CHỨNG MINH ĐẠI SỐ PHÉP CỘNG ĐIỂM TRÊN ĐƯỜNG CONG TWISTED EDWARDS (TỔNG QUÁT)

Hoàng Đức Thắng*, **Đặng Minh Tuấn***†
* Học viện Công nghệ Bưu chính Viễn thông
† Viện Nghiên cứu Ứng dụng Công nghệ CMC

***Tóm tắt*—Hệ mật RSA đang được thay thế dần bởi hệ mật dựa trên đường cong elliptic, hiện ở Việt Nam đã có 73 triệu căn cước công dân gắn chip [1] sử dụng chữ ký số ECDSA (Elliptic Curve Digital Signature Algorithm) để xác thực định danh công dân, tuy nhiên kể từ năm 2017 đến nay đã có nhiều nghiên cứu về hệ mật dựa trên đường cong Edwards bởi nó có nhiều ưu điểm hơn hệ mật elliptic [2], cho đến nay đã có 18 nền tảng Blockhain sử dụng hệ mật dựa trên đường cong Edwards làm cơ sở mật mã nguyên thủy [3]. Chứng minh đại số cho đường cong Edwards đã có trong [4]. Mở rộng nghiên cứu về đường cong Edwards, Bernstein cùng đồng nghiệp đã đưa ra một lớp đường cong mới tổng quát hóa dựa trên đường cong Edward gọi là twisted Edward cho bởi phương trình $ax^2+y^2 = 1+dx^2y^2$ và chứng minh đại số cho phép cộng bằng lý thuyết hình học xạ ảnh.Theo như hiểu biết của chúng tôi, hiện chưa có chứng minh đại số phép cộng cho trường hợp tổng quát này. Bài báo này đưa ra phương pháp chứng minh đại số cho trường hợp quát đồng thời cũng phát biểu và chứng minh định lý về tính đồng dạng giữa đường cong Edwards tổng quát và đường cong elliptic tổng quát dạng Weierstrass.**

***Từ khóa*—twisted Edward, phép cộng, ECC.**

I. ĐẶT VẤN ĐỀ

Năm 2007, Edward đề xuất dạng đường cong vốn được khái quát hóa từ Gauss và Euler là: $x^2 + y^2 = c^2(1 + dx^2y^2)$ trên trường k phi nhị phân (non-binary) [4]. Năm 2017, đường cong Edwards đã được chuẩn hóa trong tiểu chuẩn về Internet RFC 8032 [2] và đến năm 2019 đường cong này đã được đề xuất đưa vào tiêu chuẩn về chữ ký số FIPS 186-5 (bản Draft) [5]. Chữ ký số dựa trên đường cong Edward (EdDSA) đang là xu thế thay cho ECDSA trong các nền tảng Blockchain hiện đại [3] như: Solana, XRP, Cardano, Near, Polkadot, Stellar, Monero, NEM, Tenzor, Elrond, Kusama, Hedera Hashgraph, Decred, Waves, Nano, Algorand, IOST, Siacoin ...

Chữ ký số EdDSA nhiều ưu điểm hơn so với ECDSA như: hiệu năng cao hơn; không cần cần phải dùng thành phần số ngẫu nhiên duy nhất cho từng chữ ký số như ECDSA; kích thước khóa công khai và chữ ký số nhỏ hơn; chữ ký số EdDSA có khả năng kháng tấn công kênh kề (side-channel attack); công thức chữ ký số có thể áp dụng với mọi điểm trên đường cong mà không phải loại trừ điểm kỳ dị ...

Năm 2008, Bernstein và cộng sự đã khái quát nghiên cứu về đường cong Edwards và đề xuất phương trình đường cong mở rộng hơn có dạng $ax^2 + y^2 = 1 + dx^2y^2$ với $ad(a - d) \neq 0$ [6]: $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2})$, và triển khai công thức tính toán nhanh sử dụng hệ tọa độ xạ ảnh để ứng dụng vào công thức cộng hai điểm đồng thời cũng nghiên cứu các lớp đường cong Edwards thỏa mãn tính đồng dạng với đường cong Weierstrass khi d không phải là số chính phương trên trường k và cũng chỉ ra số phép tính trong công thức cho đường cong Edwards ít hơn so với đa số đường cong Weierstrass. Tuy nhiên các tác giả mới chỉ đề cập đến chứng minh đại số công thức phép cộng bằng phương pháp hình học xạ ảnh mà chưa có chứng minh đại số do đó trong bài báo này chúng tôi sẽ sử dụng khai triển đại số để chứng minh cho phép cộng hai điểm trên đường cong đồng thời cũng phát biểu và chứng minh định lý về tính đồng dạng giữa đường cong Edwards tổng quát và đường cong elliptic tổng quát dạng Weierstrass.

II. ĐƯỜNG CONG TWISTED EDWARDS

A. Định nghĩa về đường cong Edwards

Trong phần này, chúng tôi trình bày các công thức của phép tính cộng trên đường cong Edward và twisted Edward trong [6].

Định nghĩa 1. *Cho trường k có char(k) $\neq$ 2 và $d \in K\{0, 1\}$. Đường cong Edward là đường cong cho bởi phương trình:*

$$E_{E,d} : x^2 + y^2 = 1 + dx^2y^2$$

Đường cong twisted Edwards là đường cong với hai số phân biệt a, d thỏa $ad(a - d) \neq 0$:

$$E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2$$

Đường cong Edwards là đường cong twisted Edwards với hệ số $a = 1$.

Tác giả liên hệ: Đặng Minh Tuấn,
Email: tuandm@ptit.edu.vn
Đến toà soạn: 11/09/2022, chỉnh sửa: 12/12/2022, chấp nhận đăng: 22/12/2022.

Định nghĩa 2. *Hai đường cong gọi là đồng dạng (birationally equivalent) nếu tồn tại ánh xạ hữu tỉ ánh xạ hầu hết các điểm trên đường cong này thành các điểm trên đường cong khác và ngược lại sao cho thỏa mãn luật cộng:*

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1$$
$$\phi_i(P+Q) = \phi_i(P) + \phi_i(Q)$$

Trong đó ϕ_i là ánh xạ hữu tỉ và các điểm P, Q, P+Q đều xác định với ϕ_i.

Trong [6] Bernstein và cộng sự đã chứng minh đường cong twisted Edward và đường cong Montgomery là hai đường cong đồng dạng. Và chúng ta cũng thể ánh xạ từ đường cong Montgomery sang đường Weierstrass. Trong [7] các tác giả này cũng xây dựng phép ánh xạ trực tiếp cho phép chứng minh đường cong Edward đồng dạng với đường cong Weierstrass có điểm bậc 4. Tiếp theo chúng tôi phát biểu và chứng minh định lý về ánh xạ trực tiếp từ đường cong Weierstrass tới đường cong twisted Edwards.

Định lý 1. *Đường cong twisted Edward đồng dạng với đường cong Weierstrass có điểm bậc bốn trên trường K với char(K) $\neq$ 2. Hay tồn tại ánh xạ ϕ từ đường cong Weierstrass tới đường cong twisted Edwards.*

Chứng minh:

Xét đường cong Weierstrass trên trường K có dạng $E(K):\ y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$, không mất tính tổng quát đặt $y' = y - \frac{a_1x}{2}$ (do char(K) $\neq 2$) ta thu được đường cong có dạng:
$E(k):\ y'^2 + a_1'y' = x^3 + a_2'x^2 + a_3'x + a_4'$
Tương tự, đặt $y'' = y' - \frac{a_1'}{2}$ ta thu được đường cong có dạng:
$E(K):\ y''^2 = x^3 + a_1''x^2 + a_2''x + a_3''$
Giả sử $P(x_1, y_1)$ là điểm bậc 4 thuộc đường cong $E(K)$ ($y_1 \neq 0$) do đó $2P(x_2, y_2)$ là điểm thuộc đường cong $E(k)$ có điểm bậc 2 nên $2P + 2P = 0 \leftrightarrow 2P = -2P \leftrightarrow (x_2, y_2) = -(x_2, y_2) = (x_2, -y_2)$ do đó $2P$ có tọa độ $y(2P) = 0$.
Đặt $x' = x - x_2$ và do $y(2P) = 0$ ta thu được đường cong có dạng:

$$E(K):\ y^2 = x^3 + a_1x^2 + a_2x \tag{1}$$

Như vậy ta có điểm $(0,0)$ là điểm bậc 2 thuộc đường cong trên. Đường thẳng đi qua điểm $2P = (0,0)$ và tiếp tuyến với E tại $P(x_1, y_1)$ có phương trình là:

$$y = \lambda x + b, \tag{2}$$

khi đó ta có:

$$\lambda = \frac{3x_1^2 + 2a_1x_1 + a_2}{2y_1} \tag{3}$$
$$b = 0$$

Từ (2) và (3) ta thu được phương trình:

$$\begin{aligned} y_1 &= \lambda x_1 + b \\ &= \frac{3x_1^2 + 2a_1x_1 + a_2}{2y_1}x_1 + 0 \\ \leftrightarrow\ \ 2y_1^2 &= 3x_1^3 + 2a_1x_1^2 + a_2x_1 \end{aligned} \tag{4}$$

Lại có $2P \in (1)$:

$$\begin{aligned} y_1^2 &= x_1^3 + a_1x_1^2 + a_2x_1 \\ \leftrightarrow\ \ 2y_1^2 &= 2x_1^3 + 2a_1x_1^2 + 2a_2x_1 \end{aligned} \tag{5}$$

Trừ vế với vế của (4) cho (5) ta thu được:

$$\begin{aligned} x_1^3 &= a_2x_1 \\ \leftrightarrow\ \ x_1^2 &= a_2 \qquad\qquad (\text{do } x_1 \neq 0) \end{aligned}$$

Thay vào (4) ta được:

$$\begin{aligned} 2y_1^2 &= 3x_1^3 + 2a_1x_1^2 + a_2x_1 \\ \leftrightarrow\ \ a_1 &= \frac{y_1^2 - 2x_1^3}{x_1^2} = \frac{y_1^2}{x_1^2} - 2x_1 \end{aligned}$$

Xét phương trình (1):

$$\begin{aligned} y^2 &= x^3 + a_1x^2 + a_2x \\ &= x(x^2 + a_1x + a_2) \end{aligned}$$

Nếu $\delta = a_1^2 - 4a_2$ thì đường cong tự cắt chính nó - trái với định nghĩa về đường cong elliptic. Do đó:

$$\begin{aligned} \delta \neq 0 \leftrightarrow\ & (\frac{y_1^2}{x_1^2} - 2x_1)^2 - 4x_1^2 \neq 0 \\ \leftrightarrow\ & \frac{y_1^2}{x_1^2}(\frac{y_1^2}{x_1^2} - 4x_1) \neq 0 \\ \leftrightarrow\ & \frac{y_1^2}{x_1^2} - 4x_1 \neq 0 \end{aligned} \tag{6}$$

Nếu $\frac{y_1^2}{x_1^2} - 4x_1 = t^2$ thì phương trình (1) có dạng $y^2 = x(x - x_1)(x - x_2)$.
Bây giờ ta cần xác định phép biến đổi ϕ giữa $y^2 = x^3 + a_1x^2 + a_2x$ và $au^2 + v^2 = 1 + du^2v^2$.
T đặt $(\frac{x}{y}) = u$. Mặt khác, xét đường cong:

$$\begin{aligned} E_{E,a',d'} : a'u^2 + v^2 &= 1 + d'u^2v^2 \\ \leftrightarrow v^2 &= \frac{1 - a'u^2}{1 - d'u^2} \\ \leftrightarrow v^2 &= \frac{1 - a'\frac{x^2}{y^2}}{1 - d'\frac{x^2}{y^2}} \\ \leftrightarrow v^2 &= \frac{y^2 - a'x^2}{y^2 - d'x^2} \\ \leftrightarrow v^2 &= \frac{x^3 + a_1x^2 + a_2x - a'x^2}{x^3 + a_1x^2 + a_2x - d'x^2} \\ \leftrightarrow v^2 &= \frac{x^2 + (a_1 - a')x + a_2}{x^2 + (a_1 - d')x + a_2} \\ \leftrightarrow v^2 &= \frac{(x + \frac{a_1 - a'}{2})^2 + a_2 - \frac{(a_1 - a')^2}{4}}{(x + \frac{a_1 - d'}{2})^2 + a_2 - \frac{(a_1 - d')^2}{4}} \end{aligned}$$

Để RHS là số chính phương ta cần thỏa mãn: $\begin{cases} 4a_2 = (a_1 - a')^2 \\ 4a_2 = (a_1 - d')^2 \end{cases}$

Hay a', d' là nghiệm của phương trình $(x - a_1)^2 = 4a_2$ mà $a_2 = x_1^2$ nên phương trình này có 2 nghiệm: $\left[\begin{array}{l} x = a_1 + 2x_1 = (\frac{y_1}{x_1})^2 \\ x = a_1 - 2x_1 = (\frac{y_1}{x_1})^2 - 4x_1 \end{array} \right.$

Vậy, ta có:

$$\begin{cases} \phi : u = x/y \text{ và } v = (x + (a_1 - a')/2)/(x + (a_1 - d')/2) \\ \phi^{-1} : x = ((a_1 - a')/2 - v(a_1 - d')/2)/(v - 1), y = x/u \end{cases}$$

Trong đó a' và d' được chọn thỏa $a'd'(a' - d') \neq 0$ do vậy ta có thể chọn:

$$\begin{cases} a' = (\frac{y_1}{x_1})^2 \\ d' = (\frac{y_1}{x_1})^2 - 4x_1 \end{cases}$$

Ngoại lệ xảy ra khi $y = 0$ hoặc $x = \frac{d'-a_1}{2}, u = 0$ hoặc $v = 1$. □

B. Luật cộng

Bernstein và đồng nghiệp [6] đã xây dựng phần bổ sung luật về đường cong twisted Edwards là một tính tổng quát của công thức cộng Edwards trình bày trong [6].

Định nghĩa 3. *[6] Cho trường k với char(k) $\neq$ 2 và $E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2$ với $ad(a - d) \neq 0$ là đường cong twisted Edward trên trường k. Cho $(x_1, y_1), (x_2, y_2)$ là hai điểm thuộc đường cong khi đó tổng của hai điểm trên đường cong được định nghĩa bởi:*

$$\begin{aligned}(x_3, y_3) &= (x_1, y_1) + (x_2, y_2) \\ &= \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)\end{aligned}$$

Phần tử đơn vị là điểm $(0, 1)$, phần tử nghịch đảo là:

$$-(x, y) = (-x, y)$$

Được trình bày trong [6], phép cộng là hoàn toàn - không tồn tại những điểm không xác định khi mẫu số $1 \pm dx_1x_2y_1y_2 \neq 0$ tương đương d không phải là số chính phương trên trường k với $a = 1$.

Công thức cộng ở trên đã được sử dụng rộng rãi tuy nhiên chưa có chứng minh cụ thể cho phép cộng điểm trên đường cong twisted Edwards vì vậy dưới đây chúng tôi đề xuất phần chứng minh sử dụng khai triển đại số cho phép cộng hai điểm trên đường cong được định nghĩa ở trên.

Chứng minh: Ta sẽ chứng minh điểm (x_3, y_3) có tọa độ $(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2})$ thuộc đường cong $E_{E,a,d}$, điều này tương đương:

$$\begin{aligned}&a\left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right)^2 + \left(\frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)^2 \\ &= 1 + d\left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right)^2 \left(\frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)^2\end{aligned}$$

Quy đồng 2 vế ta cần chứng minh:

$$\begin{aligned}&LHS = RHS, \text{ trong đó:} \\ &LHS = a(x_1y_2 + x_2y_1)^2(1 - dx_1x_2y_1y_2)^2 \\ &+ (1 + dx_1x_2y_1y_2)^2(y_1y_2 - ax_1x_2)^2 \\ &RHS = (1 + dx_1x_2y_1y_2)^2(1 - dx_1x_2y_1y_2)^2 \\ &+ d(x_1y_2 + x_2y_1)^2(y_2y_1 - ax_1x_2)^2\end{aligned}$$

Đặt $x_1x_2y_1y_2 = T$. Xét vế trái:

$$\begin{aligned}&LHS = a(x_1y_2 + x_2y_1)^2(1 - dx_1x_2y_1y_2)^2 \\ &+ (1 + dx_1x_2y_1y_2)^2(y_1y_2 - ax_1x_2)^2 \\ &= a(1 - dT)^2(x_1y_2 + x_2y_1)^2 \\ &+ (1 + dT)^2(y_1y_2 - ax_1x_2)^2 \\ &= a(d^2T^2 - 2dT + 1)(x_1^2y_2^2 + x_2^2y_1^2 + 2T) \\ &+ (d^2T^2 + 2dT + 1)(y_1^2y_2^2 + a^2x_1^2x_2^2 - 2aT) \\ &= (d^2T^2 + 1 - 2dT)(ax_1^2y_2^2 + ax_2^2y_1^2 + 2aT) \\ &+ (d^2T^2 + 2dT + 1)(y_1^2y_2^2 + a^2x_1^2x_2^2 - 2aT) \\ &= (d^2T^2 - 2dT + 1)(ax_1^2y_2^2 + ax_2^2y_1^2 + 2aT) \\ &+ (d^2T^2 + 2dT + 1)(y_1^2y_2^2 + a^2x_1^2x_2^2 - 2aT) \\ &= (d^2T^2 + 1)(ax_1^2y_2^2 + ax_2^2y_1^2 + 2aT) \\ &- 2dT(ax_1^2y_2^2 + ax_2^2y_1^2 + 2aT) \\ &+ (d^2T^2 + 1)(a^2x_1^2x_2^2 + y_1^2y_2^2 - 2aT) \\ &+ 2dT(a^2x_1^2x_2^2 + y_1^2y_2^2 - 2aT) \\ &= (d^2T^2 + 1)[(ax_1^2y_2^2 + ax_2^2y_1^2 + 2aT) \\ &+ (a^2x_1^2x_2^2 + y_1^2y_2^2 - 2aT)] \\ &+ 2dT[(a^2x_1^2x_2^2 + y_1^2y_2^2 - 2aT) - (ax_1^2y_2^2 + ax_2^2y_1^2 + 2aT)] \\ &= (d^2T^2 + 1)[(ax_1^2y_2^2 + ax_2^2y_1^2 + a^2x_1^2x_2^2 + y_1^2y_2^2) \\ &+ 2dT(a^2x_1^2x_2^2 + y_1^2y_2^2 - ax_1^2y_2^2 - ax_2^2y_1^2 - 4aT) \\ &= (d^2T^2 + 1)[(ax_1^2y_2^2 + y_1^2y_2^2) + (ax_2^2y_1^2 + a^2x_1^2x_2^2)] \\ &+ 2dT[(a^2x_1^2x_2^2 - ax_1^2y_2^2) + (y_1^2y_2^2 - ax_2^2y_1^2) - 4aT] \\ &= (d^2T^2 + 1)[y_2^2(ax_1^2 + y_1^2) + ax_2^2(a^2x_1^2 + y_1^2)] \\ &+ 2dT[ax_1^2(ax_2^2 - y_2^2) - y_1^2(ax_2^2 - y_2^2) - 4aT] \\ &= (d^2T^2 + 1)(ax_1^2 + y_1^2)(ax_2^2 + y_2^2) \qquad (7) \\ &+ 2dT[(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) - 4aT]\end{aligned}$$

