ĐỀ XUẤT MÃ HÓA THÔNG QUA VỊ TRÍ ĐIỂM TRÊN ĐƯỜNG CONG ELLIPTIC

PROPOSED CODING THROUGH POINT POSITIONS ON AN ELLIPTIC CURVE

Mai Mạnh Trừng*, Trần Minh Đức, Lê Thị Thu Hiền

Khoa Công nghệ thông tin, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Đến Tòa soạn ngày 09/03/2021, chấp nhận đăng ngày 22/04/2021

Tóm tắt: Bài báo dựa trên ý tưởng toán học trên đường cong Elliptic. Số học đường cong Elliptic này được ứng dụng trong bảo mật, an toàn thông tin, chứng thực, chữ ký số. So với các hệ mật truyền thống khác với cùng kích thước khóa thì hệ mật đường cong Elliptic có độ mật tốt hơn. Trong bài báo này nhóm tác giả đề xuất không cần tạo chuỗi dữ liệu để mã hóa mà chỉ cần lấy vị trí của điểm tương ứng ký tự để mã hóa. Với việc này thì bản mã ngắn gọn hơn khi gửi bản mã trên mạng sẽ chiếm ít băng thông trên quá trình truyền.

Từ khóa: Mật mã đường cong Elliptic, bảo mật, chuỗi dữ liệu.

Abstract: The paper is based on mathematical ideas on elliptic curves. This Elliptic curve arithmetic is used in security, information security, authentication, and digital signature. The Elliptic curve cryptography has better security than other traditional cryptosystems with the same key strength. In this paper, the authors propose that they do not need to create a data string to encode, but just take the position of the corresponding character point to encode. By this method, this code when sending the ciphertext on the network will take up less bandwidth on the transmission.

Keywords: Elliptic curve cryptography, security, data sequence.

1. GIỚI THIỆU

Những năm gần đây ở Việt Nam, đường cong Elliptic có vai trò quan trọng, theo Thông tư số: 39/2017/TT-BTTTT, ngày 15/12/2017 của Bộ Thông tin và Truyền thông về việc Ban hành Danh mục tiêu chuẩn kỹ thuật ứng dụng công nghệ thông tin trong cơ quan nhà nước đã khuyến nghị áp dụng giải thuật mã hóa trên đường cong Elliptic của Tiêu chuẩn về an toàn thông tin.

Nghiên cứu về các đường cong Elliptic của các nhà đại số, các nhà lý thuyết số có từ giữa thế kỷ XIX. Mật mã đường cong Elliptic curve cryptography (ECC) được phát hiện vào năm 1985 bởi Neil Koblitz và Victor Miller [1, 2]. Chúng có thể được xem như các đường cong Elliptic của các hệ mật mã logarit rời rạc. Trong đó nhóm Z_p^* được thay thế bằng nhóm các điểm trên một đường cong Elliptic trên một trường hữu hạn. Cơ sở toán học cho tính bảo mật của các hệ thống mật mã đường cong Elliptic là tính hấp dẫn tính toán của bài toán logarit rời rạc đường cong Elliptic (ECDLP).

Trên thế giới cũng có nhiều ứng dụng [3, 4, 5] sử dụng đường cong Elliptic để đảm với an toàn thông tin. Bài báo [6] cần tạo chuỗi dữ liệu, bài báo [7, 8] sử dụng thuật toán mới đề

xuất cũng sử dụng ý tưởng tạo chuỗi dữ liệu để mã hóa. Bài báo này đã cải tiến so với bài báo [7] là không sử dụng kỹ thuật sinh chuỗi dữ liệu mà lấy vị trí điểm của ký tự. Bởi vì nếu sinh chuỗi sẽ tạo ra không gian dữ liệu lớn làm ảnh hưởng băng thông trên quá trình truyền bản mã.

Hiện nay, hệ mật RSA là giải thuật khoá công khai được sử dụng nhiều, nhưng hệ mật dựa trên đường cong Elliptic (ECC) có thể thay thế cho RSA bởi mức an toàn và tốc độ xử lý cao hơn. Ưu điểm của ECC là hệ mật mã này sử dụng khoá có độ dài nhỏ hơn so với RSA nhưng độ bảo mật là như nhau như bảng 1.

