SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.04 NO. 1 2025
DOI: 10.51984/SUCP.V4I1.3835

المؤتمر العلمي الأول للتطبيقات الهندسية (ICEA'2024)
The First Scientific Conference on Engineering Applications (ICEA'2024)
Conference homepage: www.icea.ly

Security Improvement of Communication Network using Encryption by Elliptic Curve with Precomputation and Continued Fractions

*Fatimah Dawoud Mousay[1], Souad I. Mugassabi[2]

[1]Department of Mathematics,The Libyan Academy,Benghazi, Libya.
[2]Department of Mathematics, University of Benghazi, Benghazi, Libya.

Keywords:
Elliptic curve cryptography.
Diffie-Hellman encryption.
Elliptic curve over Finite field.
Simple continued fractions.
Convergence.
Invalid curve attack.

ABSTRACT

The increasing data transformation through the network, the appearance of Bitcoin and alternative information over millions of miles, the need for new or more secure methods was found. The elliptic curve cryptography is widely used in encryption. However, there are a variety of attacks such as invalid curve which is the most popular attack that can be used to manipulate the safety of cryptosystem by nonprime group order, it would be connected with methods of cryptography such as asymmetric cryptography and according to the fact that elliptic curve ciphers are based in smartcards introduce a high level of secure data transformation due its advantage of requires less computational power memory. This paper assures the need for secure key exchange by combining elliptic curve cryptography with precomputation and simple continued fractions that help us to fix and observe new mathematical attacks.

تحسين أمان شبكة الاتصال باستخدام تشفير بواسطة المنحنى البيضاوي مع الحساب المسبق والكسور المستمرة

*فاطمة موسي[1] و سعاد المقصبي[2]

[1]قسم الرياضيات، الاكاديمية الليبية، بنغازي، ليبيا.
[2]قسم الرياضيات، جامعة بنغازي، بنغازي، ليبيا.

الكلمات المفتاحية:
التقارب
لكسور المستمرة البسيطة
المنحنى البيضاوي على الحقل المحدود
تشفير المنحنى البيضاوي
تشفير ديفي-هيلمان
هجوم المنحنى غير الصالح.

الملخص

زيادة تحويل البيانات عبر الشبكة، وظهور البيتكوين والمعلومات البديلة على مسافات تصل إلى الملايين من الأميال، أدى إلى الحاجة إلى طرق جديدة أو أكثر أمانًا. يُستخدم تشفير المنحنى البيضاوي على نطاق واسع في التشفير. ومع ذلك، هناك مجموعة متنوعة من الهجمات مثل المنحنى غير الصالح والتي تعتبر الهجوم الأكثر شهرة الذي يمكن استخدامه للتلاعب بسلامة نظام التشفير من خلال ترتيب مجموعة غير الأولية، فإنه سيتم ربطه بأساليب التشفير مثل التشفير غير المتماثل ووفقًا لحقيقة أن تشفير المنحنى البيضاوي يعتمد على بطاقات ذكية تقدم مستوى عالٍ من تحويل البيانات الآمن بسبب ميزته التي تتطلب أقل قدر من قوة الحوسبة والذاكرة. تؤكد هذه الورقة على الحاجة إلى تبادل مفاتيح آمن من خلال دمج تشفير المنحنى البيضاوي مع الحساب المسبق والكسور المستمرة البسيطة التي تساعدنا على إصلاح ومراقبة الهجمات الرياضية الجديدة.

1. Introduction

Cryptography is referred to protect the information and the authentication methods among parties of communication. It also aims to protect protocols against saboteurs sharing trustworthy information. Providing a secure data, because the security via obscurity is has not worked well historically, it is crucial to both evaluate in the open and develop trust in security through algorithms. Asymmetric cryptography also known as public key cryptography was discovered in the late 1970s. It utilizes separate keys for each communication party this process is known as key exchange this algorithm requires a key pair consisting of private keys. The second type of cryptography is symmetric or cipher it requires two parties of communication to have the same secret key for both encryption and decryption. Victor Mieller published a paper titled "Use of elliptic curves in cryptography" in 1985, independently of Koblitz's suggesting of using elliptic curves in cryptography. Due to its efficiency benefits, elliptic curve encryption, or simply ECC is widely used in many applications such as IC cards, mobile devices, teleported robotics and Bitcoin. The importance of understanding the cryptography behind Bitcoin or any other cryptocurrencies to make you capable of trusting them. The advantage of ECC is the complexity of solving discrete logarithm problems makes it a strong method to encrypt information.

