Libertas Mathematica (new series)
Volume 38(2018), No. 1, 59-68

Adaptation of a Cryptosystem Based on the Arithmetic of Finite Fields to Elliptic Curves

Ounasser Abid and Omar Khadir

Abstract: In this paper, we present an encryption and decryption scheme based on the use of the discrete logarithm problem in elliptic curves. Our cryptosystem is inspired from Harn and Yang work. We show that the method is as secure as the ElGamal equivalent, and has a 1:1 expansion ratio. We also analyze the protocol security, discuss its running time and give a numerical example.

Keywords: Public key cryptography, discrete logarithm problem, elliptic curves.

MSC2010: 94A60, 14H52.

1 Introduction

The last three decades have seen enormous changes in cryptography. In the year 1976 Diffie and Hellman introduced to the world what's come to be known as public-key cryptography. As they explained in their article [7], the purpose of a key exchange protocol is to agree upon a shared key between two correspondents over an insecure channel. And a third person can not extract the common key from their intercepted communication.
Consequently, many other researchers explored this idea, and asymmetric encryption schemes appeared. The first one was RSA [20] proposed by Rivest et al. in 1977. Two years later, Rabin published his Cryptosystem [19], in which, it was proved, for the first time, that recovering the message from the cipher-text was as hard as factoring. And in 1984 ElGamal [8] devised a probabilistic encryption method with one caveat, that the cipher-text is twice the size of the plain-text. Simultaneously, asymmetric cryptography gave birth to digital signature schemes such as RSA, DSA and ECDSA [20, 15].
Meanwhile, the interest of elliptic curves in cryptography begins to grow. Especially, since the publications of Miller [18] in 1985 and Koblitz [16] in 1987. According to Blake et al. [3, p. 9], it is estimated that a key size of 173 bits for an elliptic curve system gives the same security level as 1024 bits in RSA. Which explains its interest

especially for systems with memory constraints and low computing power. Such as smart cards and network equipment.
At first, the use of elliptic curve cryptology was esoteric and complex to implement. But then new discoveries were made and researchers became well aware of its benefits. In 1985, Schoof [22] was the first to present an algorithm able to count elliptic curve points in a polynomial time. In 1999 Satoh [21] came up with a better method that works with very small characteristics. With growing popularity, elliptic curves attracted the interest of cryptanalysts. Like the Weil descent attack introduced by Frey in 1998 [10]. This attack aims to undermine the elliptic curve discrete logarithm problem by using Weil restriction of scalars for elliptic curves. In 2002 this idea was further developed by Gaudry et al. [11]. In 2000 Joux [14] published a paper where he proposed a three persons version of Diffie-Hellman protocol. Thus, pairing on elliptic curves appears to offer the most efficient way for implementing identity based cryptosystems. Such as Boneh's scheme [4], which is based on the Weil pairing.
With an added complexity, elliptic curve schemes have many advantages over the classical ones. Therefore elliptic curve implementations of almost every cryptographic algorithm were developed. Including cryptosystems [16, 6] and digital signatures [1].
In this work, we present a new cryptosystem based on elliptic curves and the ideas of Harn and Hang [13]. We discuss and analyze the security of the proposed protocol.
The rest of this paper is organized as follows. In section two, elliptic curve group is reviewed. In section three, we recall how to map text to points belonging to elliptic curves. Then, an elliptic curve analog of ElGamal cryptosystem [8] is presented. After that, Harn and Yang algorithm [13] is described. In section four we explain our proposed protocol, calculate its running time and analyze its security. And in the last section the conclusion.
Let p be a prime number. We will use $GF(p)$ to mean a finite field of all modular integers less than p. The set of integers is $\mathbb{Z}$. Let a,b,$c \in \mathbb{Z}$. The equivalence $a \equiv b \ (mod\ c)$ is used when c divides $(a - b)$, and $a = b \ mod\ c$ means that a is the remainder of b/c.
Let's start by recalling elliptic curves group.