Bảng 1. Mật mã khóa đối xứng và khóa công khai [11]

Symmetric-key	ECC	RSA/DLP
64 bit	128 bit	700 bit
80 bit	160 bit	1024 bit
128 bit	256 bit	2048-3072 bit

2. CƠ SỞ TOÁN HỌC CỦA ĐƯỜNG CONG ELLIPTIC

Đường cong Elliptic E trên trường R của các số thực được xác định bởi một phương trình:

E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ …. (1)

Ở đây a_1, a_2, a_3, a_4, a_6 là các số thực thuộc R; x và y đảm nhận các giá trị trong các số thực. Nếu L là trường mở rộng của số thực, thì nó sẽ là tập hợp các điểm hợp lý L trên đường cong Elliptic E và ∞ là điểm vô cực. Phương trình (2) được gọi là phương trình Weierstrass. Ở đây đường cong Elliptic E được xác định trên trường số nguyên K, vì a_1, a_2, a_3, a_4, a_6 là các số nguyên. Nếu E được xác định trên trường số nguyên K, thì E cũng được xác định trên bất kỳ trường mở rộng nào của K. Điều kiện $4a^3 + 27b^2 \neq 0$ đảm bảo rằng là đường cong Elliptic. Tức là, không có điểm nào tại đó đường cong có hai hoặc nhiều đường tiếp tuyến khác biệt. Điểm ∞ là điểm duy nhất trên đường thẳng ở vô cực thỏa mãn của phương trình Weierstrass [9, 10]. Trong bài báo hiện tại cho mục đích mã hóa và giải mã bằng các đường cong Elliptic, đủ để xem xét phương trình có dạng:

$$y^2 = x^3 + ax + b \quad (2)$$

Đối với các giá trị đã cho của a và b, đồ thị bao gồm giá trị dương và giá trị âm của y cho mỗi giá trị của x. Do đó đường cong này đối xứng với trục x.

Chúng tôi cũng minh họa việc triển khai hệ thống mật mã dựa trên một đường cong Elliptic với khóa đối xứng với phương trình đường cong Elliptic nhóm lựa chọn là:

$$y^2 = x^3 - 2x + 9 \pmod{37} \quad (3)$$

Với phương trình (2) thì a = –2, b = 3, ta có $4\times(-2)^3+27\times(9)^2 = 2155 \neq 0$. Do vậy, phương trình (3) là phương trình đường cong Elliptic. Chúng tôi chọn phương trình này bởi lẽ tìm được tổng số điểm của đường cong là 37 điểm tính cả điểm vô cực. Do vậy, tổng số điểm là số nguyên tố thì tất cả các điểm trên đường cong đều là điểm sinh.

2.1. Phép cộng

Giả sử P = (x_1, y_1) và Q = (x_2, y_2) là hai điểm của E. Nếu $x_1 = x_2$ và $y_1 = -y_2$ thì ta định nghĩa P + Q = ∞. Ngược lại thì P + Q = (x_3, y_3) ∈ E trong đó $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, với:

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), \; khi\, P \neq Q \\ (3x_1^2 + a)/(2y_1) \; khi\, P = Q \end{cases}$$

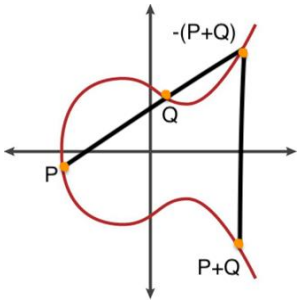
Vậy nếu P ≠ Q tức là $x_1 \neq x_2$, ta có:

$$\begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases} \quad (4)$$

Nếu P = Q tức là $x_1 = x_2$, ta có:

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \end{cases} \quad (5)$$

Chú ý rằng các điểm (x_3, y_3), $(x_3, -y_3)$ cũng nằm trên đường cong E và xét về mặt hình học, thì các điểm (x_1, y_1), (x_2, y_2), $(x_3, -y_3)$ cũng nằm trên một đường thẳng. Ngoài ra, định nghĩa một điểm cộng vô cực bằng chính nó: $P + \infty = \infty + P = P$.

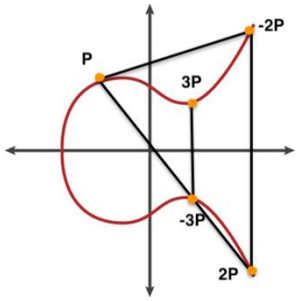


Hình 1. Tổng hai điểm của đường cong Elliptic

2.2. Phép nhân

Phép nhân một số nguyên k với một điểm P thuộc đường cong Elliptic E là điểm Q được xác định bằng cách cộng k lần điểm P và dĩ nhiên $Q \in E$: $k \times P = P + P + P \ldots + P$ (k phép cộng điểm P). Vì vậy nếu G là một điểm thuộc đường cong Elliptic E thì với mỗi số nguyên dương k luôn dễ dàng xác định được điểm $Q = k \times G$..