2. Related Work

Precomputation on Elliptic curve cryptography to hide the actual equation by another equation could be reached by the first one using a

*Corresponding author:
E-mail addresses: Alhotifatima@gmail.com, (S. I. Mugassabi) Souad.Mugassabi@uob.edu.ly
Article History : Received 17 March 2024 - Received in revised form 25 August 2024 - Accepted 15 October 2024

secret key in [1], the precomputation on elliptic curve cryptography of transform points on an elliptic curve to a fractional formula that makes the algorithm more secure. Introduce an attack on Bluetooth pairing protocols for wireless communication between devices which changes keys using authenticated Elliptic curve Diffie-Hellman (ECDH) [3]. However, the security of Diffie-Hellman is less secure than widely believed. In [4] discussing this suggestion it also applies to (ECDH) although it still resists classical cryptanalysis like Pollard-rho attacks. In [5] providing such a class making different assumptions rather than mathematical breakthroughs as it followed in this paper.

3. Elliptic Curve

One of the most popular curve structure have two possible graphs see figure1 for elliptic curve of characteristic nether 2 or 3.

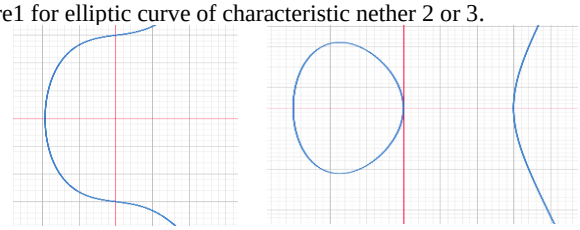


Figure 1: Elliptic curves

4. Projective plane

The concept of change points from any field (real number as the usual or finite field of characteristic p is very crucial to consider the points on the elliptic curve to construct an abelian group due it the elliptic curve over projective plan gives extra points called points at infinity which can represent them by one point on elliptic curve role the identity element as zero of real number. In addition to the importance of studying the projective plane and its relation to the theory of elliptic curve although the precomputation of points on an elliptic curve [1] familiar to this concept work.

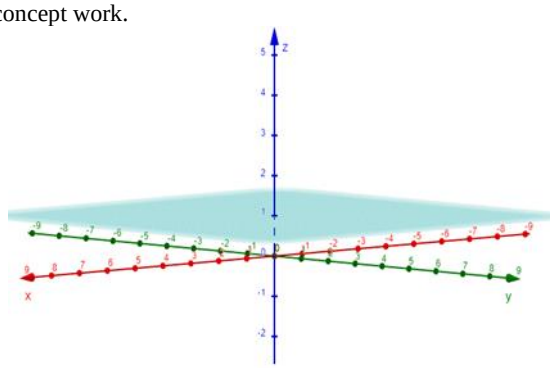


Figure 2: The geometric meaning of points on projective plane.

5. Elliptic curve over projective plane

The elliptic curve is a nonsingular projective curve in Weierstrass define as

$$y^2z = x^3 + Axz^2 + Bz^3 \quad (1)$$

where A, B constants, and every point in elliptic curve represents as $P = [x, y, 1]$. In order to comprise a group the definition of operation of points (addition) on elliptic curve defined as following:

