ĐỀ XUẤT HỆ MẬT ĐƯỜNG CONG ELLIPTIC VỚI KHÓA ĐỐI XỨNG

PROPOSE ELLIPTIC CURVE CRYPTOSYSTEMS WITH THE SYMMETRIC KEY

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

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

Đến Tòa soạn ngày 10/03/2020, chấp nhận đăng ngày 05/06/2020

Tóm tắt: Bài báo mô tả ý tưởng cơ bản về mật mã đường cong Elliptic (ECC). Số học đường cong Elliptic có thể được sử dụng để phát triển một loạt các sơ đồ mã hóa đường cong Elliptic bao gồm trao đổi khóa, mã hóa và chữ ký số. Điểm thu hút chính của mật mã đường cong Elliptic so với RSA là nó cung cấp bảo mật tương đương cho kích thước khóa nhỏ hơn, do đó giảm chi phí xử lý. Chúng tôi đề xuất một thuật toán mã hóa bằng cách sử dụng đường cong Elliptic trên các trường hữu hạn với khóa đối xứng.

Từ khóa: Đường cong Elliptic, mã hóa, giải mã, khóa đối xứng.

Abstract: The article describes the basic idea of Elliptic curve cryptography (ECC). Elliptic curve arithmetic can be used to develop a variety of Elliptic curve cryptographic schemes including key exchange, encryption, and digital signature. The principal attraction of Elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size, thereby reducing the processing overhead. We propose a new encryption algorithm using the Elliptic curve over finite fields with the symmetric key.

Keywords: Elliptic curve, encryption, decryption, symmetric key.

1. GIỚI THIỆU

Các hệ thống mật mã đường cong Elliptic (ECC) được phát minh bởi Neal Koblitz [1] và Victor Miller [2] vào năm 1985. Chúng có thể được xem như các đường cong Elliptic của các hệ thống 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).

Hệ mật đường cong Elliptic được ứng dụng trong phát hiện đường dẫn liên kết định tuyến an toàn động [3], trong công nghệ nhận dạng đối tượng bằng sóng vô tuyến hiệu quả và an toàn [4], trong các mạng cảm biến không dây sử dụng phép biến đổi lý thuyết số [5]. Trong bài báo [6], các tác giả đã trình bày việc triển khai ECC bằng cách trước tiên là chuyển đổi thông điệp thành một điểm affine trên đường cong Elliptic, sau đó áp dụng thuật toán đọc chuỗi trên bản rõ. Với chúng tôi, trong công việc mã hóa và giải mã, đầu vào là bản rõ văn bản, mỗi ký tự được xác định là một điểm trên đường cong Elliptic. Sử dụng khóa đối xứng là một giá trị ngẫu nhiên để mã hóa. Đầu ra là một bản mã gồm dãy số của các điểm trên đường cong Elliptic. 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:

$$y^2 = x^3 - 3x + 7 \pmod{31} \qquad (*)$$

2. ĐƯỜNG CONG ELLIPTIC

Đường cong Elliptic E trên trường hữu hạn

$GF(p)$ trong đó p là số nguyên tố, là tập hợp các điểm (x, y) thỏa mãn phương trình sau:

$E: y^2 = x^3 + ax + b$ (1)

Trong đó a, b là số nguyên modul p, thỏa mãn:

$4a^3 + 27b^2 \neq 0$

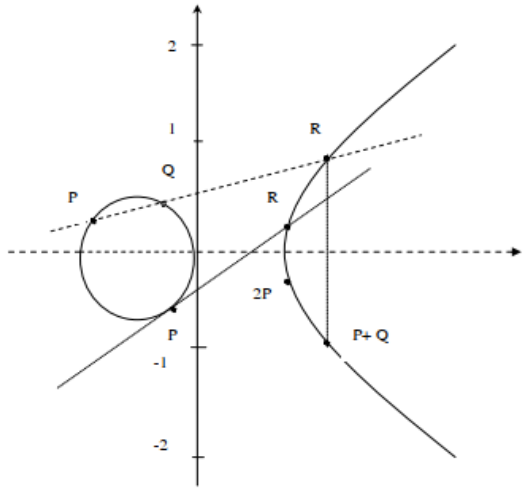
và bao gồm một điểm O gọi là điểm vô cực. Với phương trình (*) thì

$a = -3, b = 7$

ta có

$4*(-3)^3 + 27*(7)^2 = 1215 \neq 0.$

Do vậy, phương trình (*) 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. Do vậy, tổng số điểm là số nguyên tố thì tất cả các điểm trên đường cong đều là điểm sinh. Ngoài ra, với số điểm này đủ để chứa các ký tự trên bảng chữ cái tiếng Anh.