Khi tổng các điểm P và Q trên đường cong Elliptic E được chỉ ra trong hình 1. Kết quả được xác định là điểm S thu được bằng cách đảo ngược dấu của tọa độ y của điểm R, trong đó R là giao điểm của E và đường thẳng đi qua P và Q. Nếu P và Q ở cùng một vị trí, đường thẳng là tiếp tuyến của E tại P. Ngoài ra, tổng điểm tại vô cực và điểm P được xác định là chính điểm P.



Hình 2. Phép nhân trên đường cong Elliptic

3. THUẬT TOÁN MÃ HÓA VÀ GIẢI MÃ TRÊN ĐƯỜNG CONG ELLIPTIC.

Thành phần mật mã: $(\mathcal{P}, \mathcal{C}, \mathcal{E}, \mathcal{D}, \mathcal{K})$

$\mathcal{P}$: Là bản rõ; $\mathcal{C}$: Là bản mã;

$\mathcal{E}$: Là hàm mã hóa; $\mathcal{D}$: Là hàm giải mã;

$\mathcal{K}$: Là khóa.

Mã hóa:

Bước 1: Xác định tổng số điểm và điểm sinh, sử dụng phép toán cộng và nhân để tính các điểm còn lại trên đường cong.

Bước 2: Gán thứ tự bảng chữ cái và một vài ký tự đặc biệt với các điểm trên đường cong.

Bước 3: Chọn giá trị khóa $\mathcal{K}$ ngẫu nhiên.

Bước 4: Hàm mã hóa.

$$\mathcal{C} = \mathcal{E}(\mathcal{P}) = [(\mathcal{P}_i + \mathcal{K}) \bmod (n)]P \quad (6)$$

Bước 5: Tra cứu điểm vị trí điểm trên đường cong để xác định ký tự tương ứng.

Giải mã:

Bước 6: Hàm giải mã

$$\mathcal{P} = \mathcal{D}(\mathcal{C}) = [(\mathcal{C}_i - \mathcal{K}) \bmod (n)]P \quad (7)$$

Trong đó tham số ở (6), (7):

$\mathcal{P}_i$: Là vị trí của ký tự bản rõ;

$\mathcal{C}_i$: Là vị trí của ký tự bản mã;

$\mathcal{E}$: Là hàm mã hóa;

$\mathcal{D}$: Là hàm giải mã;

$\mathcal{K}$: Là khóa, là một giá trị ngẫu nhiên;

n: Là tổng số điểm trên đường cong Elliptic;

P: Là điểm sinh của đường cong Elliptic.

4. ÁP DỤNG THUẬT TOÁN

Bên A gửi cho bên B một bản rõ (văn bản đầu vào) là SECURITY. Để đảm bảo bí mật trên quá trình truyền, bên A sẽ mã hóa bản rõ trên trước khi gửi trên kênh truyền. Quá trình mã hóa được thể hiện như sau:

Bước 1: Với đường cong E ở (3) ta có 37 điểm trên đường cong tính cả điểm vô cực. Ta tìm được điểm sinh P = (17, 2). Sử dụng công thức (4) và công thức (5) điểm tính các điểm trên đường cong như bảng 2.

Bảng 2. Tập hợp tất cả các điểm trên ECC

∞	(17, 2)	(6, 18)	(10, 8)
(13, 21)	(18, 12)	(28, 36)	(4, 18)
(0, 34)	(27, 19)	(34, 32)	(16, 15)
(25, 28)	(31, 8)	(36, 11)	(12, 14)
(33, 29)	(3, 17)	(24, 24)	(24, 13)
(3, 20)	(33, 8)	(12, 23)	(36, 26)
(31, 29)	(25, 9)	(16, 22)	(34, 5)
(27, 18)	(0, 3)	(4, 19)	(28, 1)
(18, 25)	(13, 16)	(10, 29)	(6, 19)
(17, 35)			

Bước 2: Gán điểm cho các ký tự như bảng 3.

Bảng 3. Ký tự ứng với điểm trên đường cong xét từ điểm P

∞ *	(17, 2) A	(6, 18) B	(10, 8) C
(13, 21) D	(18, 12) E	(28, 36) F	(4, 18) G
(0, 34) H	(27, 19) I	(34, 32) J	(16, 15) K
(25, 28) L	(31, 8) M	(36, 11) N	(12, 14) O
(33, 29) P	(3, 17) Q	(24, 24) R	(24, 13) S
(3, 20) T	(33, 8) U	(12, 23) V	(36, 26) W
(31, 29) X	(25, 9) Y	(16, 22) Z	(34, 5) dấu cách
(27, 18) .	(0, 3) ,	(4, 19) ?	(28, 1) !
(18, 25) $	(13, 16) %	(10, 29) &	(6, 19) (
(17, 35))			

Bước 3: Chọn khóa ngẫu nhiên là K = 5

Bước 4: Hàm mã hóa

- Rõ điểm: Theo bảng 2 ta có được các ký tự bản rõ tương ứng với số điểm cho kết quả ở bảng 3.