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2, \quad y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) + y_1$$

$$P_1 + P_2 = [x_3, y_3, 1]$$

or

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$$

where

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = -[m^2(x_3 - x_1) + y_1]$$

If $P \neq Q$ then

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \quad (2)$$

and if $P = Q$ we have

$$m = \frac{3x^2 + a}{2y}.$$

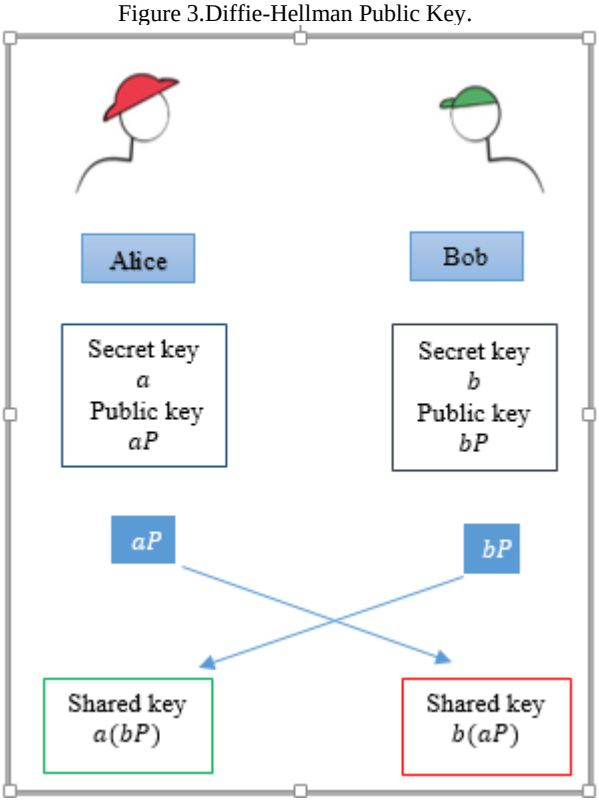
6. Point at infinity

The point [0,1,0] represents the zero element of the points on an elliptic curve it has no simpler way to be written as $y = 1$ it is appears on every vertical line so that we can define the inverse of any point $[x, y]$ as $[x, -y]$ due to the symmetric of the elliptic curve showing in figure 1.

7. Diffie-Hellman Public Key Encryption

One of the key exchange algorithms in asymmetric cryptography is called after its creators Diffie-Hellman. The primary goal is to create a shared secret between two parties.

Figure 3.Diffie-Hellman Public Key.



To construct $ECDH$ uses the points on an elliptic curve over a finite field see [7] (for more details) as G, P and Q and respect $E(F_p)$ designed to adhere to every ECC security requirement to be secure as prime order, high twist order nonsupersingular elliptic curve, and avoiding an anomalous elliptic curve which is DLP may be solved with ease with it.

Use the Pari/GP calculator version 2.16.0.

The elliptic curve equation

$$Y^2 = X^3 + \frac{5}{2}X + \frac{4}{3} \; mod \; 67531$$

Suppose that

$$X = \frac{x}{n'l^2}, Y = \frac{y}{n'l^3}$$

So that

$$\left(\frac{y}{n'l^3}\right)^2 = \left(\frac{x}{n'l^2}\right)^3 + \frac{4}{3}\frac{x}{n'l^2} + \frac{4}{3}$$

since $l = lcm(2,3) = 6$,

choice of n' to be 1

$$y^2 = x^3 + 3240x + 62208 \; mod \; 67531 \quad (4)$$

The point (64801,51707) in (4) can be written as:

$$G = \left(\frac{64801}{36}, \frac{51707}{216}\right) = \left[\frac{64801}{36}, \frac{51707}{216}, 1\right]$$

It would be easy to see that the secret key is 1, however the points

$$P = \left(\frac{38647}{36}, \frac{20414}{216}\right) = [231882, 20414, 216]$$

It can be simply its y coordinate to

$$P = \left(\frac{38647}{36}, \frac{10207}{108}\right) = \left[\frac{38647}{36}, \frac{10207}{108}, 1\right]$$

But multiply by 108 deduce to

$$[115941, 10207, 108]$$

Because there exist $\lambda = 2$ such that

$$[231882, 20414, 216] \equiv [115941, 10207, 108]$$

8. SIMPLE CONTINUED FRACTIONS

An expression of the form $a_0 + \cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots+\cfrac{1}{a_n}}}} = [a_0; a_1, a_2, \dots, a_n]$, is called a finite simple continued fraction (SCF) [9-14], where a_n is a positive integer number for all $n \geq 1$, a_0 is an integer number.

