Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 1, pp. 1–15
DOI : 10.47974/JDMSC-1637

A generalization of ElGamal signature variants over elliptic curves

M. Ihia *
O. Khadir †
Laboratory of Mathematics, Cryptography,
Mechanics and Numerical Analysis
University Hassan II of Casablanca
Mohammedia 28806
Morocco

Abstract

The ElGamal signature is a scheme invented by Taher Elgamal in 1984 based on the problem of the discrete logarithm. In our day, there are several variants of this signature. In this paper, we will present the version of many variants schemes of ElGamal over elliptic curves. We will give some examples.

Subject Classification: *(2000) 94A60, 14H52.*

Keywords: *Public key cryptography, Elliptic curves, ElGamal digital signature.*

1. Introduction

Public key cryptography or asymmetric cryptography appeared in 1976 by Diffie-Hellman [2]. They described a key exchange method for constructing a private key between two entities over any channel. Digital signature is among the important branches of public key cryptography. It replaces the handwritten type. Each signature scheme consists of three steps: the first is the generation of keys, the second is the equation of the signature and the third is the verification of validity. To sign a message, a user signs the hash of the document with their secret key, and everyone can verify the validity of the signature with their public key. Every signature is based on a difficult problem such as: factorization of large numbers or problem of discrete logarithm. [1] It is used in banking cards, financial transactions, confidential messages....etc.

* *E-mail:* `marouane.ihia@gmail.com (Corresponding Author)`
† *E-mail:* `khadir@hotmail.com`

There are several signature schemes such as RSA [16] in 1978, Rabin [15] in 1979, Guillou-Quisquater [4] in 1990. One of the most famous signature is that of ElGamal [3], its security is based on the difficulty of the discrete logarithm problem. It was upgraded by the US government under the name of DSA [12]. Several variants of this scheme have appeared (See Table 1). In particular Horster et al. [7] have published an inventory of variants of the ElGamal signature.

In 1986 Koblitz [11] and Miller [14] proposed independently the groups of elliptic curves instead of groups $\mathbb{Z}/p\mathbb{Z}$ as bases of cryptosystem. After their work the elliptic curves over fields have become primordial in cryptography. Koblitz has released the elliptic curves version of the ElGamal signature. The general known weakness for the Elliptic Curve Digital Signature Algorithm (ECDSA) is using one ephemeral key sign in two different messages. In their article [19] the authors proposed a new technique inspired from the work of Liao and Shen. To further improve the strength of the ElGamal algorithm, a paper [20] published in 2021 uses $-\varphi(N)$ as a parameter in the generation instead of the usual $-s$. In our own publication of 2019, see [8], we presented some solutions to the mentioned problem by modifying the hash function. The main advantage promised by elliptic curves cryptography is the reduction of the size of the key, which reduces the storage and transmission needs. It is essential to be able to find a cyclic subgroup of a curve E whose order is divisible by a large prime number. Most signatures protocols have analogues on these curves. It should be noted that a small key on elliptic curves can provide the same level of security offered by an RSA system based on a large number. In this work, for its theoretical and educational interest, we propose to construct the elliptic curves versions of these variants.

The paper is organized as follows: the second Section is a reminder of elliptic curves and ElGamal signature scheme. The third Section contains our contribution. We conclude in the fourth Section.

Throughout the sequel we use classical notations: For every prime integer, we denote by $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the field of modular integers with p elements. Let a, b and c be three integers we write $a \equiv b\,[c]$ if c divides the difference $a - b$ and $a = b \bmod c$ if a is the remainder in the division of b by c.

Let us start by recalling the construction of elliptic curve groups.

2. Elliptic curves [18, 5]

Elliptic curves can be defined over finite fields $\mathbb{F}_q$, where q is a power of a prime number. We suppose that the characteristic is not 2 or 3. An elliptic curve is the set of elements $(x, y) \in \mathbb{F}_q^2$ that verfy the modular equation $y^2 = x^3 + ax + b$, where the discriminant $-(4a^3 + 27b^2) \neq 0$. A particular point at infinity, denoted by $\mathcal{O}$, is added to the curve as a neutral element. It is well known that an additive operation of points over the elliptic curve is formulated by the following conditions (see for instance [8]):

1. Identity: $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E(\mathbb{F}_q)$.
2. Opposite: If $P = (x, y) \in E(\mathbb{F}_q)$ then the point $-P = (x, y)$ is the opposite of P.
3. Point addition: Let $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E(\mathbb{F}_q)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where

$x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$

with $m = \frac{y_2 - y_1}{x_2 - x_1}$.

