Về việc đếm điểm của đường cong elliptic dạng Edwards cuộn định nghĩa trên trường hữu hạn

Phó Đức Tài, Võ Tùng Linh

***Tóm tắt*— Trong bài báo này, nhóm tác giả nghiên cứu việc đếm điểm của đường cong Edwards cuộn định nghĩa trên trường hữu hạn. Cụ thể, nhóm tác giả xây dựng các công thức tường minh cho phép xác định chính xác số điểm k-hữu tỉ của một đường cong Edwards cuộn khi biết số điểm k-hữu tỉ của đường cong tương đương song hữu tỉ dạng Weierstrass hoặc Montgomery tương ứng. Từ đó, nhóm tác giả đưa ra thuật toán để đếm số điểm của đường cong Edwards cuộn trên trường hữu hạn.**

***Abstract*— In this paper, we are interested in counting points on a twisted Edwards curve defined over a finite field. In particular, we construct explicit formulae allowing to determine exactly the number of k-rational points on a twisted Edwards curve when the number of k-rational points on the birational equivalent curve of Weierstrass or Montgomery form respectively is known. Using these formulae, we introduce an algorithm to count points on the twisted Edwards curve define over a finite field.**

***Keywords*— counting points; twisted Edwards curve; Montgomery curve; Weierstrass curve; elliptic curve.**

***Từ khoá*— đường cong Edwards cuộn; đường cong Montgomery; đường cong Weierstrass; đường cong elliptic; đếm điểm.**

I. GIỚI THIỆU

Các đường cong elliptic dạng chuẩn Edwards lần đầu được Harold Edwards đưa ra trong [8], sau đó được nhóm tác giả Daniel J Bernstein, Peter Birker cùng các cộng sự tổng quát hoá trong [3]. Theo đó, ta có với k là một trường hữu hạn với đặc số nguyên tố $p \neq 2$, đường cong elliptic cho bởi phương trình:

$$E_{Ed} : ax^2 + y^2 = 1 + dx^2y^2 \qquad (1)$$

với $a, d \in k$ thoả mãn $ad(a - d) \neq 0$ được gọi là *đường cong Edwards cuộn (twisted Edwards curve)* định nghĩa trên trường k. Không giống như các đường cong elliptic dạng Weierstrass, trên đường cong Edwards cuộn người ta có thể xây dựng phép cộng và phép nhân đôi điểm với cùng một công thức duy nhất. Điều này mang lại cho các đường cong Edwards cuộn hiệu quả cao hơn về mặt tính toán cũng như khả năng kháng lại các tấn công kênh kề tốt hơn khi so với những dạng đường cong elliptic khác [4–6, 9]. Do đó, việc xây dựng các giao thức, lược đồ mật mã sử dụng các đường cong dạng chuẩn Edwards đang ngày càng trở nên phổ biến, tiêu biểu có thể kể đến như lược đồ chữ ký số EdDSA [5, 10] - lược đồ chữ ký số tất định hiện đã được công nhận là một trong những chuẩn chữ ký số của NIST [1]. Xu hướng sử dụng rộng rãi các đường cong dạng chuẩn Edwards trong các ứng dụng mật mã đã làm nảy sinh yêu cầu cần xây dựng các đường cong dạng này thoả mãn các tiêu chuẩn an toàn để sử dụng trong thực tế.

Để có thể sử dụng trong các cài đặt thực tế, các hệ mật mã đường cong elliptic cần được xây dựng trên những đường cong có số điểm lớn và thoả mãn các tiêu chuẩn an toàn đặt ra. Do đó, với các đường cong được sinh, ta cần đếm số điểm của đường cong đó trên trường xác định, sau đó kiểm tra các tiêu chuẩn an toàn tương ứng. Việc đếm số điểm của một đường cong elliptic trên trường hữu hạn luôn là một bài toán phức tạp và tốn nhiều chi phí tính toán. May mắn thay, những kết quả nghiên cứu tuyệt vời của các nhà toán học và mật mã, bắt đầu từ René Schoof [13], sau đó là Noam Elkies và A. O. L. Atkin đã cung cấp cho chúng ta một thuật toán hiệu quả để đếm số điểm đường cong elliptic trên trường hữu hạn với kích thước lên đến hàng trăm bit, gọi là *Thuật toán Schoof-Elkies-Atkin*,

Bài báo được nhận ngày 02/5/2022. Bài báo được nhận xét bởi phản biện thứ nhất ngày 11/5/2022 và được chấp nhận đăng ngày 18/5/2022. Bài báo được nhận xét bởi phản biện thứ hai ngày 16/5/2022 và được chấp nhận đăng ngày 26/5/2022.

hay một cách ngắn gọn, *Thuật toán SEA* [7, 14].

Những mô tả rõ ràng của Thuật toán SEA hiện nay chỉ áp dụng cho các đường cong elliptic dạng chuẩn Weierstrass mà chưa có các phiên bản tương ứng cho các đường cong dạng Edwards cuộn. Vậy nên, để có thể đếm điểm của các dạng đường cong elliptic không phải Weierstrass, ta cần "đi đường vòng" mới có thể thực hiện được. Phương pháp "đi đường vòng" ở đây là từ đường cong dạng chuẩn Edwards (1), ta sẽ biến đổi chúng về dạng chuẩn Weierstrass, sau đó sử dụng Thuật toán SEA để đếm số điểm của đường cong đó, rồi từ kết quả nhận được để tính ra số điểm của đường cong ban đầu. Tuy nhiên, hầu hết các phép biến đổi qua lại giữa các dạng đường cong elliptic chỉ là các phép biến đổi song hữu tỉ, do vậy không bảo toàn số điểm của đường cong đó. Một cách cụ thể, giả sử E_{Ed} là một đường cong dạng chuẩn Edwards định nghĩa trên trường hữu hạn k được biến đổi về đường cong dạng chuẩn Weierstrass E_W tương ứng. Do k là một trường hữu hạn nên tập các điểm k-hữu tỉ của E_{Ed} và E_W, ký hiệu lần lượt là $E_{Ed}(k)$ và $E_W(k)$, đều là các tập có lực lượng hữu hạn. Do đó, ta hoàn toàn có thể viết được

$$\#E_{Ed}(k) = \#E_W(k) + \alpha$$

với α là một số nguyên nào đó. Bài toán đặt ra ở đây là cần xác định chính xác giá trị α này.