Theorem (1)

The real number α is a rational number if and only if it can be expressed as a finite SCF.

Theorem (2)

The SCF $[a_0; a_1, \dots, a_n]$ can be defined as

$[a_0; a_1, \dots, a_n] = a_0 + \frac{K_{n-1}(a_2)}{K_n(a_1)}$, or

$[a_0; a_1, \dots, a_n] = \frac{K_{n+1}(a_0)}{K_n(a_1)}$, where

$$K_i(a_j) = a_{i+(j-1)}K_{i-1}(a_j) + K_{i-2}(a_j), \qquad i = 1,2, \dots, n,$$

$j = 0,1,2, \dots, n$, $K_{-i}(a_j) = 0$ and $K_0(a_j) = 1$.

Definition (2)

(i) $[a_0; a_1, \dots, a_n] = [b_0; b_1, \dots, b_n]$ if $a_i = b_i$ for $i = 0,1,2, \dots, n$.

(ii) $[a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_n - 1,1]$.

(iii) $[a_0; \dots, a_{j-1}, 0, a_{j+1}, \dots, a_n] = [a_0; \dots, a_{j-1} + a_{j+1}, \dots, a_n]$.

(iv) $[a_0; \dots, a_{j-1}, 0,0, a_{j+1}, \dots, a_n] = [a_0; \dots, a_{j-1}, a_{j+1}, \dots, a_n]$.

Theorem (3)

Let $[a_0;a_1, \dots, a_n]$ be SCF, the sequences $p_0, p_1, \dots, p_n$ and $q_{0,}q_1 \dots, q_n$ be defined recursively by $p_m = K_{m+1}(a_0)$ and $q_m = K_m(a_1)$, for $m = 0,1, \dots, n$ where $K_{m+1}(a_0)$ and $K_m(a_1)$ as in definition (2), then the m-th convergence $c_m = [a_0;a_1, \dots, a_m]$ is give by

$$c_m = \frac{p_m}{q_m}$$

Example (2)

Use the Pari/GP calculator version 2.16.0.

Suppose Alice and Bob agree on elliptic curve equation (4) in example (1) with the point$P = \left(\frac{38647}{36}, \frac{20414}{216}\right)$, the simple continued fraction for $\frac{38647}{36}$ is $[1073; 1,1,8,2]$ and the convergent are

$c_0 = \frac{1073}{1}$, $c_1 = \frac{1074}{1}$, $c_2 = \frac{2147}{2}$, $c_3 = \frac{18250}{17}$ and $c_4 = \frac{38647}{36}$.

Also, the simple continued fraction for $\frac{20414}{216} = \frac{10207}{108}$ is $[94; 1,1,26,2]$ and the convergent are

$c_0 = \frac{94}{1}$, $c_1 = \frac{95}{1}$, $c_2 = \frac{189}{2}$, $c_3 = \frac{5009}{53}$ and $c_4 = \frac{10207}{108}$.

Alice choose the integer $a = 177$ as her private key she then computes aP first she need to rewrite the generator P on the integer form by multiplying P' coordinates by l^2, l^3 respectively. So that her public key will be

$aP = 771(38647,20414) = (20262,16730)$.

Thus she rewrite her public key in fraction form as $aP = \left(\frac{20262}{36}, \frac{16730}{216}\right)$, the simple continued fraction for $\frac{20262}{36} = \frac{3377}{6}$ is $[562; 1,5]$ and the convergent are $c_0 = \frac{562}{1}$, $c_1 = \frac{563}{1}$ and $c_2 = \frac{3377}{6}$.

Also, the simple continued fraction for $\frac{16730}{216} = \frac{8365}{108}$ is $[77; 2,4,1,9]$ and the convergent are $c_0 = \frac{77}{1}$, $c_1 = \frac{155}{1}$, $c_2 = \frac{697}{9}$, $c_3 = \frac{852}{11}$ and $c_4 = \frac{8365}{108}$.