Otherwise $P + Q = \mathcal{O}$.

4. Point doubling: Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$, where $P \neq -P$. Then $2P = (x_3, y_3)$, where

$x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$

with $m = \frac{3x_1^2 + a}{2y_1}$.

Otherwise $2P = \mathcal{O}$.

For more details, we also refer the reader to references [1, 10, 18]. The addition is used to build an abelian group.

Theorem 1 ([6, p. 287, 8])**:** *The finite set* $E(\mathbb{F}_q)$, *with the binary additive operation, constitues a commutative group and its identity element is the point at infinity* $\mathcal{O}$.

Several efficient methods exist for the computaion of $kM = M + M + \ldots + M$, *where k is a natural integer and M a point in the elliptic curves. see for instance* [13, *p*. 615].

Definition 1 ([9, p. 180])**:** Let p be a prime and let $P, Q \in E(\mathbb{F}_p)$. Suppose we know that there exists an integer x such that: $Q = xP$ The elliptic curve discrete logarithm problem is how to find x.

Definition 2 (|18, *p*. 177|, |8|)**:** A cryptographic hash function H, is a function such that the image of any element of long length gives a result having a smaller fixed length, and should have the following properties:

1. For an arbitrary message m, it is possible to compute the value $H(m)$ rapidly.
2. H is preimage resistant: Given y, it is too hard to determine a message m such that $H(m) = y$.
3. H is strongly collision-free: It is computationally infeasible to construct two message m_1 and m_2 such that $m_1 \neq m_2$ and $H(m_1) = H(m_2)$.

2.1 *ElGamal Digital Signature over elliptic curves [18, p. 175]*

Here we recall the ElGamal elliptic curves digital signature protol. Assume that the user Alice would like to sign the document m. She first must product a public key. She selects an elliptic curve E over a finite field $\mathbb{F}_q$ and a point $A \in E(\mathbb{F}_q)$. The order of the point A is a large prime n. Alice also chooses a random secret integer a and determine $B = aA$.

The equation of the signature is

$$xB + sR = H(m)A \tag{1}$$

Alice's public key is E, $\mathbb{F}_q$, A, and B. The only private key is a.

If Alice accepts to sign the message m, she follows the next three steps:

1. Calculates $H(m)$.
2. Chooses a random integer k co-prime with n and computes $R = kA = (x, y)$.
3. Determines $s \equiv k^{-1}(H(m) - ax)\,[n]$.

The digital signature of the message m is then (m, R, s).

Bob or anybody can verify the signature by following the next three steps:

1. Bob downloads Alice's public key.
2. He then calculate $V_1 = xB + sR$ and $V_2 = H(m)\,A$.
3. If $V_1 = V_2$, Bob declares the validation of Alice signature. If not he refuses Alice signature.

3. Our contribution

We take the equation

$$\alpha^u \equiv y^v r^w \ [p] \tag{2}$$

we find $u \equiv xv + kw \ [p-1]$, indeed:

We have $y \equiv \alpha^x \ [p]$ and $r \equiv \alpha^k \ [p]$, we replace y and r in (2):

$$\alpha^u \equiv y^v r^w \equiv (\alpha^x)^v (\alpha^k)^w \equiv \alpha^{xv} \alpha^{kw} \equiv \alpha^{xv+kw} \ [p]$$

$$\alpha^{\overline{xv+kw}} \equiv 1 \ [p] \Leftrightarrow \frac{u}{xv+kw} \equiv 1 \ [p-1]$$

$$u \equiv xv + kw \ [p-1]$$

We select u, v and w as a permutation of the parameters (m, r, s) we took the table from [7]:

Table 1

Variations of the ElGamal schemes

	u	v	w	Signing equation [$p-1$]	Verification [p]
1	m	r	s	$m \equiv xr + ks$	$\alpha^m \equiv (\alpha^x)^r r^s$
2	m	s	r	$m \equiv xs + kr$	$\alpha^m \equiv (\alpha^x)^s r^r$
3	s	r	m	$s \equiv xr + km$	$\alpha^s \equiv (\alpha^x)^r r^m$
4	s	m	r	$s \equiv xm + kr$	$\alpha^s \equiv (\alpha^x)^m r^r$
5	r	s	m	$r \equiv xs + km$	$\alpha^r \equiv (\alpha^x)^s r^m$
6	r	m	s	$r \equiv xm + ks$	$\alpha^r \equiv (\alpha^x)^m r^s$

Now, we pass to the elliptic curves (EC) version.

We take the equation

$$u\,A = v\,B + w\,R \tag{3}$$

we find $u \equiv xv + kw \ [n]$, where n is the order of A, indeed:

We have $B = a\,A$ and $R = k\,A = (x, y)$, we replace B and R in (3):

$$u\,A = v\,B + w\,R = v\,a\,A + w\,k\,A = (v\,a + w\,k)A$$

$$(u - v\,a - w\,k)A = \mathcal{O} \Leftrightarrow u - v\,a - w\,k \equiv 0 \ [n]$$

$$u \equiv v\,a + w\,k \ [n]$$

with $\mathcal{O}$ is the identity element of curve

We select u, v and w as a permutation of the parameters ($H(m)$, x, s), where H is a hach funcion [13, p. 33], [17, p. 119]. We obtain the table 2 below:

Table 2

Variations of the ElGamal schemes over EC

	u	v	w	**Signing equation [n]**	**Verification**
1	$H(m)$	x	s	$H(m) \equiv xa + sk$	$H(m)\ A = x\ B + s\ R$
2	$H(m)$	s	x	$H(m) \equiv sa + xk$	$H(m)\ A = s\ B + x\ R$
3	s	x	$H(m)$	$s \equiv xa + H(m)k$	$s\ A = x\ B + H(m)\ R$
4	s	$H(m)$	x	$s \equiv H(m)a + xk$	$s\ A = H(m)\ B + x\ R$
5	x	s	$H(m)$	$x \equiv sa + H(m)k$	$x\ A = s\ B + H(m)\ R$
6	x	$H(m)$	s	$x \equiv H(m)a + sk$	$x\ A = H(m)\ B + s\ R$

Example 1: $E_p(\alpha, \beta)$ be an elliptic curve with $\alpha = -3$, $\beta = 7$ and p = 18645503.

$(\Delta \equiv -(4\alpha^3 + 27\beta^2) \equiv 1215\ [p])$.

The cardinality of the elliptic curve is

$$\#E_p(\alpha, \beta) = 18649165 = 5 \times 19 \times 196307$$

Alice chooses randomly the point A = (94334, 2703067) whose order is n = 196307 and the integer a = 116543. She computes $B = a\ A$ = (16494089, 3643228).

The public and private key of Alice are $(A, B, E_p(\alpha, \beta))$ and a respectively.

To sign the message m such that $H(m)$ = 45615, Alice calculates:

1. selects k = 68691, and computes $R = k\ A$ = (13902473, 10159846).
2. $s \equiv xa + H(m)k \equiv 73103\ [196307]$.

The message signature is ($H(m)$, R, s) = (45615, (13902473, 10159846), 73103).

Bob verifies the signature as follows:

He computes $s\ A$ = (10017819, 7308504) and $x\ B + H(m)\ R$ = (10017819, 7308504). He finds $s\ A = x\ B + H(m)\ R$. Hence the signature is valid.

We saw in the previous paragraph that the coefficients u, v and w are permutations of (m, r, s). Now we will work on other permutations illustrated in the table 3 below [17, *p*. 119]:

Table 3

Others variations of the ElGamal schemes

Type	permutation of (u, v, w)		
1	mr	s	1
2	mr	ms	1
3	ms	rs	1
4	mr	rs	1

3.1 *First type*

We take the first equation $\alpha^u \equiv y^v r^w \ [p]$, with $(u, v, w) = (mr, s, 1)$ and we transform it over EC, we obtain $u\,A = v\,B + w\,R$, and we select u, v and w as a permutation of the parameters $(H(m)\,x, s, 1)$. We determine the table 4 below:

Table 4

Variations of the first type over EC

	u	v	w	Signing equation $[n]$	Verification
1	$H(m)x$	s	1	$H(m)x \equiv sa + k$	$H(m)x\,A = s\,B + R$
2	$H(m)x$	1	s	$H(m)x \equiv a + sk$	$H(m)x\,A = B + s\,R$
3	1	s	$H(m)x$	$1 \equiv sa + H(m)xk$	$A = s\,B + H(m)x\,R$
4	1	$H(m)x$	s	$1 \equiv H(m)xa + sk$	$A = H(m)x\,B + s\,R$
5	s	1	$H(m)x$	$s \equiv a + H(m)xk$	$s\,A = B + H(m)x\,R$
6	s	$H(m)x$	1	$s \equiv H(m)xa + k$	$s\,A = H(m)x\,B + R$

Example 2: This example illustrates the sixth equation in the table 4 above.

Let $E_p(\alpha, \beta)$ be an elliptic curve with $\alpha = 11$, $\beta = 41$ and $p = 24645431$.

$(\Delta \equiv -(4\alpha^3 + 27\beta^2) \equiv 1215\ [p])$.

The cardinality of the elliptic curve is

$$\#E_p(\alpha, \beta) = 24646374 = 2 \times 3^2 \times 1369243.$$

Alice chooses randomly the point $A = (79373, 21641896)$ whose order is $n = 1369243$ and the integer $a = 896511$. She computes $B = a\,A = (4582294, 7711464)$.

The public and private key of Alice are $(A, B, E_p(\alpha, \beta))$ and a respectively.

To sign the message m such that $H(m) = 472712$, Alice calculates:

1. selects $k = 1237691$, and computes $R = k\,A = (4914431, 15515666)$.
2. $s \equiv H(m)xa + k \equiv 1142180\ [n]$.

The message signature is $(H(m), R, s) = (472712, (4914431, 15515666), 1142180)$.

Bob verifies the signature as follows:

He computes $s\,A = (10027767, 8873854)$ and $H(m)x\,B + R = (10027767, 8873854)$. He finds $s\,A = H(m)x\,B + R$. Hence the signature is valid.

3.2 *Second type*

In the second type, we select u, v and w as a permutation of the parameters $(H(m)x, H(m)s, 1)$. We get the table 5 below:

Table 5

Variations of the second type over EC

	u	v	w	**Signing equation** $[n]$	**Verification**
1	$H(m)x$	$H(m)s$	1	$H(m)x \equiv H(m)sa + k$	$H(m)x\,A = H(m)s\,B + R$
2	$H(m)x$	1	$H(m)s$	$H(m)x \equiv a + H(m)sk$	$H(m)x\,A = B + H(m)s\,R$
3	1	$H(m)s$	$H(m)x$	$1 \equiv H(m)sa + H(m)xk$	$A = H(m)s\,B + H(m)x\,R$
4	1	$H(m)x$	$H(m)s$	$1 \equiv H(m)xa + H(m)sk$	$A = H(m)x\,B + H(m)s\,R$
5	$H(m)s$	1	$H(m)x$	$H(m)s \equiv a + H(m)xk$	$H(m)s\,A = B + H(m)x\,R$
6	$H(m)s$	$H(m)x$	1	$H(m)s \equiv H(m)xa + k$	$H(m)s\,A = H(m)x\,B + R$

Example 3: This example illustrates the fifth equation in the table 5 above.

Let $E_p(\alpha, \beta)$ be an elliptic curve with $\alpha = -1$, $\beta = 2$ and $p = 34122713$.

$(\Delta \equiv -(4\alpha^3 + 27\beta^2) \equiv 104\ [p])$.

The cardinality of the elliptic curve is

$$\#E_p(\alpha, \beta) = 34126972 = 2^2 \times 11 \times 775613.$$

Alice chooses randomly the point A = (7565130, 14911564) whose order is n = 775613 and the integer a = 567233. She computes $B = a\,A$ = (29959132, 28604135).

The public and private key of Alice are $(A, B, E_p(\alpha, \beta))$ and a respectively.

To sign the message m such that $H(m)$ = 487957, Alice calculates:

1. selects k = 543292, and computes $R = k\,A$ = (19276789, 9385819).
2. $s \equiv \frac{a+H(m)xk}{H(m)} \equiv 32285\,[n]$.

The message signature is ($H(m)$, R, s) = (487957, (19276789, 9385819), 32285).

Bob verifies the signature as follows:

He computes $H(m)s\,A$ = (33450257, 21279245) and $B + H(m)x\,R$ = (33450257, 21279245). He finds $H(m)s\,A = B + H(m)x\,R$. Hence the signature is valid.

3.3 *Third type*

In the third type, we select u, v and w as a permutation of the parameters ($H(m)s$, xs, 1). We determine the table 6 below:

Table 6

Variations of the third type over EC

	u	v	w	Signing equation [n]	Verification
1	$H(m)s$	xs	1	$H(m)s \equiv xsa + k$	$H(m)s\,A = xs\,B + R$
2	$H(m)s$	1	xs	$H(m)s \equiv a + xsk$	$H(m)s\,A = B + xs\,R$
3	1	xs	$H(m)s$	$1 \equiv xsa + H(m)sk$	$A = xs\,B + H(m)s\,R$
4	1	$H(m)s$	xs	$1 \equiv H(m)sa + xsk$	$A = H(m)s\,B + xs\,R$
5	xs	1	$H(m)s$	$xs \equiv a + H(m)sk$	$xs\,A = B + H(m)s\,R$
6	xs	$H(m)s$	1	$xs \equiv H(m)sa + k$	$xs\,A = H(m)s\,B + R$

Example 4: This example illustrates the first equation in the table 6 above.

Let $E_p(\alpha, \beta)$ be an elliptic curve with $\alpha = -5$, $\beta = 17$ and $p = 21388099$.

$(\Delta \equiv -(4\alpha^3 + 27\beta^2) \equiv 7303\,[p])$.

The cardinality of the elliptic curve is

$$\#E_p(\alpha,\beta) = 21391490 = 2\times 5\times 2139149.$$

Alice chooses randomly the point A = (611292, 12032361) whose order is n = 2139149 and the integer a = 1176511. She computes $B = a\,A$ = (6735074, 15301261).

The public and private key of Alice are $(A, B, E_p(\alpha,\beta))$ and a respectively.

To sign the message m such that $H(m)$ = 987342, Alice calculates:

1. selects k = 737618, and computes $R = k\,A$ = (17458251, 12357292).
2. $s \equiv \frac{k}{H(m)-xa} \equiv 318966\ [n]$.

The message signature is $(H(m), R, s)$ = (987342, (17458251, 12357292), 318966).

Bob verifies the signature as follows:

He computes $H(m)s\,A$ = (16693595, 3685319) and $xs\,B + R$ = (16693595, 3685319). He finds $H(m)s\,A = xs\,B + R$. Hence the signature is valid.

3.4 *Fourth type*

In the fourth type, we select u, v and w as a permutation of the parameters $(H(m)x, xs, 1)$. We determine the table 7 below:

Table 7

Variations of the fourth type over EC

	u	v	w	**Signing equation** $[n]$	**Verification**
1	$H(m)x$	xs	1	$H(m)x \equiv xsa + k$	$H(m)x\,A = xs\,B + R$
2	$H(m)x$	1	xs	$H(m)x \equiv a + xsk$	$H(m)x\,A = B + xs\,R$
3	1	xs	$H(m)x$	$1 \equiv xsa + H(m)xk$	$A = xs\,B + H(m)x\,R$
4	1	$H(m)x$	xs	$1 \equiv H(m)xa + xsk$	$A = H(m)x\,B + xs\,R$
5	xs	1	$H(m)x$	$xs \equiv a + H(m)xk$	$xs\,A = B + H(m)x\,R$
6	xs	$H(m)x$	1	$xs \equiv H(m)xa + k$	$xs\,A = H(m)x\,B + R$

Example 5: This example illustrates the third equation in the table 7 above.

Let $E_p(\alpha,\beta)$ be an elliptic curve with $\alpha = -19$, $\beta = 19$ and p = 32510113.

$(\Delta \equiv -(4\alpha^3 + 27\beta^2) \equiv 32492424\ [p]).$

The cardinality of the elliptic curve is

$$\#E_p(\alpha, \beta) = 32510728 = 2^3 \times 4063841.$$

Alice chooses randomly the point A = (11518, 28991050) whose order is n = 4063841 and the integer a = 332188. She computes $B = a\,A$ = (2758667, 28033360).

The public and private key of Alice are $(A, B, E_p(\alpha, \beta))$ and a respectively.

To sign the message m such that $H(m)$ = 11842, Alice calculates:

1. selects k = 253998, and computes $R = k\,A$ = (2646770, 6939109).
2. $s \equiv \frac{1-H(m)xk}{xa} \equiv 635408\ [n]$.

The message signature is ($H(m)$, R, s) = (11842, (2646770, 6939109), 635408).

Bob verifies the signature as follows:

He computes $xs\,B + H(m)x\,R$ = (11518, 28991050). He finds $A = xs\,B + H(m)x\,R$. Hence the signature is valid.

There exists two others variants: (ms, r, 1) and (m, rs, 1).

3.5 *Fifth type*

In the fifth type, we select u, v and w as a permutation of the parameters ($H(m)s$, x, 1). We determine the table 8 below:

Table 8
Variations of the fifth type over EC

	u	v	w	**Signing equation [n]**	**Verification**
1	$H(m)s$	x	1	$H(m)s \equiv xa + k$	$H(m)s\,A = x\,B + R$
2	$H(m)s$	1	x	$H(m)s \equiv a + xk$	$H(m)s\,A = B + x\,R$
3	1	x	$H(m)s$	$1 \equiv xa + H(m)sk$	$A = x\,B + H(m)s\,R$
4	1	$H(m)s$	x	$1 \equiv H(m)sa + xk$	$A = H(m)s\,B + x\,R$
5	x	1	$H(m)s$	$x \equiv a + H(m)sk$	$x\,A = B + H(m)s\,R$
6	x	$H(m)s$	1	$x \equiv H(m)sa + k$	$x\,A = H(m)s\,B + R$

Example 6: This example illustrates the second equation in the table 8 above.

Let $E_p(\alpha, \beta)$ be an elliptic curve with $\alpha = 31,\ \beta = 33$ and $p = 28646539$.

$(\Delta \equiv -(4\alpha^3 + 27\beta^2) \equiv 148567\ [p])$.

The cardinality of the elliptic curve is

$$\#E_p(\alpha, \beta) = 28645978 = 2 \times 14322989.$$

Alice chooses randomly the point A = (711513, 12370042) whose order is n = 14322989 and the integer a = 9862188. She computes $B = a\ A$ = (1263189, 9329056).

The public and private key of Alice are $(A, B, E_p(\alpha, \beta))$ and a respectively.

To sign the message m such that $H(m)$ = 7741842, Alice calculates:

1. selects k = 13267831, and computes $R = k\ A$ = (17517806, 12107727).
2. $s \equiv \frac{a + xk}{H(m)} \equiv 6181771\ [n]$.

The message signature is $(H(m), R, s)$ = (7741842, (17517806, 12107727), 6181771).

Bob verifies the signature as follows:

He computes $H(m)s\ A$ = (28450019, 28055901) and $B + x\ R$ = (28450019, 28055901. He finds $H(m)s$ A = $B + x\ R$. Hence the signature is valid.

3.6 *Sixth type*

In the sixth type, we select u, v and w as a permutation of the parameters ($H(m)$, xs, 1). We determine the table 9 below:

Table 9
Variations of the sixth type over EC

	u	v	w	**Signing equation [n]**	**Verification**
1	$H(m)$	xs	1	$H(m) \equiv xsa + k$	$H(m)\ A = xs\ B + R$
2	$H(m)$	1	xs	$H(m) \equiv a + xsk$	$H(m)\ A = B + xs\ R$
3	1	xs	$H(m)$	$1 \equiv xsa + H(m)k$	$A = xs\ B + H(m)\ R$
4	1	$H(m)$	xs	$1 \equiv H(m)a + xsk$	$A = H(m)\ B + xs\ R$
5	xs	1	$H(m)$	$xs \equiv a + H(m)k$	$xs\ A = B + H(m)\ R$
6	xs	$H(m)$	1	$xs \equiv H(m)a + k$	$xs\ A = H(m)\ B + R$

Example 7: This example illustrates the fourth equation in the table 9 above.

Let $E_p(\alpha,\beta)$ be an elliptic curve with $\alpha=-17,\ \beta=23$ and p = 32769769.

$(\Delta \equiv -(4\alpha^3+27\beta^2) \equiv 32764400\ [p]).$

The cardinality of the elliptic curve is

$$\#E_p(\alpha,\beta) = 32771810 = 2\times 5\times 3277181.$$

Alice chooses randomly the point A = (345143, 2110053) whose order is n = 3277181 and the integer a = 7762123. She computes $B = a\,A$ = (26330265, 26185579).

The public and private key of Alice are $(A,B,E_p(\alpha,\beta))$ and a respectively.

To sign the message m such that $H(m)$=154194, Alice calculates:

1. selects k = 6710831, and computes $R = k\,A$ = (20689271, 4324893).
2. $s \equiv \frac{1-H(m)a}{xk} \equiv 211663\ [n].$

The message signature is $(H(m), R, s)$ = (154194, (20689271, 4324893), 211663).

Bob verifies the signature as follows:

He computes $H(m)\,B + xs\,R$ = (345143, 2110053). He finds $A = H(m)\,B + xs\,R$. Hence the signature is valid.

4. Conclusion

In this work, inspired by the work of Horster et al., and for a theoretical and pedagogical interest, we presented a series of digitale signatures based on elliptic curves. The descriptions were illustrated by examples.

References

[1] J. Buchmann, Introduction to Cryptography, Springer Science & Business Media (2013).

[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654 (1976).

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472 (1985).

[4] L. C. Guillou and J. J. Quisquater, "A 'paradoxical' identity-based signature scheme resulting from zero-knowledge," in Proc. Advances Cryptol., pp. 216–231, Springer-Verlag (1990).

[5] D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer Science & Business Media (2006).

[6] J. Hoffstein, J. Pipher, and J. H. Silverman, An Introduction to Mathematical Cryptography, Springer (2008).

[7] P. Horster, M. Michels, and H. Peterson, "Generalized ElGamal signatures for one message block," Citeseer (1994).

[8] M. Ihia and O. Khadir, "Amelioration of ElGamal digital signature schemes," *Int. J. Inf. Sec.*, vol. 42, pp. 117–126 (2019).

[9] N. Koblitz, A Course in Number Theory and Cryptography, 2nd ed., Springer-Verlag (1994).

[10] N. Koblitz, Algebraic Aspects of Cryptography, vol. 3 of Algorithms and Computation in Mathematics, Springer-Verlag (1998).

[11] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209 (1987).

[12] D. W. Kravitz, "Digital signature algorithm," Google Patents, US Patent 5, 231, 668, July 27 (1993).

[13] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press (1996).

[14] V. S. Miller, "Use of elliptic curves in cryptography," in Conf. Theory Appl. Cryptogr. Tech., pp. 417–426 (1985).

[15] O. M. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Massachusetts Institute of Technology, Cambridge Lab for Computer Science (1979).

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126 (1978).

[17] D. R. Stinson, Cryptography: Theory and Practice, Chapman and Hall/CRC (2005).

[18] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press (2008).

[19] N. Mehibel and M. Hamadouche, "A new enhancement of elliptic curve digital signature algorithm," *J. Discrete Math. Sci. Cryptogr.,* vol. 23, no. 3, pp. 743–757 (2020).

[20] D. M. Kuryazov, "Development of electronic digital signature algorithms with compound modules and their cryptanalysis," *J. Discrete Math. Sci. Cryptogr.,* vol. 24, no. 4, pp. 1085–1099 (2021).

Received September, 2021

Revised March, 2022