Bảng 3. Ký tự ứng với điểm trên đường cong

S	E	C	U	R	I	T	Y
(24, 13)	(18, 12)	(10, 8)	(33, 8)	(24, 24)	(27, 19)	(3, 20)	(25, 9)

- Áp dụng: $\mathcal{C} = \mathcal{E}(\mathcal{P}) = [(\mathcal{P}_i + \mathcal{K}) \bmod (n)]P$

Xét ký tự 'S': Ta được $\mathcal{P}_i$ của 'S' là 19P ứng với điểm (24, 13)

Ta có $\mathcal{C} = [(19+5) \bmod 37]P = 24P = 24(17, 2) = (31, 29)$, điểm này tương ứng với ký tự 'X'.

Ta có $\mathcal{C} = [(5+5) \bmod 37]P = 10P = 10(17, 2) = (34, 32)$, điểm này tương ứng với ký tự 'J'. Tương tự dùng hàm mã hóa ta xác định được các ký tự mã hóa còn lại.

Tương tự các ký tự còn lại ta được kết quả như bảng 4.

Bảng 4. Bảng các ký tự sau khi mã hóa

Ký tự	Rõ điểm	Mã điểm	Bản mã
S	(24, 13)	(31, 29)	X
E	(18, 12)	(34, 32)	J
C	(10, 8)	(0, 34)	H
U	(33, 8)	(16, 22)	Z
R	(24, 24)	(36, 26)	W
I	(27, 19)	(36, 11)	N
T	(3, 20)	(25, 9)	Y
Y	(25, 9)	(4, 19)	?

Ta được chuỗi mã hóa là: "XJHZWNY?"

Bản mã này được gửi trên kênh truyền cho bên B.

Giải mã:

Khi bên B nhận được bản mã và tiến hành giải mã như sau:

Bước 6: Hàm giải mã

- Khóa để giải mã $\mathcal{K} = 5$
- Áp dụng $\mathcal{P} = \mathcal{D}(\mathcal{C}) = [(\mathcal{C}_i - \mathcal{K}) \bmod (n)]P$

Xét điểm (31, 29) có vị trí 24P trên đường cong, ta có:

P = [(24 - 5) mod 37]P = 19P= 19(17, 2) = (36, 26) ứng với ký tự 'S'

Tương tự xét điểm (34, 32) có vị trí 10P trên đường cong, ta có:

P = [(10 - 5) mod 37]P = 5P = 5(17, 2) = (18, 12) ứng với ký tự 'E'.

Tương tự với các điểm còn lại ta được kết quả giải mã như bảng 5:

Bảng 5. Bảng kết quả giải mã

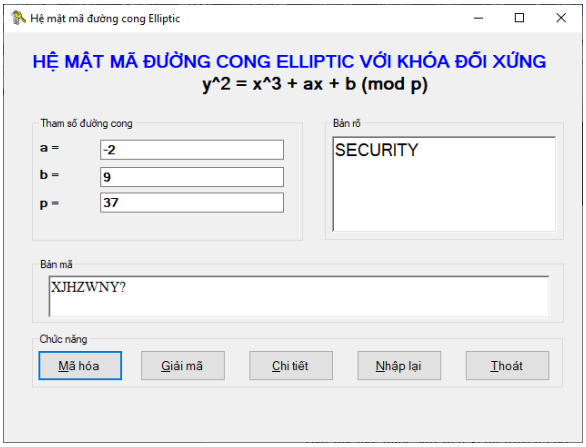
Bản mã	Mã điểm	Rõ điểm	Ký tự
X	(31, 29)	(24, 13)	S
J	(34, 32)	(18, 12)	E
H	(0, 34)	(10, 8)	C
Z	(16, 22)	(33, 8)	U
W	(36, 26)	(24, 24)	R
N	(36, 11)	(27, 19)	I
Y	(25, 9)	(3, 20)	T
?	(4, 19)	(25, 9)	Y

Vậy ta được bản rõ ban đầu là: SECURITY.

5. CÀI ĐẶT CHƯƠNG TRÌNH

Thuật toán được cài đặt trên thiết bị với cấu hình phần cứng là: CPU Intel(R) Core(TM) i5, 2.5 GHz; RAM: 4 GB; HDD: 500 GB; Và phần mềm với Hệ điều hành Windows 10, môi trường lập trình Visual studio .NET-2019.