2 Overview of elliptic curve group

Elliptic curves have many applications in a variety of mathematical fields. Including encryption [18, 16] and factoring integers [17]. And they were used in number theory to prove Fermat's Last Theorem [25].
We mean by elliptic curve $E(K)$ an irreducible non-singular projective algebraic

curve of genus one with a point at infinity $\mathcal{O}$, defined over a field K with $char(K) \neq 2; 3$. It is the set of all solutions (x, y) for the equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

The point $\mathcal{O}$ plays the role of the neutral element in addition. By change of variables we obtain a simple Weierstrass equation [23] which we will use from now on:

$$y^2 = x^3 + ax + b$$

with $a, b \in K$ and the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. Which means that the equation above defines a non-singular curve. i.e., its graphic representation has no isolated points, cusps, or self-intersections. The graph of a real elliptic curve has two components when $\Delta < 0$, and it has one component when $\Delta > 0$.
We are interested in elliptic curves over a field $\mathbb{F}_p$, where p is prime. We define $E_p(a, b)$ over $\mathbb{F}_p$ as $\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 \equiv x^3 + ax + b \ (mod\ p)\} \cup \{\mathcal{O}\}$, with $a, b \in \{1, 2, ..., p-1\}$ and $4a^3 + 27b^2 \neq 0 \ (\ mod\ p)$.

Definition 2.1. Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be two points on $E_p(a, b)$. Let $R(x_3, y_3)$ be the sum of P and Q We can define addition of two points as follows. First, when P and Q are the same point, i.e., point doubling, there are two cases. If $y_1 = 0$ then $R = \mathcal{O}$. If $y_1 \neq 0$ then

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 \ (\ mod\ p),\ \lambda \equiv \dfrac{3x_1^2 + a}{2y_1} \ (\ mod\ p) \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \ (\ mod\ p) \end{cases}$$

And when $P \neq Q$, then we have:

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \ (\ mod\ p),\quad \lambda \equiv \dfrac{y_2 - y_1}{x_2 - x_1} \ (\ mod\ p) \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \ (\ mod\ p) \end{cases}$$

The set of the points of elliptic curve plus a point at infinity $\mathcal{O}$, equipped with addition constitute a group. Moreover it is a finite abelian group.

3 Previous work

We first recall how to represent a message by mean of points in elliptic curve.

3.1 How to encode a message by elliptic curves

The encryption and decryption processes are done on points in elliptic curve. The representation of messages as points in an elliptic curve is performed using mapping algorithms such as in reference [9]. The method presented here can be found in [24, p. 174]
Let p be a prime and m a message such $0 < m < \frac{p}{100} - 1$, so $0 < 100m + 100 < p$ which means:

$$\forall i \in \{0, 1, 2, ..., 99\}, 0 < 100m + i < p$$

Let $x_i = 100m + i$ for all $i \in \{0, 1, 2, ..., 99\}$. As i can be seen as the reminder of x_i by m, knowing any x_i suffices to get m.
Half the elements of $GF(p)$ are quadratic residues modulo p, because p is prime. Let's pose:

$$z_i \equiv (x_i^3 + ax_i + b) \ (mod\ p)$$

There is a probability of 2^{-100} that all z_i are not perfect squares modulo p. So there is a big chance to find an element z_{i_0} satisfying the relation above and at the same time it is a quadratic residue modulo p. Let y be an integer in $\{0, ..., p-1\}$ as $z_{i_0} \equiv y^2 \ (mod\ p)$. On one hand, we can calculate y, especially if p is a Blum prime. i.e. $p \equiv 3 \ (mod\ 4)$. On the other hand, the point (z_{i_0}, y) is in the elliptic curve $E_p(a, b)$ because it verifies its equation.
Now we review the elliptic curve analog of ElGamal cryptosystem as explained in [12, p. 14] and [16].