Cho đến nay, một số đường cong dạng chuẩn Edwards cuộn an toàn đã được xây dựng và đề xuất đưa vào sử dụng, chẳng hạn như đường cong Edwards Ed25519 hoặc Ed448 [11]. Hoặc như trong công trình [2], các tác giả cũng đã xây dựng thuật toán để sinh các đường cong Edwards có số điểm đủ lớn để sử dụng trong các ứng dụng mật mã. Để nhận được các đường cong này, phương pháp cơ bản vẫn là biến đổi song hữu tỉ từ các đường cong dạng Weierstrass hoặc Montgomery tương ứng. Tuy nhiên, hiện tại chưa thấy tài liệu nào đưa ra một cách tường minh về công thức liên hệ giữa số điểm k-hữu tỉ của đường cong Edwards cuộn và những dạng đường cong tương đương song hữu tỉ khác. Mục tiêu của bài báo này chính là thiết lập công thức liên hệ giữa số điểm k-hữu tỉ của đường cong Edwards cuộn với các đường cong dạng Montgomery và Weierstrass tương ứng, từ đó có thể mô tả thuật toán "đường vòng" để đếm số điểm một đường cong Edwards cuộn.

Đóng góp chính của bài báo: Trong bài báo này, qua các Định lý 4, Mệnh đề 5 và Hệ quả 6 sẽ chỉ ra công thức liên hệ giữa số điểm k-hữu tỉ của một đường cong Edwards cuộn với các đường cong tương đương song hữu tỉ dạng Montgomery và Weierstrass của nó. Từ đó, nhóm tác giả xây dựng thuật toán đơn giản để đếm số điểm của đường cong Edwards cuộn định nghĩa trên một trường hữu hạn. Đồng thời với Mệnh đề 7, nhóm tác giả đánh giá tỉ lệ phân bố của đường cong được sinh khi các hệ số được chọn ngẫu nhiên đều.

Bố cục của bài báo: Phần II trình bày việc biến đổi tương đương song hữu tỉ từ một đường cong Edwards cuộn E_{Ed} về đường cong Montgomery E_M. Sau đó là một trong những kết quả chính - Định lý 4 đưa ra công thức liên hệ giữa $\#E_{Ed}(k)$ và $\#E_M(k)$. Phần III tập trung vào quan hệ giữa đường cong Montgomery E_M và đường cong Weierstrass E_W tương ứng cũng như công thức liên hệ giữa số điểm của chúng. Phần IV trình bày việc biến đổi song hữu tỉ trực tiếp từ đường cong Edwards cuộn sang đường cong Weierstrass. Từ đó chỉ ra công thức tính số điểm của E_{Ed} từ số điểm của E_M. Cũng trong phần này, nhóm tác giả mô tả một thuật toán để đếm số điểm của đường cong Edwards cuộn trên trường hữu hạn. Phần Kết luận tổng kết những kết quả đạt được và đề cập đến một số hướng nghiên cứu tiếp theo gắn với đường cong Edwards cuộn và việc đếm điểm của nó.

Các ký hiệu: Xuyên suốt trong bài báo này, k được sử dụng để ký hiệu trường có đặc số khác 2 (có thể khác cả 3); p ký hiệu cho đặc số nguyên tố của trường k; E_{Ed}, E_M, E_W lần lượt ký hiệu các đường cong Edwards cuộn, Motgomery và dạng chuẩn Weierstrass; Các chữ cái Hy Lạp $\phi, \psi, \varphi, \Phi, \Gamma, \Psi$ ký hiệu cho các phép biến đổi giữa các đường cong; Bên cạnh đó, các ký hiệu còn lại trong bài sẽ được định nghĩa trước khi sử dụng.

II. Đường cong Edwards cuộn và đường cong Montgomery

Trước hết, để thuận tiện cho việc trình bày, dưới đây nhóm tác giả nhắc lại một số định nghĩa được sử dụng trong bài báo này.

Định nghĩa 1 ([3, Định nghĩa 2.1])**.** Cho k là một trường với đặc số khác 2 và các phần tử $a, d \in k$ thoả mãn $ad(a-d) \neq 0$. Một *đường*

cong Edwards cuộn với các hệ số a, d là đường cong được cho bởi phương trình

$$E_{Ed} : ax^2 + y^2 = 1 + dx^2y^2.$$

Một *đường cong Edwards* là một đường cong Edwards cuộn với $a = 1$.

Định nghĩa 2 ([3, Định nghĩa 3.1])**.** Cho k là một trường với đặc số khác 2 và các phần tử $A \in k\backslash\{-2, 2\}, B \in k\backslash\{0\}$. *Đường cong Montgomery* với các hệ số A và B là đường cong được cho bởi phương trình

$$E_M : Bv^2 = u^3 + Au^2 + u. \quad (2)$$

Trong các định nghĩa trên, k là một trường tuỳ ý với đặc số khác 2. Tuy nhiên, ngoại trừ một lớp đường cong elliptic đặc biệt định nghĩa trên các trường nhị phân, các hệ mật mã đường cong elliptic thường được xây dựng trên những đường cong định nghĩa trên các trường hữu hạn có đặc số p rất lớn. Do đó, trong phạm vi bài báo này, để đơn giản nhóm tác giả chỉ làm việc với các trường k *hữu hạn* có đặc số khác 2, 3.

Một khái niệm quan trọng nữa mà chúng ta cần đề cập đến, đó là khái niệm "*tương đương song hữu tỉ (birational equivalence)*" giữa các đường cong.

Định nghĩa 3 ([12])**.** Giả sử E và E' là hai đường cong định nghĩa trên một trường k. Ta nói rằng E và E' là *tương đương song hữu tỉ* nếu tồn tại các ánh xạ được cho bởi các phân thức (các ánh xạ hữu tỉ) $\varphi : E \to E'$ và $\varphi' : E' \to E$ sao cho $\varphi \circ \varphi'$ là ánh xạ đồng nhất trên E ngoại trừ tại một số hữu hạn điểm và $\varphi' \circ \varphi$ là ánh xạ đồng nhất trên E' ngoại trừ tại một số hữu hạn điểm.

Các ánh xạ φ, φ' được gọi là *các phép đổi biến song hữu tỉ* giữa E và E'.

Bây giờ, với đường cong Edwards cuộn E_{Ed} định nghĩa trên một trường hữu hạn k có đặc số khác 2 bởi phương trình (1), đặt

$$A = \frac{2(a+d)}{a-d}, \qquad B = \frac{4}{a-d}.$$

Khi đó, theo khẳng định (i) của Định lý 3.2 trong [3], đường cong E_{Ed} là tương đương song hữu tỉ với đường cong dạng Montgomery định nghĩa trên trường k bởi phương trình

$$E_M : Bv^2 = u^3 + Au^2 + u. \quad (3)$$

Phép đổi biến $E_{Ed} \to E_M$ được cho bởi

$$(x, y) \mapsto (u, v) = \left(\frac{1+y}{1-y}, \frac{1+y}{(1-y)x}\right). \quad (4)$$

Phép đổi biến ngược tương ứng $E_M \to E_{Ed}$ được cho bởi

$$(u, v) \mapsto (x, y) = \left(\frac{u}{v}, \frac{u-1}{u+1}\right). \quad (5)$$

Ký hiệu tập $E_{Ed}(k) = \{(x, y) \in k \times k : ax^2 + y^2 = 1 + dx^2y^2\}$, và $E_M(k) = \{(u, v) \in k \times k : Bv^2 = u^3 + Au^2 + u\} \cup \{\infty\}$ lần lượt là tập các điểm k-hữu tỉ trên đường cong E_{Ed}, E_M tương ứng, trong đó $E_M(k)$ bao gồm điểm trung hoà ∞, và $E_{M/k}(k) = \{(u, v) \in k \times k : Bv^2 = u^3 + Au^2 + u\}$ là tập chỉ gồm các điểm k-hữu tỉ của E_M. Lực lượng của các tập này được ký hiệu lần lượt là $\#E_{Ed}(k), \#E_M(k), \#E_{M/k}(k)$. Trong định lý dưới đây, nhóm tác giả sẽ chỉ ra mối quan hệ giữa $\#E_{Ed}(k)$ và $\#E_M(k), \#E_{M/k}(k)$.

Định lý 4. *Ta có*

$$\#E_{Ed}(k) = \begin{cases} \#E_M(k) - 2, \text{ nếu } \left(\frac{a}{p}\right) = -1, \\ \#E_M(k) - 4, \text{ nếu } \left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = 1, \\ \#E_M(k), \text{ nếu } \left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1. \end{cases}$$

Chứng minh: Định nghĩa ánh xạ

$$\phi : E_{Ed}(k) \to E_{M/k}(k)$$

cho bởi (4):

$$(x, y) \mapsto (u, v) = \left(\frac{1+y}{1-y}, \frac{1+y}{(1-y)x}\right).$$

Ta thấy ánh xạ này xác định tại mọi điểm trong $E_{Ed}(k)$ ngoại trừ những điểm có toạ độ (x, y) thoả mãn

$$x(1 - y) = 0.$$

Xét các trường hợp:

– Nếu $x = 0$, phương trình (1) trở thành

$$y^2 = 1,$$

điều này dẫn đến

$$y = \pm 1.$$

– Nếu $y = 1$, phương trình (1) trở thành

$$ax^2 = dx^2.$$

Do $a \neq d$ nếu suy ra phương trình chỉ có nghiệm $x = 0$.

Như vậy, với ánh xạ ϕ chỉ tồn tại 2 điểm ngoại lệ là

$$Q = (0, \pm 1).$$

Định nghĩa ánh xạ

$$\phi^{-1} : E_{M/k}(k) \to E_{Ed}(k)$$

cho bởi (5):

$$(u, v) \mapsto (x, y) = \left(\frac{u}{v}, \frac{u-1}{u+1}\right).$$

Ta thấy ánh xạ này xác định tại mọi điểm trong $E_{M/k}(k)$ ngoại trừ tại các điểm có toạ độ (u, v) thoả mãn

$$v(u + 1) = 0.$$

Xét các trường hợp:

- $v = 0$: Khi đó, phương trình (3) trở thành

$$0 = u^3 + Au^2 + u = u(u^2 + Au + 1).$$

  + Nếu $(A - 2)(A + 2) = \frac{4^2 ad}{(a-d)^2}$ là chính phương trong k, điều này tương đương với ad là chính phương trong k thì phương trình trên có các nghiệm $u = 0, \frac{-A \pm \sqrt{(A-2)(A+2)}}{2}$.
  + Ngược lại, nếu $(A - 2)(A + 2) = \frac{4^2 ad}{(a-d)^2}$ là không chính phương trong k, có nghĩa ad không là chính phương trong k thì phương trình trên chỉ có nghiệm $u = 0$.

- $u = -1$: Khi đó, phương trình (3) trở thành

$$Bv^2 = A - 2.$$

  + Nếu $\frac{A-2}{B} = d$ là chính phương trong k, thì phương trình trên có các nghiệm $v = \pm\sqrt{(A - 2)/B}$.
  + Ngược lại, nếu $\frac{A-2}{B} = d$ không là chính phương trong k thì phương trình trên không có nghiệm.