Hình 1. Tổng hai điểm của đường cong Elliptic

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 $P + Q = O$. Ngược lại thì $P + Q = (x_3, y_3) \in E$, trong đó $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, với:

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

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

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

Nếu $P = Q$, tức là $x_1 = x_2$, ta có:

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

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 + O = O + P = P.

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.

3. THUẬT TOÁN ĐỀ XUẤT

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

$\mathcal{P}$: là bản rõ;

$\mathcal{C}$: là bản mã;

$\mathcal{E}$: là hàm mã hóa;

$\mathcal{D}$: là hàm giải mã;

$\mathcal{K}$: là khóa.

Bước 1: Xác định tổng số điểm của đường cong Elliptic, tìm điểm sinh của đường cong Elliptic.

Bước 2: Chuyển đổi tổng số điểm (n) sang hệ đếm cơ số 2. Tìm được m là số chữ số của chuỗi số vừa đổi. Ví dụ $n = 86$ ta được dãy số 1010110. Ta có $m = 7$.

Bước 3: Lập ma trận M với kích thước $(n + 1)*m$. Trong đó $n + 1$ là số hàng, n là tổng số điểm của đường cong E, m là số cột (m số chữ của một hàng). Ta có ma trận

$$M = \begin{pmatrix} a_{0,0}a_{0,1}\dots\dots a_{0,m} \\ a_{1,0}a_{1,1}\dots\dots a_{1,m} \\ \dots\dots \\ a_{n,0}a_{n,1}\dots\dots a_{n,m} \end{pmatrix}$$

Với $n = 86$ ta có kích thước của ma trận M là 87×7.

$$M = \begin{pmatrix} 0000000 \\ 0000001 \\ 0000010 \\ 0000011 \\ \dots\dots \\ 1010110 \end{pmatrix}$$

Mã hóa:

Bước 4: Chọn giá trị khóa $\mathcal{K}$ ngẫu nhiên.

Bước 5: Hàm mã hóa

$$\mathcal{C} = \mathcal{E}(\mathcal{P}) = \mathcal{C} = \mathcal{E}(\mathcal{P}) = [(\mathcal{P}_i + \mathcal{K}) \bmod (n)]P \quad (4)$$

Bước 6: Đọc chuỗi số nhị phân của tọa độ điểm mã hóa theo bước 3.

Giải mã:

Bước 7: Xét đoạn gồm m chữ số của chuỗi số mã hóa, chuyển đổi dãy số nhị phân nhận được sang thập phân tìm được tọa độ điểm.

Bước 8: Hàm giải mã

$$\mathcal{P} = \mathcal{D}(\mathcal{C}) = [(\mathcal{C}_i - \mathcal{K}) \bmod (n)]P \quad (5)$$

Trong đó tham số ở (4), (5), trong đó:

$\mathcal{P}_i$: 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;

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): COMPUTER. 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: Xác định tổng số điểm của đường cong Elliptic, tìm điểm sinh của đường cong Elliptic.

Với đường cong E ở (*) ta có 37 điểm trên đường cong tính cả điểm vô cực. Ta tìm được điểm sinh P = (18; 9). Sử dụng công thức (2) và công thức (3) điểm tính các điểm trên đường cong.

Bảng 1. Tập hợp tất cả các điểm trên ECC

(18; 9)	(4; 11)	(28; 19)	(17; 23)
(6; 9)	(7; 22)	(22; 7)	(30; 28)
(15; 19)	(16; 5)	(1; 25)	(19; 12)
(3; 5)	(12; 5)	(29; 25)	(2; 3)
(0; 21)	(10; 27)	(10; 4)	(0; 10)
(2; 28)	(29; 6)	(12; 26)	(3; 26)
(19; 19)	(1; 6)	(16; 26)	(15; 12)
(30; 3)	(22; 24)	(7; 9)	(6; 22)
(17; 8)	(28; 12)	(4; 20)	(18; 22)
O			

Bước 2: Chuyển đổi tổng số điểm (n) sang hệ đếm cơ số 2. Tìm được m là số chữ số của

chuỗi số vừa chuyển đổi.