3.2 ElGamal elliptic curve cryptosystem

Let $E_p(a, b)$ be a fixed finite elliptic curve. In order for Bob to receive a message m over an insecure channel from Alice, he needs to select a point G with a large order n, he chooses a private key d randomly in $\{1, ...n\}$ and calculates $A = dG$. He publishes the elliptic curve public key parameters (p, a, b, G, A, n).
If Alice likes to send a message M in $E_p(a, b)$ to Bob, she selects a random number k and calculates two point $C_1 = kG$ and $C_2 = M + kA$, then she sends C_1 and C_2 to Bob.
We have $C_2 - dC_1 = M + kA - d(kG) = M + kA - k(dG) = M$. Upon reception of C_1 and C_2, Bob computes M by $M = C_2 - dC_1$.
To select a generator in an elliptic curve $E_p(a, b)$, the point must have an order equal to the cardinality of $E_p(a, b)$. We can choose an EC with prime cardinality, in this case all the points are generators. References [2, 5] explain how to construct elliptic curve with prime order.

3.3 Harn and Yang Method

The scheme of Lein Harn and Shoubao Yang [13] is described in three steps:
Step 1 : Distribution
Let p be a prime of the form $p = 2p' + 1$, where p' is also a prime (p is a safe prime). Let α be a generator in $GF(p)$. Alice selects her secret key x_a, then she publishes her public key $y_a \equiv \alpha^{x_a} \ (mod\ p)$. Bob takes k_b randomly in $\{1, 2, ..., p-1\}$, so that $K_{AB} \equiv (y_a)^{k_b} \ (mod\ p)$ is a primitive element modulo p'. Then Bob calculates his public session key $y_b \equiv \alpha^{k_b} \ (mod\ p)$, and he transmits y_b to Alice. Which computes the session shared key $K_{AB} \equiv (y_b)^{x_a} \ (mod\ p)$.
Step 2 : Encryption
Let's suppose that Bob wants to send the following messages $\{m_1, m_2, ..., m_n\}$ to Alice. For every i he determines:

$$\begin{cases} K_{i,1} \equiv K_{i-1,1} K_{AB} \equiv (K_{AB})^i \ (mod\ p') & , K_{0,1} = 1 \\ K_{i,2} \equiv \alpha^{K_{i,1}} \ (mod\ p) \end{cases}$$

He calculates the cipher-text C_i of the message m_i by : $C_i \equiv K_{i,2} m_i \ (mod\ p)$. Then, Bob sends $\{C_1, C_2, ..., C_n\}$ to Alice.
Step 3 : Decryption
To decipher all C_i Alice uses the following equation:

$$m_i \equiv C_i (K_{i,2})^{-1} \ (mod\ p)$$

The inverse of $K_{i,2}$ modulo p can be obtained without knowing $K_{i,2}$. We have $1 \equiv \alpha^{p-1} \equiv \alpha^{K_{i,1}+(p-1-K_{i,1})} \equiv K_{i,2} \alpha^{p-1-K_{i,1}} \ (mod\ p)$, so $(K_{i,2})^{-1} \equiv \alpha^{p-1-K_{i,1}} \ (mod\ p)$

4 Our contribution

4.1 Presentation of the protocol

We describe our algorithm in three phases:
Key agreement: Bob and Alice agree on a generator G in a cyclic elliptic curve E defined by a and b modulo a prime p of the form $p = 2p' + 1$, where p' is also a prime.
As in Diffie-Hellman protocol [7], Alice and Bob choose k_a and k_b randomly in $\{1, ..., p-1\}$ as their respective secrets. Then, Alice sends $k_a G$ to Bob, who sends her back $k_b G$. Thus, they both have a common key $K_{AB} = k_a k_b G$.
Encryption: We suppose that Bob wants to send to Alice multiple messages $\{M_1, ..., M_l\}$. For every i he computes:

$$\begin{cases} K_{i,1} = iK_{AB} = K_{i-1,1} + K_{AB} & , \ with\ K_{0,1} = \mathcal{O} \\ K_{i,2} = G + K_{i,1} \end{cases}$$

Then, he calculates C_i the cipher point of M_i by : $C_i = K_{i,2} + M_i$. And he sends $\{C_1, C_2, ..., C_l\}$ to Alice.
Decryption: Upon reception of $\{C_1, C_2, ..., C_l\}$, Alice can get $\{M_1, M_2, ..., M_l\}$ by the equation $M_i = C_i - K_{i,2}$. Because she is able to compute $K_{i,2}$ for every i.

Example 4.1. Let E be an elliptic curve defined by $y^2 = x^3 + x + 6$ over $GF(p)$, with $p = 2.1289 + 1 = 2579$. And let the generator be the point $G = (2573, 1140)$. To create the shared key K_{AB}, Alice selects $k_a = 1327$ and sends $k_aG = (2456, 629)$ to Bob, who chooses a random number too $k_b = 1987$ and sends $k_bG = (187, 823)$ back to her. Now they both can calculate $K_{AB} = k_ak_bG = (1770, 154)$.
To encipher these three points $M_1 = (2, 2575)$ $M_2 = (3, 2573)$ $M_3 = (2254, 2554)$. We have to compute their corresponding $K_{i,1}$ and $K_{i,2}$:

$$K_{1,1} = K_{AB} = (1770, 154) \quad K_{1,2} = G + K_{1,1} = (2562, 216)$$
$$K_{2,1} = 2K_{AB} = (2089, 1110) \; K_{2,2} = G + K_{2,1} = (619, 1688)$$
$$K_{3,1} = 3K_{AB} = (666, 333) \quad K_{3,2} = G + K_{3,1} = (1028, 2059)$$

From which we calculate the corresponding cipher points:

$$C_1 = K_{1,2} + M_1 = (1435, 2480)$$
$$C_2 = K_{2,2} + M_2 = (1481, 2389)$$
$$C_3 = K_{3,2} + M_3 = (1758, 1479)$$

By deciphering the points we get the plain points we started with:

$$M_1 = C_1 - K_{1,2} = (2, 2575)$$
$$M_2 = C_2 - K_{2,2} = (3, 2573)$$
$$M_3 = C_3 - K_{3,2} = (2254, 2554)$$

4.2 Running time and Discussion

Let t_{add} and t_{mult} be respectively the times needed to perform point addition and a scalar multiplication. Key setup needs $4t_{mult}$ (k_aG, k_bG, $k_a(k_bG)$ and $k_b(k_aG)$). Suppose that the correspondent wants to send just one message. In encryption, three additions are executed. Plus one more addition for deciphering. In total encryption and decryption cost $4t_{add}$ for every message sent. Note that we don't make use of multiplication except in key exchange. Which represents a huge computation gain in comparison to other algorithms.
In ElGamal cryptosystem [8], encrypting the same message twice generates different cipher-texts, which gives it an advantage over RSA [20]. But, with the inconvenience of a 2:1 expansion of the plain-text's length after encryption. i.e., two cipher-texts are generated for each message. Our method keeps the probabilistic aspect of the ElGamal's algorithm with a 1:1 expansion ratio, one cipher-text for each message, thus decreasing network bandwidth utilization by half.

4.3 Security analysis

Since there are no proven techniques to demonstrate the security of a encryption scheme. All we can do is to see whether there is a way to break it. Also, we can check it against known attacks. Let Eve be Alice's opponent. Let's evaluate her possible attacks.
1. Chosen plain-text attack:
Eve can obtain an encryption key $K_{i,2}$. But getting $K_{i,1}$ from $K_{i,2} = G + K_{i,1}$ is considered as hard as solving discrete logarithm problem.
Knowing $K_{i,2}$ does not allow Eve to get $K_{i+1,2}$ nor $K_{i-1,2}$, since $K_{i,2} = G + K_{i,1}$ and $K_{i+1,2} = G + (K_{i,1}.K_{AB})$. And she does not know K_{AB} the session common secret key.
2. Known plain-text attack:
If, somehow, Eve got hold of two cipher-texts $C_i = K_{i,2} + M$ and $C_j = K_{j,2} + M$ of a known message M. She could not extract neither $K_{i,2}$ nor $K_{j,2}$. In the case when C_i and C_j are generated during the same session. She can't get the session secret key K_{AB}. If C_i and C_j are generated during two different sessions. Then there is no relation between $K_{i,2}$ and $K_{j,2}$, so Eve can't get K_{AB}.
Note that C_i and C_j can not be equal, because k_a and k_b are chosen randomly and they are tested to be different from used keys in precedent sessions.
3. Cipher-text attack:
We have $C_i = K_{i,2} + M_i$. Since Eve does not know $K_{i,2}$, she cannot obtain M_i. Even if she has $K_{i,2}$, obtaining M_i from the last equation is considered to be as hard as the elliptic curve discrete logarithm problem.

5 Conclusion

In this work, we presented a variant of a Diffie and Hellman cryptosystem over elliptic curves. We also analyzed the protocol security and calculated its running time.

6 Acknowledgements

This work is supported by MMSy e-Orientation project.

References

[1] O. Abid, J. Ettanfouhi, and O. Khadir, *New digital signature protocol based on elliptic curves*, International journal on cryptography and information security

(2012), 210–216.

[2] A Oliver L Atkin and François Morain, *Elliptic curves and primality proving*, Mathematics of computation **61** (1993), no. 203, 29–68.

[3] I. F. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, vol. 265, Cambridge university press, 1999.

[4] Dan Boneh and Matt Franklin, *Identity-based encryption from the weil pairing*, Annual international cryptology conference, Springer, 2001, pp. 213–229.

[5] R. Bröker and P. Stevenhagen, *Constructing elliptic curves of prime order*, Contemp. Math **463** (2008), 17–28.

[6] D. Brown, *Standards for efficient cryptography, sec 1: elliptic curve cryptography*, Released Standard Version **1** (2009).

[7] W. Diffie and M. E. Hellman, *New directions in cryptography*, Information Theory, IEEE Transactions on **22** (1976), no. 6, 644–654.

[8] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, Advances in cryptology, Springer, 1984, pp. 10–18.

[9] P. A. Fouque, A. Joux, and M. Tibouchi, *Injective encodings to elliptic curves*, Australasian Conference on Information Security and Privacy, Springer, 2013, pp. 203–218.

[10] Gerhard Frey and Herbert Gangl, *How to disguise an elliptic curve (weil descent)*, Talk at ECC **98** (1998), 128–161.

[11] Pierrick Gaudry, Florian Hess, and Nigel P Smart, *Constructive and destructive facets of weil descent on elliptic curves*, Journal of Cryptology **15** (2002), no. 1, 19–46.

[12] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, Springer Science & Business Media, 2006.

[13] L. Harn and S. Yang, *Public-key cryptosystem based on the discrete logarithm problem*, International Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1992, pp. 469–476.

[14] A. Joux, *A one round protocol for tripartite diffie–hellman*, International Algorithmic Number Theory Symposium, Springer, 2000, pp. 385–393.

[15] Jonathan Katz, Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone, *Handbook of applied cryptography*, CRC press, 1996.

[16] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of computation **48** (1987), no. 177, 203–209.

[17] H. W. Lenstra Jr, *Factoring integers with elliptic curves*, Annals of mathematics (1987), 649–673.

[18] V. S. Miller, *Use of elliptic curves in cryptography*, Conference on the Theory and Application of Cryptographic Techniques, Springer, 1985, pp. 417–426.

[19] M. O. Rabin, *Digitalized signatures and public-key functions as intractable as factorization*, Tech. report, DTIC Document, 1979.

[20] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.

[21] Takakazu Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, JOURNAL-RAMANUJAN MATHEMATICAL SOCIETY **15** (2000), no. 4, 247–270.

[22] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod* ‘, Mathematics of computation **44** (1985), no. 170, 483–494.

[23] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

[24] L. C. Washington, *Elliptic curves: number theory and cryptography*, CRC press, 2008.

[25] A. Wiles, *Modular elliptic curves and fermat's last theorem*, Annals of mathematics **141** (1995), no. 3, 443–551.

Ounasser Abid
Laboratory of Mathematics, Cryptography,
Mechanics and Numerical Analysis, FSTM,
University Hassan II of Casablanca,
Morocco
E-mail: abidounasser@gmail.com

Omar Khadir
Laboratory of Mathematics, Cryptography,
Mechanics and Numerical Analysis, FSTM,
University Hassan II of Casablanca,
Morocco
E-mail: khadir@hotmail.com