Như vậy, ta có các điểm ngoại lệ cụ thể cho ánh xạ ϕ^{-1} như sau:

- Nếu $\left(\frac{ad}{p}\right) = -1$:
  + Nếu $\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p} =\right) = -1$: Chỉ có 1 điểm ngoại lệ là
$$P = (0, 0).$$
  + Nếu $\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = 1$: Các điểm ngoại lệ là
$$P = (0, 0), (-1, \pm\sqrt{(A - 2)/B}).$$
- Nếu $\left(\frac{ad}{p}\right) = 1$:
  + Nếu $\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = 1$: Các điểm ngoại lệ là
$$P = (0, 0), ((-A \pm \sqrt{(A - 2)(A + 2)})/2, 0),$$
$$(-1, \pm\sqrt{(A - 2)/B}).$$
  + Nếu $\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1$: Các điểm ngoại lệ là
$$P = (0, 0), (-1, \pm\sqrt{(A - 2)/B}).$$

Ký hiệu $\Im(\phi)$, $\Im(\phi^{-1})$ lần lượt là tập ảnh của các ánh xạ ϕ, ϕ^{-1} tương ứng; $\text{Except}(\phi)$, $\text{Except}(\phi^{-1})$ lần lượt là tập các điểm ngoại lệ của ϕ, ϕ^{-1} tương ứng. Ta sẽ chỉ ra

$$\Im(\phi) \cap \text{Except}(\phi^{-1}) = \emptyset$$

và

$$\Im(\phi^{-1}) \cap \text{Except}(\phi) = \emptyset.$$

Đầu tiên, cần phải chứng minh

$$\Im(\phi) \cap \text{Except}(\phi^{-1}) = \emptyset,$$

điều này tương đương với việc chỉ ra rằng với mỗi điểm $P = (u, v) \in \text{Except}(\phi^{-1})$, sẽ không tồn tại điểm $Q = (x, y) \in E_{Ed}(k)$ sao cho $\phi(Q) = P$. Thật vậy, ta xét các trường hợp cụ thể sau:

- Với $P = (0, 0)$: Giả sử tồn tại điểm $Q = (x, y) \in E_{Ed}(k)$ sao cho $\phi(Q) = (0, 0)$. Từ (4), ta có

$$\begin{cases} \frac{1+y}{1-y} &= 0 \\ \frac{1+y}{(1-y)x} &= 0 \end{cases}$$

  Hệ phương trình trên cùng với phương trình (1) cho ta kết quả $Q = (0, -1)$, điều này là không thể vì điểm $(0, -1) \in \text{Except}(\phi)$.

Do đó không tồn tại điểm $Q \in E_{Ed}(k)$ để $\phi(Q) = (0,0)$.

– Với $P = (-1, \pm\sqrt{(A-2)/B})$: Giả sử tồn tại điểm $Q = (x,y) \in E_{Ed}(k)$ sao cho $\phi(Q) = (0,0)$. Từ (4), ta có

$$\begin{cases} \frac{1+y}{1-y} &= -1 \\ \frac{1+y}{(1-y)x} &= \pm\sqrt{(A-2)/B} \end{cases}$$

Hệ phương trình trên vô nghiệm, suy ra không tồn tại điểm $Q \in E_{Ed}(k)$ thoả mãn $\phi(Q) = P$.

– Với $P = ((-A \pm \sqrt{(A-2)(A+2)})/2, 0)$: Giả sử tồn tại điểm $Q = (x,y) \in E_{Ed}(k)$ sao cho $\phi(Q) = (0,0)$. Từ (4), ta có

$$\begin{cases} \frac{1+y}{1-y} &= \frac{-A \pm \sqrt{(A-2)(A+2)}}{2} \\ \frac{1+y}{(1-y)x} &= 0 \end{cases}$$

Giải hệ phương trình trên cùng với (1) cho ta điểm $Q = (0,-1)$, điều này là vô lý vì điểm $(0,-1) \in \text{Except}(\phi)$. Do đó không tồn tại $Q \in E_{Ed}(k)$ sao cho $\phi(Q) = P$.

Tiếp theo, chứng minh

$$\Im(\phi^{-1}) \cap \text{Except}(\phi) = \emptyset.$$

Thật vậy, ta xét các trường hợp cụ thể sau:

– Với $Q_1 = (0,1)$: Giả sử tồn tại $P_1 = (u,v) \in E_{M/k}(k)$ sao cho $\phi^{-1}(P_1) = (0,1)$. Từ (5) ta có

$$\begin{cases} \frac{u}{v} &= 0 \\ \frac{u-1}{u+1} &= 1 \end{cases}$$

Hệ phương trình trên vô nghiệm, suy ra không tồn tại điểm $P_1 \in E_{M/k}(k)$ sao cho $\phi^{-1}(P_1) = Q_1$.

– Với $Q_1 = (0,-1)$: Giả sử tồn tại $P_1 = (u,v) \in E_{M/k}(k)$ sao cho $\phi^{-1}(P_1) = (0,-1)$. Từ (5) ta có

$$\begin{cases} \frac{u}{v} &= 0 \\ \frac{u-1}{u+1} &= -1 \end{cases}$$

Giải hệ phương trình trên cùng với phương trình đường cong (3) cho ta kết quả $P_1 = (0,0)$. Điều này là vô lý vì điểm $(0,0)$ là điểm ngoại lệ của ϕ^{-1}. Do vậy không tồn tại điểm $P_1 \in E_{M/k}(k)$ sao cho $\phi^{-1}(P_1) = (0,-1)$.

Bây giờ, chứng minh với mọi điểm $R = (x,y) \in E_{Ed}(k)$ và $R \notin \text{Except}(\phi)$, ta có

$$\phi^{-1}(\phi(R)) = R.$$

Thật vậy, do $R \notin \text{Except}(\phi)$ nên điểm $\phi(R)$ được xác định. Đặt $R' = (u,v) = \phi(R) \in \Im(\phi)$ và từ (4) ta có

$$R' = (u,v) = \left(\frac{1+y}{1-y}, \frac{1+y}{(1-y)x}\right).$$

Theo chứng minh ở trên, $\Im(\phi) \cap \text{Except}(\phi^{-1}) = \emptyset$, suy ra $\phi^{-1}(R')$ được xác định và thay toạ độ R' vào (5), ta có

$$\begin{aligned} \phi^{-1}(\phi(R)) &= \phi^{-1}(R') \\ &= \left(\frac{u}{v}, \frac{u-1}{u+1}\right) \\ &= \left(\frac{\frac{1+y}{1-y}}{\frac{1+y}{(1-y)x}}, \frac{\frac{1+y}{1-y}-1}{\frac{1+y}{1-y}+1}\right) \\ &= (x,y) \\ &= R. \end{aligned}$$