Tương tự, ta xét vế phải:

$$\begin{aligned}&RHS = (1 + dx_1x_2y_1y_2)^2(1 - dx_1x_2y_1y_2)^2 \\ &+ d(x_1y_2 + x_2y_1)^2(y_2y_1 - ax_1x_2)^2 \\ &= d(x_1y_2 + x_2y_1)^2(y_2y_1 - ax_1x_2)^2 \\ &+ (1 + dT)^2(1 - dT)^2 \\ &= (1 - d^2T^2)^2 + d(x_1y_2 + x_2y_1)^2(y_1y_2 - ax_1x_2)^2\end{aligned}$$

$$
\begin{aligned}
&= (1-d^2T^2)^2 + \\
&d[(x_1^2y_2^2 + x_2^2y_1^2) + 2T][(y_1^2y_2^2 + a^2x_1^2x_2^2) - 2aT] \\
&= (1-d^2T^2)^2 \\
&+ d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) \\
&- 2adT(x_1^2y_2^2 + x_2^2y_1^2) + 2dT(y_1^2y_2^2 + a^2x_1^2x_2^2) - 4adT^2 \\
&= [(1-d^2T^2)^2 \\
&+ d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) - 4adT^2] \\
&- 2adT(x_1^2y_2^2 + x_2^2y_1^2) + 2dT(y_1^2y_2^2 + a^2x_1^2x_2^2) \\
&= [(1-d^2T^2)^2 \\
&+ d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) - 4adT^2] \\
&+ 2dT[-a(x_1^2y_2^2 + x_2^2y_1^2) + (y_1^2y_2^2 + a^2x_1^2x_2^2)] \\
&= [(1-d^2T^2)^2 + \\
&d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) - 4adT^2] \\
&+ 2dT[(-ax_2^2y_1^2 + a^2x_1^2x_2^2) + (-ax_1^2y_2^2 + y_1^2y_2^2)] \\
&= [(1-d^2T^2)^2 + \\
&d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) - 4adT^2] \\
&+ 2dT[ax_2^2(-y_1^2 + ax_1^2) - y_2^2(ax_1^2 - y_1^2)] \\
&= [(1-d^2T^2)^2 \\
&+ d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) - 4adT^2] \\
&+ 2dT(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) \\
&= [(1-d^2T^2)^2 \\
&+ d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) + 4adT^2 - 8adT^2] \\
&+ 2dT(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) \\
&= [(1-d^2T^2)^2 + \\
&d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) + 4adT^2] \\
&+ 2dT(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) - 8adT^2 \\
&= [(1-d^2T^2)^2 + \qquad (8) \\
&d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) + 4adT^2] \\
&+ 2dT[(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) - 4aT]
\end{aligned}
$$

Mặt khác, lại có:

$$
\begin{aligned}
&d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) + 4adT^2 \\
&= d(x_1^2y_1^2y_2^4 + a^2x_1^4x_2^2y_2^2 + y_1^4y_2^2x_2^2 + a^2x_1^2x_2^4y_1^2 \\
&+ 4aT^2) \\
&= d[(a^2x_1^4x_2^2y_2^2 + y_1^4y_2^2x_2^2 + 2aT^2) + (a^2x_1^2x_2^4y_1^2 \\
&+ x_1^2y_1^2y_2^4 + 2aT^2)] \\
&= d[(a^2x_1^4x_2^2y_2^2 + y_1^4y_2^2x_2^2 + 2ax_1^2x_2^2y_1^2y_2^2) \\
&+ (a^2x_1^2x_2^4y_1^2 + x_1^2y_1^2y_2^4 + 2ax_1^2x_2^2y_1^2y_2^2)] \\
&\text{(vì } T = x_1x_2y_1y_2\text{)} \\
&= d[x_2^2y_2^2(a^2x_1^4 + 2ax_1^2y_1^2 + y_1^4) \\
&+ x_1^2y_1^2(a^2x_2^4 + y_2^4 + 2ax_2^2y_2^2)] \\
&= dx_2^2y_2^2(ax_1^2 + y_1^2)^2 + dx_1^2y_1^2(ax_2^2 + y_2^2)^2 \qquad (9)
\end{aligned}
$$

Xét:

$$
\begin{aligned}
&(1-d^2T^2)^2 = (d^2T^2+1)(d^2T^2+1) - 4d^2T^2 \\
&= (d^2T^2+1)(d^2T^2+1) \\
&+ (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) \\
&- (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)(d^2T^2 + 1 + dx_1^2y_1^2 + dx_2^2y_2^2) \\
&- (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)(d^2x_1^2x_2^2y_1^2y_2^2 + 1 + dx_1^2y_1^2 + dx_2^2y_2^2) \\
&- (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)[(d^2x_1^2x_2^2y_1^2y_2^2 + dx_1^2y_1^2) \\
&+ (dx_2^2y_2^2 + 1)] - (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)[dx_1^2y_1^2(dx_2^2y_2^2+1) + (dx_2^2y_2^2+1)] \\
&- (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)(dx_1^2y_1^2+1)(dx_2^2y_2^2+1) \\
&- (1+d^2T^2)(dx_1^2y_1^2 + dx_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)(dx_1^2y_1^2+1)(dx_2^2y_2^2+1) \\
&- (dx_1^2y_1^2 + dx_2^2y_2^2 + d^3T^2x_1^2y_1^2 + d^3T^2x_2^2y_2^2) - 4d^2T^2 \\
&= (d^2T^2+1)(dx_1^2y_1^2+1)(dx_2^2y_2^2+1) \\
&- (dx_1^2y_1^2 + d^3T^2x_1^2y_1^2 + 2d^2T^2) \\
&- (dx_2^2y_2^2 + d^3T^2x_2^2y_2^2 + 2d^2T^2) \\
&= (d^2T^2+1)(dx_1^2y_1^2+1)(dx_2^2y_2^2+1) \\
&- dx_1^2y_1^2(2dx_2^2y_2^2 + 1 + d^2x_2^4y_2^4) \\
&- dx_2^2y_2^2(2dx_1^2y_1^2 + 1 + d^2x_1^4y_1^4) \\
&= (d^2T^2+1)(ax_1^2+y_1^2)(ax_2^2+y_2^2) \\
&- dx_1^2y_1^2(dx_2^2y_2^2+1)^2 - dx_2^2y_2^2(dx_1^2y_1^2+1)^2 \\
&= (d^2T^2+1)(ax_1^2+y_1^2)(ax_2^2+y_2^2) \qquad (10) \\
&- dx_2^2y_2^2(ax_1^2+y_1^2)^2 - dx_1^2y_1^2(ax_2^2+y_2^2)^2
\end{aligned}
$$

Thay (9), (10) vào (8), ta thu được:

$$
\begin{aligned}
RHS = &[(1-d^2T^2)^2 \\
&+ d(x_1^2y_2^2 + x_2^2y_1^2)(y_1^2y_2^2 + a^2x_1^2x_2^2) + 4adT^2] \\
&+ 2dT[(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) - 4aT] \\
&= (d^2T^2+1)(ax_1^2+y_1^2)(ax_2^2+y_2^2) \\
&- dx_2^2y_2^2(ax_1^2+y_1^2)^2 - dx_1^2y_1^2(ax_2^2+y_2^2)^2 \\
&+ dx_2^2y_2^2(ax_1^2+y_1^2)^2 + dx_1^2y_1^2(ax_2^2+y_2^2)^2 \\
&+ 2dT[(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) - 4aT] \\
&= (d^2T^2+1)(ax_1^2+y_1^2)(ax_2^2+y_2^2) \\
&+ 2dT[(ax_1^2 - y_1^2)(ax_2^2 - y_2^2) - 4aT] = LHS
\end{aligned}
$$

Từ (7), (8), (9), (10) ta có $LHS = RHS$ là điều phải chứng minh. □

III. KẾT LUẬN

Trong bài báo này, chúng tôi đã chứng minh phép cộng hai điểm trên đường cong trong hệ tọa độ affine bằng cách triển khai đại số công thức phép cộng mà

không cần phải dựa vào các lý thuyết về hình học xạ ảnh, mặc dù phần chứng minh đại số là khá dài tuy nhiên chứng mình này chỉ cần sử dụng kiến thức đại số phổ thông, đồng thời cũng phát biểu và chứng minh định lý về tính đồng dạng giữa đường cong Edwards tổng quát và đường cong elliptic tổng quát dạng Weierstrass.

TÀI LIỆU THAM KHẢO

[1] Thân Hoàng, "Bộ Công an đã cấp 73 triệu căn cước công dân gắn chip," 2022. [Online]. Available: https://tuoitre.vn/bo-cong-an-da-cap-73-trieu-can-cuoc-cong-dan-gan-chip-20221011142441326.htm

[2] S. Josefsson and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA - RFC 8032)," 2017. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8032

[3] Nash, "Cryptography behind the top 100 cryptocurrencies," 2021. [Online]. Available: http://ethanfast.com/top-crypto.html

[4] H. M. Edwards, "A normal form for elliptic curves," *Bulletin of the American Mathematical Society*, vol. 44, no. 3, pp. 393–422, 2007.

[5] NIST, "Digital Signature Standard (DSS) - FIPS 186-5 (Draft)," *NIST*, 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/186/5/draft

[6] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "Twisted edwards curves," in *Progress in Cryptology – AFRICACRYPT 2008*, S. Vaudenay, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 389–405.

[7] D. J. Bernstein and T. Lange, "Faster addition and doubling on elliptic curves," in *Advances in Cryptology – ASIACRYPT 2007*, K. Kurosawa, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 29–50.

NOVEL ALGEBRAIC PROOF OF ADDITION FORMULA ON EDWARDS CURVES

Abstract: *From 2017 to date, there have been many studies on cryptosystems based on Edwards curve because it has many advantages over the elliptic curve cryptography [2], so far there are 18 Blockhain platforms using an Edwards curve-based cryptosystem as the basis primitive cryptography.The proof of addition formula for Edwards curve was given already in [4]. Expansion of research study on the Edwards curve, Bernstein and colleagues introduced a new class of curves that generalize curve Edward, called twisted Edward given by equation* $ax^2 + y^2 = 1 + dx^2y^2$ *and also provided the proof of addition formula by the theory of projective geometry. According to to the best of our knowledge, there is currently no algebraic proof addition for this general case. This article proposed an algebraic proof for the general case and also proved the theorem about equivalence between the general Edwardscurve and general Weierstrass elliptic curve.*

Keyword: twisted Edward, addition law, ECC.

TS. Đặng Minh Tuấn nhận bằng tiến sỹ ngành toán học tại Viện KHCN QS. Hiện tại TS. Đặng Minh Tuấn đang giảng dạy tại Học viện Công nghệ Bưu chính Viễn thông và nghiên cứu tạ Viện Nghiên cứu Ứng dụng công nghệ CMC. Các hướng nghiên cứu chủ yếu là mật mã, Blockchain, AI.

Hoàng Đức Thắng Sinh viên hiện đang theo học ngành an toàn thông tin tại Học viện Công nghệ Bưu chính Viễn thông.