Chương trình thực hiện cài đặt thuật toán mã hóa và giải mã trên đường cong Elliptic dùng ngôn ngữ lập trình C# của Visual studio .NET -2019 với giao diện như hình 3. Chương trình chạy cho kết quả đúng đắn với thuật toán đã trình bày ở trên.



Hình 3. Giao diện chương trình

6. KẾT LUẬN

Trong thuật toán mã hóa được đề xuất cải tiến ở đây, các bên giao tiếp đồng ý sử dụng đường cong Elliptic và điểm sinh P trên đường cong này. Tính bảo mật của mật mã đường cong Elliptic phụ thuộc vào độ khó của việc tìm giá trị của k, với kP trong đó k là một số lớn ngẫu nhiên và P là một điểm sinh ngẫu nhiên trên đường cong Elliptic. Đây là vấn đề logarit rời rạc đường cong Elliptic. Độ bảo mật còn phụ thuộc m, m là số chữ số của một nhóm số và m dài hay ngắn phụ thuộc tổng số điểm (n) trên đường cong Elliptic mà n lại phụ thuộc tham số của đường cong. Các tham số đường cong Elliptic cho các sơ đồ mã hóa nên được lựa chọn cẩn thận để chống lại tất cả các cuộc tấn công đã biết của bài toán logarit rời rạc đường cong Elliptic (ECDLP). Do đó, phương pháp mã hóa được đề xuất cải tiến ở đây cung cấp bảo mật đầy đủ chống lại việc phá mã, chi phí tính toán tương đối thấp. Ngoài ra, nó là ánh xạ ký tự dạng 1 → 1 giữa bản rõ và bản mã khi gửi bản mã trên đường truyền sẽ

không tốn băng thông so với các thuật toán trước. Thuật toán được cài đặt và thử nghiệm trên ngôn ngữ lập trình C# cho kết quả đúng đắn theo thuật toán đề xuất.

TÀI LIỆU THAM KHẢO

[1] Darrel Hankerson, Alfered Menezes, Scott Vanstone*, "A Gide to elliptic curve Cryptography"*, Springer, 2004.

[2] V. Miller, *"Uses of Elliptic curves in Cryptography. In advances in Cryptography"* (CRYPTO 1985), Springer LNCS 218,417-4 26, 1985.

[3] S. Sugantha Priya, Dr. M. Mohanraj, "*A Review on Secure Elliptic Curve Cryptography (ECC) and Dynamic Secure Routing Link Path Detection Algorithm" (DSRLP) Under Jamming Attack*, ISSN: 0474-9030, Vol-68-Issue-30, February, 2020.

[4] Utku Gulen, Selcuk Baktir*, "Elliptic Curve Cryptography for Wireless Sensor Networks Using the Number Theoretic Transform"*, journal-sensors, Published: 9 March, 2020.

[5] Negin Dinarvand, Hamid Barati, "*An efficient and secure RFID authentication protocol using elliptic curve cryptography"*, Springer Science, LLC, 2017.

[6] F. Amounas and E.H. El Kinani, "*ECC Encryption and Decryption with a Data Sequence"*, Applied Mathematical Sciences, Vol. 6, no. 101, 5039 – 5047, 2012.

[7] Mai Mạnh Trừng, Lê Thị Thu Hiền, Trần Minh Đức, *"Đề xuất hệ mật đường cong Elliptic với khóa đối xứng",* Tạp chí Khoa học Công nghệ, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp, 2020.

[8] Mai Mạnh Trừng, Đỗ Trung Tuấn, Lê Phê Đô, Lê Trung Thực, Đào Thị Phương Anh, "*Xây dựng hệ mật mã đường cong Elliptic với khóa đối xứng Affine để mã hóa giải mã văn bản tiếng Việt*", Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), 724-732, Nha Trang, ngày 8-9/10/2020.

[9] Alfred J. Menezes and Scott A. Vanstone, *"Elliptic Curve Cryptosystems and their implementations"*, Journal of Cryptology, Volume-6, Number-4, pages 209-224, 1993.

[10] Enge A, "*Elliptic curves and their applications to cryptography"*, Norwell, MA: Kulwer Academic publishers, 1999.

[11] S. Sandeep, Kumar, *"Elliptic curve cryptography for constrained devices*", PhD thesis, Ruhr-University Bochum, June, 2006.

Thông tin liên hệ: **Mai Mạnh Trừng**

Điện thoại: 0912355022 - Email: mmtrung@uneti.edu.vn

Khoa Công nghệ thông tin, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp.