N}^{-1}$ in $\mathbb{F}_p$. And for each element at infinity $\Theta_k$, we denote $[\Theta_k] = k$.

Consider the following application :

$$
\Lambda : E_{a, b}(\mathbb{F}_q[e]) \rightarrow E_{\pi(a), \pi(b)}(\mathbb{F}_q) \times \mathbb{F}_q \\
P \mapsto (\pi(P), [\mathbb{N}^{-1}] P)
$$

Due to the equality $\mathbb{N} \pi(P) = \Theta$ in $E_{\pi(a), \pi(b)}(\mathbb{F}_q)$, $\mathbb{N} [\mathbb{N}^{-1}] P$ is an element at infinity of $E_{a, b}(\mathbb{F}_q[e])$. So $\Lambda$ is well defined. The application $\pi$ is a morphism and the group law in $E_{a, b}(\mathbb{F}_q[e])$ satisfies $\Theta_k + \Theta_{k'} = \Theta_{k+k'}$. So it is easy to verify that $\Lambda$ is a morphism. Now consider the application $f$ :

$$
f : E_{\pi(a), \pi(b)}(\mathbb{F}_q) \times \mathbb{F}_q \rightarrow E_{a, b}(\mathbb{F}_q[e]) \\
(P, k) \mapsto (1 - \mathbb{N} [\mathbb{N}^{-1}]) P + \Theta_k
$$

where $P$ denotes any lift of $P$ (a lift $P$ of $P$ is a point of $E_{a, b}(\mathbb{F}_q[e])$ which satisfies $\pi(P) = P$).

Firstly, this application is well defined : let $P_1$ and $P_2$ be two lifts of $P$ in $E_{a, b}(\mathbb{F}_q[e])$, we have : $(1 - \mathbb{N} [\mathbb{N}^{-1}]) P_1 - (1 - \mathbb{N} [\mathbb{N}^{-1}]) P_2 = (1 - \mathbb{N} [\mathbb{N}^{-1}]) (P_1 - P_2)$. However there exists $u$ in $\mathbb{F}_q$ such that $(P_1 - P_2) = \Theta_u$ due to $\pi(P_1 - P_2) = P - P = \Theta$. Also there exists an integer $v$ such that $1 - \mathbb{N} [\mathbb{N}^{-1}] = vp$ in $\mathbb{Z}$.

So $(1 - \mathbb{N} [\mathbb{N}^{-1}]) P_1 - (1 - \mathbb{N} [\mathbb{N}^{-1}]) P_2 = vp\Theta_u = \Theta_{vp}\Theta_u = \Theta_0$. And $f$ is well defined.

Secondly, $f$ is the inverse of $\Lambda$ :

- **let $P$ an element of $E_{a, b}(\mathbb{F}_q[e])$**, we have :
  \[
  f \circ \Lambda(P) = f(\pi(P), [\mathbb{N} [\mathbb{N}^{-1}]) P)) = (1 - \mathbb{N} [\mathbb{N}^{-1}]) P + \Theta_{[\mathbb{N} [\mathbb{N}^{-1}]) P} = (1 - \mathbb{N} [\mathbb{N}^{-1}]) P + \mathbb{N} [\mathbb{N}^{-1}]) P = P
  \]

- **let $(P, k)$ an element of $E_{\pi(a), \pi(b)}(\mathbb{F}_q) \times \mathbb{F}_q$**, we denote by $P$ any lift of $P$ in $E_{a, b}(\mathbb{F}_q[e])$ and we have :
  \[
  \Lambda \circ f(P, k) = \Lambda((1 - \mathbb{N} [\mathbb{N}^{-1}]) P + \Theta_k) = (\pi((1 - \mathbb{N} [\mathbb{N}^{-1}]) P + \Theta_k), [\mathbb{N} [\mathbb{N}^{-1}] ((1 - \mathbb{N} [\mathbb{N}^{-1}]) P + \Theta_k))
  \]
The Discrete Logarithm problem is easily solved on $E$ Let over curve on $E$ so, it may be interesting to consider an ElGamal cryptosystem over a Weierstrass cubic curve $E$. Similar theorem stand for the Computational Diffie-Hellman problem. Theorem 4.2: Let $E_{a,b}(\mathbb{F}_q[\varepsilon])$ be a Weierstrass cubic curve on $\mathbb{F}_q[\varepsilon]$ and $P$ an element of $E_{a,b}(\mathbb{F}_q[\varepsilon])$: if $p$ does not divide $N$, then the Discrete Logarithm problems over $E_{a,b}(\mathbb{F}_q[\varepsilon])$ of base $P$ and over $E_{\pi(a),\pi(b)}(\mathbb{F}_q)$ of base $\pi(P)$ are equivalent.

Then, $\pi((1 - N[N^{-1}])P + \Theta_k) = \pi(P) - N\pi([N^{-1}]P) + \pi(\Theta_k)$
$= P - \Theta + \Theta = P$;
and, $[N[N^{-1}]((1 - N[N^{-1}])P + \Theta_k)]$
$= [N[N^{-1}]((1 - N[N^{-1}])NP + [N^{-1}]N\Theta_k)]$
$= [N[N^{-1}](\epsilon_p\Theta[NP] + (1 - \epsilon_p)\Theta_k)] = [\Theta[N^{-1}]\epsilon_p[NP]+(1-\epsilon_p)k]$.

So, $\pi$ is the inverse of $\Lambda$ which is an isomorphism.
Finally, $\Lambda$ and its inverse are computable in polynomial time in $\log(q)$ due to the efficiency of each computation: the group law is computable in a polynomial time in $\log(q)$, a lift in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ in a constant time (choosing a random value for the infinitesimal part of $x$ or $y$); and computing $N$ requires a polynomial time in $\log(q)$ thanks to the SEA algorithm [Ler97].

The Discrete Logarithm problem is easily solved on $E$. Then from lemma 4.1 comes theorem 4.2:

**Theorem 4.2** Let $E_{a,b}(\mathbb{F}_q[\varepsilon])$ be a Weierstrass cubic curve on $\mathbb{F}_q[\varepsilon]$ and $P$ an element of $E_{a,b}(\mathbb{F}_q[\varepsilon])$: if $p$ does not divide $N$, then the Discrete Logarithm problems over $E_{a,b}(\mathbb{F}_q[\varepsilon])$ of base $P$ and over $E_{\pi(a),\pi(b)}(\mathbb{F}_q)$ of base $\pi(P)$ are equivalent.

Similar theorem stand for the Computational Diffie-Hellman problem.

So, it may be interesting to consider an ElGamal cryptosystem over a Weierstrass cubic curve on $\mathbb{F}_q[\varepsilon]$ for which the reduction on $\mathbb{F}_q$ resists the Discrete Logarithm problem.

**Remark.** choice of good initialization parameters for an ElGamal cryptosystem over $E_{a,b}(\mathbb{F}_q[\varepsilon])$.

Let $E_{a,b}$ a Weierstrass cubic curve on $\mathbb{F}_q[\varepsilon]$ such that $p$ does not divide the cardinal $N$ of $E_{\pi(a),\pi(b)}(\mathbb{F}_q)$. Then if $E_{a,b}(\mathbb{F}_q[\varepsilon])$ is cyclic, we can choose a generator $P$ of $E_{a,b}(\mathbb{F}_q[\varepsilon])$ and a secret key $sk$ in $[2, Nq - 1]$. Due to the Euclidean division, we have $sk = \alpha q + \beta$ with $\alpha \in [0, N - 1]$ and $\beta \in [0, q - 1]$. The isomorphism $\Lambda$ of lemma 4.1, allows us to find easily the value of $\beta$: we have $[N[N^{-1}]skP] = \alpha q[N[N^{-1}]P] + \beta[N[N^{-1}]P] = \beta[N[N^{-1}]P]$ and, we can compute the value of $\beta$ if $N[N^{-1}]P \neq 0$. Then it is as hard to find $sk$ than $\alpha$. So, it is useless to choose secret keys between 2 and $Nq - 1$: we can just choose secret keys between 2 and $N - 1$ and compute the corresponding public key $Pk = skP$.

In the next section, we will construct a cryptosystem "à la" ElGamal on an elliptic curve over $\mathbb{F}_p[\varepsilon]$. 

37
5 Cryptosystem We

5.1 Encoding problem: some existing solutions

With the ElGamal cryptosystem over a finite cyclic group $G$ defined in section 2, the plaintext has to be encoded by an element of $G$. With $G$ the set of $\mathbb{F}_q$-rational points of an elliptic curve, this type of encoding is not trivial: an element of $E_{a_0, b_0}(\mathbb{F}_q)$ is written in the form $(x_0, y_0)$ where $y_0^2 = x_0^3 + a_0 x_0 + b_0$. For instance, if we want to encode a plaintext by the value $x_0$, this one must be such that $x_0^3 + a_0 x_0 + b_0$ is a square in $\mathbb{F}_q$. But this condition is not satisfied by all $x_0$ in $\mathbb{F}_q$ and we cannot encode all the plaintexts so easily.

Some solutions to this problem have been found.

The following one is described in [Men93]. The coordinates $(x, y)$ of the point $rP$ are used to mask a plaintext $(m_1, m_2)$ in $\mathbb{F}_q^2$. If $x = 0$ and $y = 0$, then the ciphertext is $(rP, x_m, y_m)$. The decryption is easy when the private key is known: $(x, y) = rP$ is recovered by computing $sk rP$ and then the plaintext is obtained by two divisions. Then no specific condition is imposed to $m_1$ and $m_2$, and the encoding problem is solved.

But this method has a drawback: if an adversary finds a half of the plaintext e.g. $m_2$, then he can compute $y$ and therefore some possible values of $x$ by solving $X^3 + aX + b - y^2 = 0$ within a time polynomial in $\log q$. Then this adversary knows $m_1$ with at least a probability of $1/3$. As a consequence, the security of this method can be improved by sending the ciphertext $(rP, x_m)$. Nevertheless, even so, a drawback persists. Suppose an adversary intercepts a ciphertext $(rP, x_m)$, then he can easily compute $s(m) = x_m m^{-1}$ for all values $m$ in $\mathbb{F}_q$. So, he can test if a value $m$ is a possible plaintext for the intercepted ciphertext. Indeed, this function $s$ satisfies $s(m_1) = x$, and then $s(m_1)^3 + as(m_1) + b$ is a square in $\mathbb{F}_q$. In order to test a value $m$ to be a possible plaintext, he computes $s(m)^3 + as(m) + b$; if this last value is not a square in $\mathbb{F}_q$, then $m$ cannot be the expected plaintext. So, the enemy can eliminate a number of order $q/2$ of candidates to be the corresponding plaintext of a given ciphertext.

About the transmission rate of this method, it can be improved by compression of points of an elliptic curve. It consists to send the first coordinate of a point and only one bit corresponding to one of the two possible values of the second coordinate. With this method, assuming that Alice and Bob know the generator $P$, then $2 \log(q) + 1$ bits are sent in order to encrypt a plaintext of $\log(q)$ bits. So the transmission rate of this method is close to 1/2.

Another idea is presented in [Joy95]. Here $q$ is a large prime. Some successive values of the first coordinate $\tilde{x}$ can be tested in order to give a representant of a plaintext $m$. The user fixes a number $k$ of successive values to test (with $k < q$) and a number $M < q/k$ which maximizes the number of plaintext he can send using this method. Then a plaintext $m \in [0, M - 1]$ can be represented by a point of first coordinate $\tilde{x} = km + j$ for a value $j \in [1, k]$. After encryption and decryption by a ElGamal cryptosystem, the receiver finds
the value $\tilde{x}$. In order to obtain $m$, he uses the relation $\lceil \frac{\tilde{x} - 1}{k} \rceil = m$.

The probability that this method fails is of order $2^{-k}$. In order to obtain a deterministic method, we must be able to find, for a given elliptic curve, a value of $k$ ensuring that there exists a point of first coordinate $\tilde{x} \in [km + 1, km + k]$ for each value $m \in [0, M - 1]$. The size of the plaintext space decreases with $k$. So, the value of $k$ must also preserve a set of plaintexts large enough so that exhaustive attack fails.

With this method, assuming that Alice and Bob know the generator $P$ and use the compression of points, $2 \log q + 2$ bits are sent in order to encrypt a plaintext of order $\log(q/k)$ bits. So the transmission rate of this method depends on the parameter $k$ and is of order $\frac{1}{2} - \frac{\log k}{2 \log q}$.

We see that there exist many methods to solve this encoding problem. We could compare advantages and drawbacks about different aspects like security or transmission rate. We propose another way: use an ElGamal cryptosystem with the group of the elements of a Weierstrass cubic curve over $\mathbb{F}_q[\epsilon]$. We will this way meet no encoding problem, while keeping the same level of security as ElGamal cryptosystem on elliptic curves. On the other hand, the transmission rate will be 1/4 at best.

### 5.2 Another solution : another group

By choosing for $G$ the set of elements of a Weierstrass cubic curve on $\mathbb{F}_q[\epsilon]$, no specific condition is imposed to $x_1$ for all elements $(x_0 + x_1 \epsilon, y_0 + y_1 \epsilon)$ such that $y_0$ is different to 0. So we construct a variant of ElGamal cryptosystem over a Weierstrass cubic curve for which the plaintext is encoded only by the indeterminate $x_1$ and $(x_0, y_0)$ is randomly chosen. This encoding gives the cryptosystem $\mathcal{W}_\epsilon$.

Consider $p$ a prime different than 2 and 3, $a$ and $b$ two elements of $\mathbb{F}_p[\epsilon]$ which define a Weierstrass cubic curve of cardinal $N_p$ with $N$ a prime different to $p$ and an element $P$, a generator of $\mathcal{E}_{a,b}(\mathbb{F}_p[\epsilon])$. These elements are the initialization parameters of the following algorithm :

**Key generation algorithm** $K_{\mathcal{W}_\epsilon}(p, a, b, P, N) \rightarrow (P_k, sk)$ :

Input : $(p, a, b, P, N)$ : initialization parameters

Output : $(P_k, sk)$ with $sk$ an integer between 2 and $N - 1$ and $P_k$ in $\mathcal{E}_{a,b}(\mathbb{F}_p[\epsilon])$

1. Randomly choose an integer $sk$ between 2 and $N - 1$.

2. Compute $P_k = skP$.

**Encryption algorithm** $E_{P_k}(m; r, R) \rightarrow (C_1, C_2)$ :

Input : $m$ in $\mathbb{F}_p$, the plaintext.

Output : $C = (C_1, C_2)$ in $\mathcal{E}_{a,b}(\mathbb{F}_p[\epsilon])^2$
1. Randomly choose an integer \( r \) between 2 and \( N - 1 \).

2. Randomly choose a point \( R = (x_0, y_0) \) in \( E_{\pi(a), \pi(b)}(\mathbb{F}_p) \) with \( y_0 \neq 0 \).

3. Compute \( M = (x_0 + m\epsilon, y_0 + y_1\epsilon) \) in \( E_{a,b}(\mathbb{F}_p[\epsilon]) \).

4. Compute \( C_1 = rpP \) and \( C_2 = rP_k + M \) in \( E_{a,b}(\mathbb{F}_p[\epsilon]) \).

Decryption algorithm \( D_{sk}^{W_\epsilon}(C_1, C_2) \rightarrow m : \)

- **Input:** \( C = (C_1, C_2) \) in \( E_{a,b}(\mathbb{F}_p[\epsilon]) \)
- **Output:** \( m \) in \( \mathbb{F}_p \).

1. Compute \( C_2 - skC_1 = M = (x_0 + m\epsilon, y_0 + y_1\epsilon) \).
2. Extract \( m \) from \( M \).

In the same way, we define the cryptosystem \( W_{\epsilon_0} \). Its unique difference with the cryptosystem \( W_\epsilon \) is the set of initialization parameters \( a \) and \( b \): we impose to \( a \) and \( b \) to be in \( \mathbb{F}_p \). Then we always consider the associated Weierstrass equation in \( \mathbb{F}_p[\epsilon] \) and we randomly choose \( P \) in \( E_{a,b}(\mathbb{F}_p[\epsilon]) \) generator of \( E_{a,b}(\mathbb{F}_p[\epsilon]) \). And the algorithms of key generation, encryption and decryption are defined in the same way.

A similar method of compression point can be used in order to send the ciphertext: for a given value of the first coordinate of an element of the Weierstrass cubic curve in \( \mathbb{F}_q[\epsilon] \), there exists at most two possible values for the second coordinate. So \( 2\log q + 1 \) bits suffice to send an element of a Weierstrass cubic curve in \( \mathbb{F}_q[\epsilon] \). Using this method of element compression, the size of the cipher text is of \( 4\log q + 2 \) bits for a plaintext of size \( \log q \). Then the transmission rate of these two cryptosystems is closed to 1/4.

In the next section, we discuss some security aspects of the cryptosystems \( W_\epsilon \) and \( W_{\epsilon_0} \).

### 6 Security - One-wayness

We want to study the security of these cryptosystems. We will consider the existence of a probabilistic algorithm which decrypts a ciphertext without the secret key with a non-negligible probability of success.

**One-wayness:**

We want to know if the encryption function is one-way. Here the goal of an adversary is to find a plaintext from a corresponding ciphertext and public instances. The notation \( a \leftarrow A \) means that the variable \( a \) is chosen randomly in \( A \).

**Definition 6.1** Consider \( (p, a, b, P, N) \) the initialization parameters of \( W_\epsilon \). Consider a probabilistic algorithm \( Z \) which takes as inputs a public key \( P_k \) and a ciphertext \( C \) and outputs a plaintext \( m \). Its probability of success in decrypting the cryptosystem \( W_\epsilon \) with initialization parameters \( (p, a, b, P, N) \) without knowing the secret key is:

\[
\text{Succ}_{W_\epsilon}^{ON}(Z) = Pr[Z(P_k, E_{P_k}(m; r, R)) = m]
\]

40
where the probability space is
\[ F_p \times [2, N - 1]^2 \times E_{\pi(a), \pi(b)}(F_p) \setminus \{(x, 0) \in E_{\pi(a), \pi(b)}(F_p)\} \times \Omega \]
with \( m \leftarrow F_p, Pk = skpP \text{ and } sk \leftarrow [2, N - 1], r \leftarrow [2, N - 1], R \leftarrow E_{\pi(a), \pi(b)}(F_p) \setminus \{(x, 0) \in E_{\pi(a), \pi(b)}(F_p)\} \) and with \( \Omega \) the set of the initial random tape of \( Z \).

We have similar definitions for the cryptosystem \( W_{\varepsilon_0} \).

When we encrypt a plaintext \( m \) with the cryptosystem \( W_{\varepsilon} \) or \( W_{\varepsilon_0} \), we use a variable \( R \) randomly chosen. Next lemma and theorem explain how to reconstruct the variable \( R \) from public instances and the plaintext \( m \).

**Lemma 6.2** Let \( a \) and \( b \) in \( F_q \), consider the associated Weierstrass cubic curve \( E_{a,b} \) over \( F_q[\varepsilon] \), then for all \( P = (x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) \in E_{a,b}(F_q[\varepsilon]) \), \( NP = \Theta_0 \) if and only if \( x_1 = y_1 = 0 \).

**Proof.** Firstly, if \( x_1 = y_1 = 0 \), then \( P = (x_0, y_0) \) is in \( E_{a,b}(F_q) \) with \( a \) and \( b \) in \( F_q \). However, if \( a \) and \( b \) are in \( F_q \), we have \( E_{a,b}(F_q) = E_{a,b}(F_q) \). Then for all \( n \in \mathbb{Z} \), \( nP = \Theta_0 \). So we have \( NP = \Theta_k \) with \( \Theta_k \in E_{a,b}(F_q) \). So, \( \Theta_k = \Theta_0 \).

Secondly, if \( N(x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) = \Theta_0 \), with the previous property, we also have \( N(x_0, y_0) = \Theta_0 \).

Then \( N(x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) - N(x_0, y_0) = N((x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) - (x_0, y_0)) \)
= \( \Theta_0 \). We have \( \pi((x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) - (x_0, y_0)) = \Theta_k \).

Then \( (x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) - (x_0, y_0) = \Theta_k \) with \( k \in F_q \) and \( Nk = 0 \). However, \( p \) and \( N \) are relatively prime, so \( k = 0 \) and \( (x_0 + x_1 \varepsilon, y_0 + y_1 \varepsilon) = (x_0, y_0) \). So, we have \( x_1 = y_1 = 0 \).

With the notation from the definition of encryption algorithm of \( W_{\varepsilon} \) in section 5, we have :

**Theorem 6.3** Let \( (p, a, b, P, N) \) initialization parameters of \( W_{\varepsilon_0} \). There exists a probabilistic algorithm which takes as inputs the initialization parameters \( (p, a, b, P, N) \), a plaintext \( m \neq 0 \) and the second part \( C_2 \) of a ciphertext \( C = (C_1, C_2) \) corresponding to \( m \) and outputs the variable \( R \) used for the encryption of the plaintext \( m \) by \( C \), with a polynomial time in \( \log(p) \) and with a probability at least equal to \( 1/3 \).

**Proof.** Firstly, note that with the notation of sections 4 and 5, we have :

\[ [N[N^{-1}]C_2] = [N[N^{-1}]M]. \]

This equality is due to lemma 4.1 :

\[ [N[N^{-1}]C_2] = rskp[N[N^{-1}]P] + [N[N^{-1}]M] = [N[N^{-1}]M] \text{ in } F_p. \]
Then, we have $\Theta_{(\mathbb{N}[\mathbb{N}^{-1}]C_2)} = M + (\mathbb{N}[\mathbb{N}^{-1}] - 1)M = M + \nu_p M$ for an integer $\nu$.

Denote $M = (x_0 + m\varepsilon, y_0 + y_1\varepsilon)$. We have $N\nu_p M = (Np)\nu M = \Theta_0$. So from lemma 6.2, $(\mathbb{N}[\mathbb{N}^{-1}] - 1)M$ is in $\mathcal{E}_{a,b}(\mathbb{F}_p)$.

Moreover, we have:

$$\pi((\mathbb{N}[\mathbb{N}^{-1}] - 1)M) = -\pi(M)$$

and so $(\mathbb{N}[\mathbb{N}^{-1}] - 1)M = (x_0, -y_0)$.

Then, according to the group law, the sum of these two points gives:

$$[\mathbb{N}[\mathbb{N}^{-1}]C_2] = (0 - m)/2y_0.$$

So, if $m \neq 0$, we have $R = (x_0, y_0)$ with $y_0 = -m/2[\mathbb{N}[\mathbb{N}^{-1}]C_2]$ and $x_0$ is a root in $\mathbb{F}_p$ of the polynomial $X^3 + aX + b - y_0^2$. The number of its roots in $\mathbb{F}_q$ is exactly one other three, so with these equalities we can construct an algorithm which outputs $R$ with a probability at least 1/3. Moreover the time of these computations is polynomial in $\log(p)$ due to the efficiency of the group law, an algorithm of fast exponentiation and an algorithm of roots extracting with a polynomial time in $\log(p)$ [vzGG99].

Then we have some results about the one-wayness of the cryptosystem $\mathcal{W}_{\varepsilon_0}$:

**Theorem 6.4** If there exists a probabilistic algorithm $Z$, with a running time $\tau$, such that: 

$$\text{Succ}_{\text{OW}_n}(Z) \geq \delta$$

then there exists a probabilistic algorithm which solves the CDH problem in $\mathcal{E}_{a,b}(\mathbb{F}_p)$ of base $\pi(P)$ with a running time $\tau + O(\log(p)M(p))$ and a probability of at least $\delta/3$ (where $M(p)$ is the complexity of computing a product in $\mathbb{F}_p$).