She can send this number to Bob

Bob choose $b = 561$ for his private key and computes bP after writing to fraction formula$bP = \left(\frac{5268}{36}, \frac{1998}{216}\right)$, the simple continued fraction for $\frac{5268}{36} = \frac{439}{3}$ is $[146; 3]$ and the convergent are $c_0 = \frac{146}{1}$ and$c_1 = \frac{439}{3}$. Also, the simple continued fraction for $\frac{1998}{216} = \frac{37}{4}$ is $[9; 4]$ and the convergent are$c_0 = \frac{9}{1}$, $c_1 = \frac{37}{4}$, $c_2 = \frac{697}{9}$, $c_3 = \frac{852}{11}$ and $c_4 = \frac{8365}{108}$.

9. Conclusion

In ECC with precomputation a secret key have found out a mathematical attack of knowing that key (n') which is appeared in the points on the elliptic curve when we using its projective formula that helps to implement this attack. From the uniqueness of the simple continued fraction formula of any fraction and its converges we will be able to find a way to protect this secret key of precomputation from that attack by using some converges of elliptic curve's coordinates and build up to a more secure algorithm.

10. Acknowledgment

The authors are grateful to Department of Mathematics in Libyan Academy, Department of Mathematics in University of Benghazi

11. References

[1] Mousay, F. D., Mugassabi, S. I., & Budalal, A. A. (2023, December). Security Measures for Ensuring Confidentiality of Information Using Encryption by Elliptic Curve with Precomputation. In *2023 IEEE 11th International Conference on Systems and Control (ICSC)* (pp. 938-942). IEEE.

[2] Wong, D. (2021). *Real-world cryptography*. Simon and Schuster.

[3] Biham, E., & Neumann, L. (2020). Breaking the bluetooth pairing–the fixed coordinate invalid curve attack. In Selected Areas in Cryptography–SAC 2019: 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers 26 (pp. 250-273). Springer International Publishing..

[4] Haakegaard, R., & Lang, J. (2015). The elliptic curve diffie-hellman (ecdh). Online at https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Haakegaard+ Lang. pd

[5] Dubois, R. (2017). Trapping ECC with invalid curve bug attacks. Cryptology ePrint Archive

[6] small subgroup and invalid curve attacks on protocols using Diffie-Hellman. In 2019 IEEE 32nd Computer Security Foundations Symposium (CSF) (pp. 78-7815). IEE

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

[8] Koshy, T. (2002). Elementary number theory with applications. Academic press.

[9] Lozano-Robledo, Á. (2011). Elliptic curves, modular forms, and their L-functions (Vol. 58). American Mathematical S

[10] Mugassabi, Souad I. and Somia M. Amsheri. "The Multiplication and Division of Simple Continued Fractions". IJISM 8.3 (2020): 130-136.

[11] Mugassabi, S., & Elmabrok, A. S. (2019) The Power of Simple Continued Fractions. EPH-International Journal of Applied Science (ISSN: 2208-2182), 1(1), 824-833.

[12] Mugassabi, Souad I., and Fatima F. Abdullah. (2020) The Addition and Subtraction Operations for two Continued Fractions. GPH-International Journal of Mathematics 2.07: 01-04.

[13] Mugassabi, S., & Mistiri, F. (2015). *The Elementary Arithmetic Operators of Continued Fractions*'. Am-Euras. *J. Sci. Res*, *10*(5), 251-263.

[14] Souad I. Mugassabi1, et al. (2022). Some Operations of Simple Continued Fractions and Snake Graphs. Libyan Journal of Basic Sciences (LJBS). Vol: 19, Issue: 2, P: 33-42.

[15] Fatima F. Abdullah, Souad I. Mugassabi, (2020). The Multiplication Operation of Two Continued Fractions with Positive Non Integer Numerators. IRJIET, Volume 4, Issue 7, pp 14-19.