Về tấn công gây lỗi trên hệ mật đường cong elliptic dựa vào đường cong xoắn

Đinh Quốc Tiến, Đỗ Đại Chí

***Tóm tắt*— Phương pháp thang Montgomery được biết đến là một thuật toán nhân vô hướng hiệu quả kháng lại các tấn công kênh kề đơn giản cũng như một số tấn công gây lỗi. Trong FDTC 08, Fouque cùng cộng sự [5] đã mô tả một tấn công gây lỗi dựa vào đường cong xoắn trên cài đặt thang Montgomery khi không sử dụng tọa độ y để chống lại các biện pháp đối phó việc xác minh điểm. Trong bài báo này, chúng tôi làm rõ công thức liên hệ giữa cấp của đường cong elliptic ban đầu E và xoắn E' của nó. Sau đó chúng tôi giải bài toán nhỏ: tính logarit rời rạc (DLP) trên đường cong xoắn E', từ đó dễ dàng nhận được kết quả của bài toán DLP trên đường cong ban đầu E, để nhận được khóa bí mật. Cuối cùng là đề xuất một số tiêu chí an toàn chống lại tấn công lỗi dựa trên đường cong xoắn.**

***Abstract*—The Montgomery ladder method is known as an efficient elliptic curve scalar multiplication algorithm, inherently resistant to simple side channel attacks as well as to some fault attacks. In FDTC 08, Fouque et al [5] has been presented an fault attack based on twist of the elliptic curve on the Montgomery ladder over prime fields, without using the y- coordinate, in the presence of a point validation countermeasure. In this paper, we demonstrate the related order formula of between the original elliptic curve and its twist curve; then we solve a small problem: solving the discrete logarithm problem (DLP) in twist curve E' can easily transfer to solve DLP in the original elliptic curve E, get a secret key. Finally we propose some security criterions to thwart twist curve based fault attack.**

Từ khóa— tấn công gây lỗi; đường cong xoắn; thang Montgomery; hệ mật đường cong elliptic.

Keywords— fault attacks; twist curve; Montgomery ladder; elliptic curve cryptosystem.

I. GIỚI THIỆU

Tấn công gây lỗi là một kỹ thuật tấn công kênh kề mạnh nhằm phá vỡ các lược đồ mật mã. Ý tưởng của tấn công này là chèn các lỗi vào trong quá trình tính toán của hệ thống và sử dụng các kết quả lỗi đầu ra để tìm một phần, hoặc toàn bộ thông tin bí mật được lưu trữ trong các thành phần an toàn. Năm 1997, Bonel cùng cộng sự lần đầu tiên giới thiệu kiểu mô hình này và chỉ ra cách thức khôi phục các khóa bí mật của hệ mật RSA và hệ mật dựa trên logarit rời rạc [3].

Trên hệ mật đường cong elliptic (ECC), tấn công gây lỗi có thể được chia thành ba loại: tấn công safe-error, tấn công dựa trên đường cong yếu và tấn công gây lỗi vi sai.

Trong đó, kiểu tấn công dựa trên đường cong yếu sẽ cố gắng chuyển một phép nhân vô hướng từ đường cong mạnh về đường cong yếu. Hầu hết các tấn công gây lỗi theo trường hợp này trên ECC đều cố gắng chuyển việc tính toán trên đường cong an toàn về một đường cong có độ an toàn yếu hơn. Điều này có thể đạt được bằng cách chèn các lỗi vào các tham số đường cong, điểm cơ sở, hoặc trong phép nhân vô hướng điểm.

Năm 2000, Biehl và các cộng sự [1] đã mô tả kiểu tấn công gây lỗi dựa vào đường cong yếu trên phép nhân vô hướng điểm trên đường cong elliptic, được mô tả khái quát như sau:

Tại đây, xét đường cong elliptic:

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

Ta thấy rằng, b không được sử dụng trong công thức cộng điểm, do vậy, công thức cộng đối với E vẫn thực hiện đúng đối với đường cong bất kỳ E' mà chỉ khác với đường cong E ở vị trí b.

$$E' : y^2 = x^3 + ax + b'.$$

Nếu không có một phương pháp phù hợp để kiểm tra việc có một điểm cơ sở $P(x, y)$ thuộc đường cong có hợp lệ hay không thì đối phương có thể chèn một điểm $P' = (\hat{x}, \hat{y}) \in E'(\mathbb{F}_p)$, trong đó $b' = \hat{y}^2 - \hat{x}^3 - a\hat{x}$. Giả sử P' được chọn sao cho $ord(E')$ có ước nhỏ r và $ord(P') = r$, thực hiện phép nhân vô hướng với đầu vào là điểm P', ta thu được kết quả $Q' = dP'$ trên E'. Khi đó, đối phương có thể giải bài toán DLP trong nhóm con cấp r sinh bởi P' và khôi phục được $d_r = d \bmod r$. Lặp lại quá trình trên với đủ nhiều các điểm P'_i, có thể suy ra $d_i \equiv d \bmod r_i$ từ dP'_i, trong đó $r_i = ord(P'_i)$, $\gcd(r_i, r_j) = 1$. Cuối cùng, áp dụng Định lý phần dư Trung Hoa để khôi phục d.