Một cách tương tự, dễ dàng chỉ ra được, với mọi điểm

$$S = (u,v) \in E_{M/k}(k) \text{ và } S \notin \text{Except}(\phi^{-1}),$$

ta có

$$\phi(\phi^{-1}(S)) = S.$$

Từ các chứng minh trên, ta suy ra tồn tại song ánh giữa các tập điểm $E_{Ed}(k) \setminus \text{Except}(\phi)$ và $E_{M/k}(k) \setminus \text{Except}(\phi^{-1})$. Từ đây nhận được hệ thức

$$\begin{aligned} \#E_{Ed}(k) &- \#\text{Except}(\phi) \\ &= \#E_{M/k}(k) - \#\text{Except}(\phi^{-1}). \end{aligned}$$

Kết hợp hệ thức này với khẳng định về số lượng các điểm ngoại lệ của ϕ, ϕ^{-1} tương ứng theo tính chính phương trong k của a và d, đồng thời từ khẳng định hiển nhiên

$$\#E_M(k) = \#E_{M/k}(k) + 1,$$

ta thu được công thức

$$\#E_{Ed}(k) = \begin{cases} \#E_M(k) - 2, \text{ nếu } \left(\frac{a}{p}\right) = -1, \\ \#E_M(k) - 4, \text{ nếu } \left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = 1, \\ \#E_M(k), \text{ nếu } \left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1. \end{cases}$$

Như vậy, ta có điều phải chứng minh. □

III. ĐƯỜNG CONG MONTGOMERY VÀ ĐƯỜNG CONG WEIERSTRASS

Giả sử ta có đường cong elliptic dạng Montgomery định nghĩa trên trường hữu hạn k có đặc số $p \neq 2, 3$ cho bởi phương trình (3) là $Bv^2 = u^3 + Au^2 + u$, với $A, B \in k$ thoả mãn $B(A^2 - 4) \neq 0$. Do $B \neq 0$ nên có thể thực hiện việc chia cả hai vế phương trình trên cho B^3 và nhận được:

$$\frac{v^2}{B^2} = \frac{u^3}{B^3} + \frac{A}{B}\frac{u^2}{B^2} + \frac{1}{B^2}\frac{u}{B}.$$

Đặt

$$X = \frac{u}{B}, s = \frac{v}{B},$$

phương trình trên trở thành:

$$s^2 = X^3 + \frac{A}{B}X^2 + \frac{1}{B^2}X.$$

Tiếp tục biến đổi phương trình trên, ta có:

$$\begin{aligned} s^2 &= X^3 + 3\frac{A}{3B}X^2 + 3\frac{A^2}{9B^2}X + \frac{A^3}{27B^3} \\ &\quad -3\frac{A^2}{9B^2}X + \frac{1}{B^2}X - \frac{A^3}{27B^3} \\ &= \left(X + \frac{A}{3B}\right)^3 + \frac{3 - A^2}{3B^2}X - \frac{A^3}{27B^3} \\ &= \left(X + \frac{A}{3B}\right)^3 + \frac{3 - A^2}{3B^2}\left(X + \frac{A}{3B}\right) \\ &\quad -\frac{3 - A^2}{3B^2}\frac{A}{3B} - \frac{A^3}{27B^3} \\ &= \left(X + \frac{A}{3B}\right)^3 + \frac{3 - A^2}{3B^2}\left(X + \frac{A}{3B}\right) \\ &\quad +\frac{2A^3 - 9A}{27B^3}. \end{aligned}$$

Đặt $t = X + \frac{A}{3B}, \varepsilon = \frac{3-A^2}{3B^2}$ và $\delta = \frac{2A^3-9A}{27B^3}$, ta nhận được phương trình đường cong có dạng chuẩn Weierstrass, ký hiệu E_W:

$$E_W : s^2 = t^3 + \varepsilon t + \delta. \tag{6}$$

Tổng hợp các phép biến đổi trên, từ đường cong dạng Montgomery

$$E_M : Bv^2 = u^3 + Au^2 + u$$

nhận được đường cong dạng chuẩn Weierstrass

$$E_W : s^2 = t^3 + \varepsilon t + \delta$$

qua phép đổi biến

$$(u, v) \mapsto (t, s) = \left(\frac{u}{B} + \frac{A}{3B}, \frac{v}{B}\right) \tag{7}$$

và các hệ số

$$\varepsilon = \frac{3 - A^2}{3B^2}, \qquad \delta = \frac{2A^3 - 9A}{27B^3}.$$

Phép đổi biến ngược để đưa E_W về E_M trong trường hợp này được cho bởi

$$(t, s) \mapsto (u, v) = \left(Bt - \frac{A}{3}, Bs\right). \tag{8}$$

Ký hiệu

$$E_W(k) = \{(t, s) \in k \times k : s^2 = t^3 + \varepsilon t + \delta\} \cup \{\infty\}$$

là tập các điểm k-hữu tỉ của đường cong E_W cùng với điểm tại vô cùng ∞, và ký hiệu

$$E_{W/k}(k) = \{(t, s) \in k \times k : s^2 = t^3 + \varepsilon t + \delta\}$$

là tập chỉ gồm các điểm k-hữu tỉ. Ta có khẳng định sau đây.

Mệnh đề 5. *Với các đường cong E_M, E_W được xác định như trên, ta có*

$$\#E_M(k) = \#E_W(k).$$

Chứng minh: Định nghĩa ánh xạ

$$: E_{M/k}(k) \to E_{W/k}(k)$$

cho bởi công thức (7):

$$(u, v) \mapsto (t, s) = \left(\frac{u}{B} + \frac{A}{3B}, \frac{v}{B}\right).$$

Không khó để chứng minh ánh xạ ψ là một song ánh với ánh xạ ngược

$$\psi^{-1} : E_{W/k}(k) \to E_{M/k}(k)$$

được cho bởi công thức (8):

$$(t, s) \mapsto (u, v) = \left(Bt - \frac{A}{3}, Bs\right).$$

Thật vậy, với một điểm $Q = (t, s) \in E_{W/k}(k)$ tuỳ ý, bằng cách tính toán trực tiếp, ta chỉ ra được

$$Q' = \psi^{-1}(Q) = (Bt - \frac{A}{3}, Bs) \in E_{M/k}(k).$$

Tiếp theo, từ định nghĩa của ψ, ta có

$$\psi(Q') = \left(\frac{Bt - A/3}{B} + \frac{A}{3B}, \frac{Bs}{B}\right) = (t, s) = Q.$$

Điều này có nghĩa là

$$\circ\, \psi^{-1}(Q) = Q, \forall Q \in E_{W/k}(k),$$

hay nói cách khác $\psi \circ \psi^{-1}$ là ánh xạ đồng nhất trên $E_{W/k}(k)$.

Tương tự, ta cũng chỉ ra được $\psi^{-1} \circ \psi$ là ánh xạ đồng nhất trên $E_{M/k}(k)$. Bên cạnh đó, việc chỉ ra tính đơn ánh của ψ, ψ^{-1} là tầm thường. Từ đó ta có ψ là song ánh, vậy nên

$$\#E_{M/k}(k) = \#E_{W/k}(k)$$

và điều này kéo theo

$$\#E_M(k) = \#E_W(k).$$

Ta có khẳng định cần chứng minh.

IV. Đường cong Edwards cuộn và đường cong Weierstrass

Giả sử ta có một đường cong elliptic dạng chuẩn Edwards định nghĩa trên trường k có đặc số nguyên tố $p \neq 2, 3$ bởi phương trình $E_{Ed} : ax^2 + y^2 = 1 + dx^2y^2$, trong đó $a, d \in k$ thoả mãn $ad(a - d) \neq 0$. Sử dụng phép đổi biến được cho bởi công thức (4)

$$(x, y) \mapsto (u, v) = \left(\frac{1 + y}{1 - y}, \frac{1 + y}{(1 - y)x}\right),$$

ta biến đổi E_{Ed} về một đường cong tương đương song hữu tỉ có dạng Montgomery $E_M : Bv^2 = u^3 + Au^2 + u$,với

$$A = \frac{2(a + d)}{a - d}, \qquad B = \frac{4}{a - d}.$$

Ký hiệu phép đổi biến này là

$$\Phi : E_{Ed} \to E_M.$$

Sử dụng phép đổi biến được cho bởi công thức (7)

$$(u, v) \mapsto (t, s) = \left(\frac{u}{B} + \frac{A}{3B}, \frac{v}{B}\right),$$

ta biến đổi E_M về một đường cong tương đương có dạng chuẩn Weierstrass

$$E_W : s^2 = t^3 + \varepsilon t + \delta,$$

với

$$\varepsilon = \frac{3 - A^2}{3B^2}, \qquad \delta = \frac{2A^3 - 9A}{27B^3}.$$

Ký hiệu phép đổi biến này là:

$$\Psi : E_M \to E_W.$$

Đặt

$$\Gamma = \Psi \circ \Phi$$

là hợp thành của Φ và Ψ. Rõ ràng,

$$\Gamma : E_{Ed} \to E_W$$

là phép đổi biến trực tiếp đưa E_{Ed} về E_W và được cho bởi công thức

$$(x, y) \mapsto (t, s) = \left(\frac{1 + y}{B(1 - y)} + \frac{A}{3B}, \frac{1 + y}{B(1 - y)x}\right). \quad (9)$$

Thay $A = \frac{2(a+d)}{a-d}, B = \frac{4}{a-d}$ vào công thức (9), ta nhận được

$$\begin{aligned} t &= \frac{1 + y}{B(1 - y)} + \frac{A}{3B} \\ &= \frac{1 + y}{\frac{4}{a-d}(1 - y)} + \frac{\frac{2(a+d)}{a-d}}{3\frac{4}{a-d}} \\ &= \frac{(a - d)(1 + y)}{4(1 - y)} + \frac{a + d}{6}, \qquad \text{và} \\ s &= \frac{1 + y}{B(1 - y)x} \\ &= \frac{1 + y}{\frac{4}{a-d}(1 - y)x} \\ &= \frac{(a - d)(1 + y)}{4(1 - y)x}. \end{aligned}$$

Như vậy, ta có công thức đổi biến từ E_{Ed} vào E_W

$$(x, y) \mapsto (t, s) = \left(\frac{(a - d)(1 + y)}{4(1 - y)} + \frac{a + d}{6}, \frac{(a - d)(1 + y)}{4(1 - y)x}\right). \quad (10)$$

Hơn nữa, ta có

$$\begin{aligned}\varepsilon &= \frac{3-A^2}{3B^2} \\ &= \frac{3-\left(\frac{2(a+d)}{a-d}\right)^2}{3\left(\frac{4}{a-d}\right)^2} \\ &= -\frac{1}{48}(a^2+14ad+d^2), \qquad \text{và} \\ \delta &= \frac{2A^3-9A}{27B^3} \\ &= \frac{2\left(\frac{2(a+d)}{a-d}\right)^3-9\frac{2(a+d)}{a-d}}{27\left(\frac{4}{a-d}\right)^3} \\ &= -\frac{1}{864}(a+d)(a^2-34ad+d^2).\end{aligned}$$

Tóm lại, với phép đổi biến $\Gamma : E_{Ed} \to E_W$ được cho bởi công thức (10), ta đã đưa đường cong dạng chuẩn Edwards $E_{Ed} : ax^2+y^2 = 1+dx^2y^2$ về đường cong tương đương song hữu tỉ có dạng chuẩn Weierstrass $E_W : s^2 = t^3+\varepsilon t+\delta$, trong đó

$$\varepsilon = -\frac{1}{48}(a^2+14ad+d^2), \tag{11}$$

$$\delta = -\frac{1}{864}(a+d)(a^2-34ad+d^2). \tag{12}$$

Về mối quan hệ giữa số điểm của đường cong dạng chuẩn Edwards E_{Ed} và đường cong dạng chuẩn Weierstrass E_W tương ứng trên trường hữu hạn k (kể cả phần tử trung hoà), ta có khẳng định sau.

Hệ quả 6. *Với các ký hiệu như ở trên, ta có*

$$\#E_{Ed}(k) = \begin{cases} \#E_W(k)-2, & \textit{nếu } \left(\frac{a}{p}\right) = -1, \\ \#E_W(k)-4, & \textit{nếu } \left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = 1, \\ \#E_W(k), & \textit{nếu } \left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1. \end{cases}$$

Chứng minh: Hệ quả này được suy trực tiếp của Định lý 4 và Mệnh đề 5. □

Xét trường hợp cụ thể $k = \mathbb{F}_p$ với $p \neq 2, 3$ là một số nguyên tố. Với các đường cong dạng chuẩn Edwards E_{Ed} được sinh ngẫu nhiên, tức là các hệ số $a, d \in \mathbb{F}_p$ được chọn ngẫu nhiên, thì tỉ lệ phân bố các đường cong này theo 3 trường hợp trong Hệ quả 6 được ước lượng trong mệnh đề phát biểu dưới đây.

Mệnh đề 7. *Giả sử các hệ số $a, d \in \mathbb{F}_p, ad(a-d) \neq 0$ của đường cong dạng chuẩn Edwards*

$$E_{Ed} : ax^2+y^2 = 1+dx^2y^2$$

được chọn một cách ngẫu nhiên đều. Khi đó tỉ lệ phân bố đường cong E_{Ed} thoả mãn các trường hợp 1, 2 và 3 tương ứng theo thứ tự từ trên xuống trong Hệ quả 6 xấp xỉ khoảng $50\%, 25\%$ và 25%.

Chứng minh: Trước hết, với $x \neq 0$ là một phần tử được chọn một cách ngẫu nhiên đều trong $\mathbb{F}_p^*$ thì xác suất để $\left(\frac{x}{p}\right) = 1$ sẽ bằng với xác suất để $\left(\frac{x}{p}\right) = -1$, và bằng $\frac{1}{2}$. Thật vậy, ký hiệu

$$\mathcal{A}_1 = \left\{x \in \mathbb{F}_p^* : \left(\frac{x}{p}\right) = 1\right\},$$

và

$$\mathcal{A}_2 = \left\{x \in \mathbb{F}_p^* : \left(\frac{x}{p}\right) = -1\right\}.$$

Xét các trường hợp sau:

- $p \equiv 1 \pmod 4$: Theo tính chất của ký tự Legendre thì

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

Do đó,

$$\left(\frac{-x}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right) = \left(\frac{x}{p}\right).$$

Suy ra

$$\#\mathcal{A}_1 = \#\mathcal{A}_2 = \frac{p-1}{2}.$$

- $p \equiv 3 \pmod 4$: Từ tính chất của ký tự Legendre, ta có

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1.$$

Do đó,

$$\left(\frac{-x}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right) = -\left(\frac{x}{p}\right).$$

Điều này cũng dẫn đến

$$\#\mathcal{A}_1 = \#\mathcal{A}_2 = \frac{p-1}{2}.$$

Bây giờ, với các trường hợp trong Hệ quả 6, ta có:

1) Trường hợp 1: Theo chứng minh ở trên thì:

$$\Pr\left[a \in_R \mathbb{F}_p^* : \left(\frac{a}{p}\right) = -1\right] = \frac{1}{2},$$

có nghĩa là tỉ lệ các đường cong E_{Ed} thuộc trường hợp này sẽ bằng 50%.

2) Trường hợp 2: Do

$$\Pr\left[a \in_R \mathbb{F}_p^*, d \in_R \mathbb{F}_p^* : \left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1\right]$$
$$= \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4},$$

suy ra tỉ lệ các đường cong E_{Ed} thuộc trường hợp này sẽ là xấp xỉ 25%.

3) Trường hợp 3: Tương tự như trên,

$$\Pr\left[a \in_R \mathbb{F}_p^*, d \in_R \mathbb{F}_p^* : \left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = 1\right]$$
$$= \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4},$$

tức là tỉ lệ các đường cong E_{Ed} thuộc trường hợp này sẽ xấp xỉ 25%.

Như vậy ta nhận được khẳng định cần chứng minh.

Từ Hệ quả 6, ta xây dựng thuật toán như dưới đây để đếm số điểm của đường cong dạng chuẩn Edwards cuộn trên trường hữu hạn.

Thuật toán 8. Đếm số điểm của đường cong Edwards cuộn trên trường hữu hạn

---

Đầu vào:

- Một đường cong Edwards cuộn $E_{Ed} : ax^2 + y^2 = 1 + dx^2y^2$ định nghĩa trên trường hữu hạn k có đặc số nguyên tố $p \neq 2, 3$.

Đầu ra:

- $\#E_{Ed}(k)$ là số điểm k-hữu tỉ của đường cong E_{Ed}.

Các bước thực hiện:

1) Tính các hệ số ε, δ theo các công thức (11) (12) và định nghĩa đường cong $E_W : s^2 = t^3 + \varepsilon t + \delta$ trên trường hữu hạn k.
2) Sử dụng Thuật toán SEA để tính $\#E_W(k)$ là số điểm k-hữu tỉ của E_W, bao gồm cả điểm trung hoà ∞.
3) Áp dụng Hệ quả 6 để tính $\#E_{Ed}(k)$ từ $\#E_W(k)$.
4) Trả về $\#E_{Ed}(k)$.

Để minh hoạ thuật toán trên, ta xét ví dụ dưới đay tương ứng với đường cong Edwards cuộn "edwards25519" trong [10].

Ví dụ 9. Xét đường cong Edwards cuộn "edwards25519" trong [10] định nghĩa trên trường $\mathbb{F}_p$ bởi phương trình

$$\text{edwards25519} : ax^2 + y^2 = 1 + dx^2y^2,$$

trong đó

$$\begin{aligned} p &= 2^{255} - 19 \\ a &= -1 \pmod p \\ d &= -121665/121666 \pmod p. \end{aligned}$$

nhóm tác giả sẽ sử dụng Thuật toán 8 ở trên để đếm số điểm của đường cong edwards25519 trên trường $\mathbb{F}_p$. Các tính toán được nhóm tác giả thực hiện với phần mềm SageMath-8.8.

```
# Khai báo đặc số p:
sage: p = 2^255 - 19; p
# Định nghĩa trường
hữu hạn K:
sage: K = GF(p); K
# Khai báo hệ số a:
sage: a = K(-1); a
# Kiểm tra tính chính
phương của a:
sage: a.is_square()
# Khai báo hệ số d:
sage: d = K(-121665/121666);
d
# Kiểm tra tính chính
phương của d:
sage: d.is_square()
# Tính hệ số A:
sage: A = K((-1)
* inverse_mod(48, p)
* (a^2 + 14 * a * d + d^2));
A
# Tính hệ số B:
```

```
sage: B = K((-1)
* inverse_mod(864, p)
* (a + d)
* (a^2 - 34 * a * d + d^2));
B
# Định nghĩa đường
cong elliptic
E : y^2 = x^3 + Ax + B
trên K:
sage: E = EllipticCurve(K,
[A, B]); E
# Đếm số điểm m = #E(K):
sage: m = E.order(); m
# Xác định số điểm n
của đường cong edwards25519.
# Trong trường hợp này n = m:
sage: n = m; n
# Phân tích n:
sage: factor(n)
```

Chạy đoạn code trên, ta tính được số điểm của đường cong edwards25519 trên trường hữu hạn $\mathbb{F}_p$ là:
$n = 2^3 * 7237005577332262213973186563042994240857116359379907606001950938285454250989.$
Đặt:
$L = 723700557733226221397318656304299424085711635937990760600195093828545425098989$
$= 2^{252} + 27742317777372353535851937790883648493,$
và giá trị đồng thừa số:

$$c = 2^3.$$

Kết quả tính toán được hoàn toàn khớp với giá trị được cho của đường cong edwards25519 trong [10].

V. Kết luận

Trong bài báo này, nhóm tác giả đã tập trung nghiên cứu việc đếm số điểm k-hữu tỉ của một đường cong Edwards cuộn E_{Ed} định nghĩa trên trường hữu hạn k. Kết quả thu được là nhóm tác giả đã đưa ra các công thức tường minh để xác định số điểm k-hữu tỉ của một đường cong Edwards cuộn từ số điểm k-hữu tỉ của các đường cong tương đương song hữu tỉ dạng Weierstrass hoặc Montgomery. Từ đó, nhóm tác giả xây dựng một thuật toán để đếm số điểm k-hữu tỉ của đường cong Edwards cuộn khi biết phương trình định nghĩa và trình bày Ví dụ 9 minh hoạ cho việc đếm số điểm của đường cong Edwards cuộn edwards25519 trong tài liệu [10].

Hướng nghiên cứu tiếp theo: Trong thời gian tiếp theo, nhóm tác giả sẽ tập trung nghiên cứu xây dựng biến thể của các Thuật toán đếm điểm Schoof hoặc SEA áp dụng trực tiếp cho đường cong Edwards cuộn. Nếu tồn tại thuật toán như vậy sẽ giúp tránh phải biến đổi song hữu tỉ đường cong Edwards cuộn về dạng Weierstrass tương ứng.

Tài liệu tham khảo

[1] FIPS 186-5. Digital signature standard (dss). Technical report, 2021.

[2] Marta Bellés-Muñoz, Barry Whitehat, Jordi Baylina, Vanesa Daza, and Jose Luis Muñoz-Tapia. Twisted edwards elliptic curves for zero-knowledge circuits. *Mathematics*, 9(23):3022, 2021.

[3] Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In *International Conference on Cryptology in Africa*, pages 389–405. Springer, 2008.

[4] Daniel J Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. Optimizing double-base elliptic-curve single-scalar multiplication. In *International Conference on Cryptology in India*, pages 167–182. Springer, 2007.

[5] Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *Journal of cryptographic engineering*, 2(2):77–89, 2012.

[6] Daniel J Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *international conference on the theory and application of cryptology and information security*, pages 29–50. Springer, 2007.

[7] Ian Blake, Gerald Seroussi, Gadiel Seroussi, and Nigel Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.

[8] Harold Edwards. A normal form for elliptic curves. *Bulletin of the American mathematical society*, 44(3):393–422, 2007.

[9] Huseyin Hisil, Kenneth Wong, Gary Carter, and Ed Dawson. Faster group operations on elliptic curves. In *Information Security 2009: proceedings of the 7th Australasian Information Security Conference*, pages 7–19. Australian Computer Society, 2009.

[10] Simon Josefsson and Ilari Liusvaara. Edwards-curve digital signature algorithm (eddsa). Technical report, 2017.

[11] Adam Langley, Mike Hamburg, and Sean Turner. Elliptic curves for security. Technical report, 2016.

[12] Christiane Peters. *Curves, Codes, and Cryptography*. PhD thesis, PhD thesis, Technische Universiteit Eindhoven, 2011.

[13] René Schoof. Elliptic curves over finite fields and the computation of square roots mod *p*. *Mathematics of computation*, 44(170):483–494, 1985.

[14] René Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie de nombres de Bordeaux*, 7(1):219–254, 1995.

[15] Dinh Tien Thanh, Nguyen Quoc Toan, Nguyen Van Son, and Nguyen Van Duan. An algorithm to select a secure twisted elliptic curve in cryptography. *Journal of Science and Technology on Information security*, 1(15):17–25, 2022.

SƠ LƯỢC VỀ TÁC GIẢ

Phó Đức Tài

Đơn vị công tác: Trường Đại học Khoa học Tự nhiên, Đại Học Quốc gia Hà Nội.
Email: taipd@vnu.edu.vn
Quá trình đào tạo: Tốt nghiệp Cử nhân Toán học tại Đại học Tổng hợp Hà Nội vào năm 1994; Thạc sĩ Toán học tại Đại học Utrecht, Hà Lan vào năm 1996; Tiến sĩ Toán học tại Đại học thành lập Tokyo, Nhật Bản vào năm 2001.
Hướng nghiên cứu hiện nay: Hình học đại số; Lý thuyết kỳ dị; Đại số máy tính; Mật mã.

Võ Tùng Linh

Đơn vị công tác: Viện Khoa học - Công nghệ mật mã, Ban Cơ yếu Chính phủ.
Email: beathovenvn@gmail.com
Quá trình đào tạo: Tốt nghiệp Cử nhân Toán học vào năm 2005 và Thạc sĩ Toán học vào năm 2014 tại Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia Hà Nội.
Hướng nghiên cứu hiện nay: Mật mã khoá công khai; Mật mã đường cong elliptic; Đường cong đại số.