Xác định đươc tổng số của đường cong là 37 điểm, tức là n = 37. Chuyển sang nhị phân ta được dãy số 100101. Ta có m = 6.

Bước 3: Lập ma trận m có kích thước 38 × 6

$$M = \begin{pmatrix} 000000 \\ 000001 \\ 000010 \\ 000011 \\ \cdots\cdots \\ 100101 \end{pmatrix}$$

Mã hóa:

Bước 4: Chọn khóa ngẫu nhiên là $\mathcal{K}$ = 3;

Bước 5, 6: Hàm mã hóa, đọc chuỗi số.

Bảng 2. Ký tự ứng với điểm trên đường cong xét từ điểm P

(18; 9) A	(4; 11) B	(28; 19) C	(17; 23) D
(6; 9) E	(7; 22) F	(22; 7) G	(30; 28) H
(15; 19) I	(16; 5) J	(1; 25) K	(19; 12) L
(3; 5) M	(12; 5) N	(29; 25) O	(2; 3) P
(0; 21) Q	(10; 27) R	(10; 4) S	(0; 10) T
(2, 28) U	(29; 6) V	(12; 26) W	(3; 26) X
(19; 19) Y	(1; 6) Z	(16; 26) dấu cách	(15; 12) .
(30; 3) ?	(22; 24) !	(7; 9) :	(6; 22) [
(17; 8)]	(28; 12) “	(4; 20) ‘	(18; 22) ,
O			

- 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

C	O	M	P	U	T	E	R
(28, 19)	(29, 25)	(3, 5)	(2, 3)	(2, 28)	(0, 10)	(6, 9)	(10, 27)

- Áp dụng: $\mathcal{C} = \mathcal{E}(\mathcal{P}) = [(\mathcal{P}_i + \mathcal{K}) \bmod (n)]P$
- Xét ký tự ‘C’: Ta được $\mathcal{P}_i$ của ‘C’ là 3P ứng với điểm (28, 19)

Ta có $\mathcal{C}$ = [(3+3) mod 37]P = 6P = 6(18; 9) = (7; 22). Với x = 7 và y = 22 đọc chuỗi số ở ma trận M ở bước 3. Ta có: 000111, 010110.

Tương tự xét ký tự ‘O’: Ta được $\mathcal{P}_i$ của ‘O’ là 15P ứng với điểm (29, 25).

Ta có $\mathcal{C}$ = [(15+3) mod 37]P =18P = 18(18; 9) = (10, 27). Với x = 10 và y = 27 đọc chuỗi số ở ma trận M ở bước 3. Ta có: 001010, 011011.

Tương tự các ký tự còn lại ta được:

Bảng 4. Bảng các ký từ sau khi mã hóa

Ký tự	Rõ điểm	Mã điểm	Chuỗi số mã hóa
C	(28; 19)	(7; 22)	000111 010110
O	(29; 25)	(10; 27)	001010 011011
M	(3; 5)	(2; 3)	000010 000011
P	(2; 3)	(10; 4)	001010 000100
U	(2; 28)	(3; 26)	000011 011010
T	(0; 10)	(12; 26)	001100 011010
E	(6; 9)	(30; 28)	011110 011100
R	(10; 27)	(2; 28)	000010 011100

Vậy bản mã sau khi mã hóa là: 000111 010110 001010 011011 000010 000011 001010 000100 000011 011010 001100 011010 011110 011100 000010 011100.

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

Giải mã:

Bước 7: Chuyển sang thập phân

Với m = 6, ta xét chuỗi : $000111_{(2)} = 0\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 1\times2^1 + 1\times2^0 = 7$

Tương tự, $010110_{(2)}$ = 22 do vậy, ta được điểm (7; 22).

Ta tính toán với chuỗi số còn lại ta xác định được (10 ; 27); (2 ; 3); (10 ; 4); (3 ; 26); (12 ; 26); (30, 28); (2 ; 28).

Bước 8: Hàm giải mã

- Khóa để giải mã $\mathcal{K}$ = 3;
- Áp dụng $\mathcal{P} = \mathcal{D}(\mathcal{C}) = [(\mathcal{C}_i - \mathcal{K}) \bmod (n)]P$.

Xét điểm (7; 22) có vị trí 6P trên đường cong, ta có:

$\mathcal{P}$ = [(6–3) mod 37]P = 3P= 3(18, 9) = (28; 19) ứng với ký tự 'C'

Tương tự xét điểm (10; 27) có vị trí 18P trên đường cong, ta có

$\mathcal{P}$ = [(18–3) mod 37]P = 15P = 15(18, 9) = (29; 25) ứng với ký tự 'O'.

Tương tự với các điểm còn lại ta được:

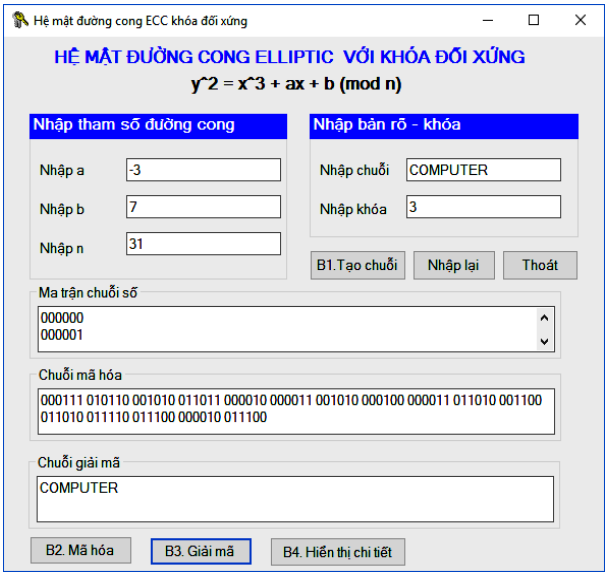
Bảng 5. Bảng kết quả giải mã

Chuỗi số mã hóa	Mã điểm	Rõ điểm	Ký tự
000111 010110	(7, 22)	(28, 19)	C
001010 011011	(10, 27)	(29, 25)	O
000010 000011	(2, 3)	(3, 5)	M
001010 000100	(10, 4)	(2, 3)	P
000011 011010	(3, 26)	(2, 28)	U
001100 011010	(12, 26)	(0, 10)	T
011110 011100	(30, 28)	(6, 9)	E
000010 011100	(2, 28)	(10, 27)	R

Vậy ta được bản rõ ban đầu là: COMPUTER.

5. CÀI ĐẶT CHƯƠNG TRÌNH

Phần cứng: CPU Intel(R) Core(TM) i5, 2.5 GHZ; RAM: 4 GB; HDD: 500 GB; Phần mềm: Hệ điều hành Windows 10, phần mềm lập trình Visual studio .NET – 2017.



Hình 2. Giao diện chương trình

Chương trình được cài đặt với ngôn ngữ lập trình C# như giao diện ở hình 2. Kết quả chạy đúng với thuật toán trình bày ở trên.

6. KẾT LUẬN

Trong thuật toán mã hóa được đề xuất 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 *k*P 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 ở đây cung cấp bảo mật đầy đủ chống lại việc phá mã chi phí tính toán tương đối thấp. 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] N. Koblitz, "*Elliptic curve cryptosystems, Mathematics of Computation"*, 203 – 209, 1987.

[2] V. Miller, *"Uses of elliptic curves in cryptography, Advances in Cryptology – Crypto"*, Lecture Notes in Computer Science, SpringerVerlag, 417 -426, 1986.

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

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

[6] D. Sravana Kumar, CH. Suneetha, A. ChandrasekhAR, *"Encryption of Data Using Elliptic Curve Over Finite Fields"*, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January. 2012.

Thông tin liên hệ: **Mai Mạnh Trừng**

Điện thoại: 0912.355.022 - Email: mmtrung@uneti.edu.vn

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