**Proof.** Let $Z$ be a probabilistic algorithm which decrypts the cryptosystem with initialization parameters $(p, a, b, P, N)$. Let $(A = \alpha\pi(P), B = \beta\pi(P))$ an instance of the Computational Diffie Hellman problem in $\mathcal{E}_{a,b}(\mathbb{F}_p)$ of base $\pi(P)$. Then, the algorithm from figure 1 returns $\alpha\beta\pi(P)$: thanks to theorem 6.3, the computation of $x_0, y_0$ and $y_1$ allows to know the value of $M = (x_0 + m\varepsilon, y_0 + y_1\varepsilon)$ used for encryption of $m$ by $C$ with the public key $P_k$. Then $Q = C_2 - M = \alpha P_k = \alpha p^\beta P$ and $\text{Res} = p^\beta p^{-1}\text{mod}\mathbb{N}\alpha\beta\pi(P) = (1 + \varepsilon N)\alpha\beta\pi(P)$ for $\varepsilon$ in $\mathbb{Z}$. But $\mathbb{N}\pi(P) = \Theta$, so we have $\text{Res} = \alpha\beta\pi(P)$.

\[\boxdot\]

7 Conclusion

We have described two new cryptosystems $\mathcal{W}_{\varepsilon}$ and $\mathcal{W}_{\varepsilon_0}$, which use elliptic curve background and present no encoding problem. Their transmission rate is of order 1/4 and the cryptosystem $\mathcal{W}_{\varepsilon_0}$ satisfies one-wayness property under CDH problem in the underlying elliptic curve. It would be interesting to know if such result exists for the cryptosystem $\mathcal{W}_{\varepsilon}$.
CDH algorithm

Inputs:
\( \{p, a, b, P, N\} \): initialization parameters of \( W_{\varepsilon 0} \)
\[ A = \alpha \pi(P) \in E_{a,b}(\mathbb{F}_p) \]
\[ B = \beta \pi(P) \in E_{a,b}(\mathbb{F}_p) \]

Output:
\( \alpha \beta \pi(P) \).

Algorithm:
Randomly choose \( C_2 \in E_{a,b}(\mathbb{F}_p[\varepsilon]) \)
\[ C := (\Lambda^{-1}(A, 0), C_2) \]
\[ \text{P}k := p\Lambda^{-1}(B, 0) \]
Ask \( m := Z(p, a, b, P, \text{P}k, C) \)
if \( m = 0 \) then Return(\( CDH \) algorithm \( p, a, b, P, N, A, B \)) end if
Compute
\[ y_0 = -m/(2[N \mod {N^{-1}C_2}]) \]
Compute
\[ x_0 := \text{a root of } x^3 + ax + b - y_0^2 \]
Compute
\[ y_1 := m(3x_0^2 + a_0)/2y_0 \]
Compute
\[ Q := C_2 - (x_0 + m\varepsilon, y_0 + y_1\varepsilon) \]
Compute
\[ k := \left[p^{-1} \mod N\right] \in [1, N - 1] \]
Compute Res := \( k \pi(Q) \)
Return(Res)

Figure 1: Algorithm for solving CDH problem relative to the algorithm \( Z \)

Anyway, if we have the goal to break one of these systems for all initialization parameters, the task will be harder for \( W_{\varepsilon} \) than for \( W_{\varepsilon 0} \), due to the inclusion of corresponding sets. But \( W_{\varepsilon 0} \) could stay stronger than \( W_{\varepsilon} \); for instance, if an algorithm were found for breaking \( W_{\varepsilon} \) for all initialization parameters \( (a, b) \) except in \( \mathbb{F}_p^2 \). We could have some kind of results concerning indistinguishability of \( W_{\varepsilon 0} \) and DDH problem over the underlying elliptic curve, by using for instance [Poi02].

Acknowledgements

I am very grateful to Louis Grandboulan and Marc Girault for helpful criticism and valuable suggestions.

References