Ý tưởng ở trên là tương tự như tấn công nhóm con nhỏ của Lim và Lee [8], như sau:

Khi đã tính được $d_1 \equiv d \bmod r_1$, $0 < d < q$, ta có $0 < d = k_1 r_1 + d_1 < q \Rightarrow 0 < k_1 < (q - d_1)/r_1 < q/r_1$. Ta thấy, nếu tìm được k_1 thì sẽ tính được d. Hơn nữa, $0 < k_1 < q/r_1$ nên việc tìm số bit bí mật của d được rút gọn về bài toán tìm $(q - r_1)$ bit bí mật của k_1. Do đó, việc biết được $d_1 \equiv d \bmod r_1$ sẽ làm lộ một phần thông tin bit của d. Bằng cách sử dụng đủ nhiều các điểm P_i' có $ord(P_i') = r_i$ là trơn thì số bit bí mật của d được rút gọn lại chỉ còn $(q - \sum r_i)$ bit (theo Định lý phần dư Trung Hoa). Khi đó, chúng ta có thể sử dụng phương pháp Pollard Rho, Pollard Lambda hay Shank để tìm giá trị d một cách hiệu quả. Hơn nữa, nếu tổng số bit bí mật $\sum r_i$ vượt quá $|q|$ thì ta có thể tìm d mà chỉ cần sử dụng Định lý phần dư Trung Hoa.

Trong bài báo, sau Mục giới thiệu, trong Mục II chúng tôi trình bày một số lý thuyết về đường cong elliptic. Sau đó trong Mục III chúng tôi mô tả tấn công trên đường con xoắn và làm rõ cách thức khôi phục giá trị vô hướng bí mật từ tấn công gây lỗi dựa trên đường cong xoắn. Một số tiêu chí an toàn nhằm đối phó kiểu tấn công gây lỗi này được đề xuất trong mục IV. Cuối cùng là Mục Kết luận.

II. MỘT SỐ LÝ THUYẾT VỀ ĐƯỜNG CONG ELLIPTIC

A. Đường cong elliptic và xoắn của đường cong elliptic

Định nghĩa 1 [10]. *Đường cong elliptic E xác định trên trường K, $char(K) \neq 2,3$, ký hiệu là E/K, được cho bởi phương trình Weierstrass rút gọn như sau:*

$$E: y^2 = x^3 + ax + b, \quad (1.1)$$

trong đó $a, b \in K$ và thỏa mãn $4a^3 + 27b^2 \neq 0$.

$E(K) = \{(x, y) \in K \times K : y^2 - x^3 - ax - b = 0\} \cup \{\mathcal{O}\}$ *và $j-$bất biến của E cho bởi* $j(E) = 1728\dfrac{4a^3}{4a^3 + 27b^2}$.

Định nghĩa 2 [7]. *Hai đường cong elliptic E_1 và E_2 xác định trên K và cho bởi phương trình Weierstrass rút gọn $E_1: y^2 = x^3 + ax + b$ và $E_2: y^2 = x^3 + a'x + b'$ được gọi là đẳng cấu trên K nếu tồn tại $u \in K^*$ sao cho phép đổi biến $(x, y) \to (u^2 x, u^3 y)$ biến đổi phương trình của E_1 thành phương trình của E_2.*

Định lý 3 [7]. *Các đường cong elliptic $E_1: y_1^2 = x_1^3 + Ax_1 + B$ và $E_2: y_2^2 = x_2^3 + ax_2 + b$ xác định trên K là đẳng cấu trên K nếu và chỉ nếu tồn tại $\mu \in K^*$ sao cho $a = \mu^4 A$, $b = \mu^6 B$. Nếu tồn tại một μ như vậy, thì phép đổi biến $(x_2, y_2) = (\mu^2 x_1, \mu^3 y_1)$, chuyển phương trình E_2 thành phương trình E_1.*

Mệnh đề 4 [10]. *Hai đường cong elliptic mà đẳng cấu trên K thì có cùng $j-$bất biến. Ngược lại, hai đường cong có cùng $j-$bất biến là đẳng cấu trên bao đóng đại số $\bar{K}$.*

Trong đó, $\bar{K}$ được gọi là bao đóng đại số của K nếu $\bar{K}$ là mở rộng đại số của K và là một trường đóng đại số, nghĩa là $\bar{K}$ chứa một nghiệm của mọi đa thức khác không trong $\bar{K}$.

Định lý 5 (Định lý Hasse) [10]. *Gọi E là một đường cong elliptic xác định trên $\mathbb{F}_p$. Khi đó,*

$$|E(\mathbb{F}_p)| = p + 1 - t,$$

trong đó, $|t| \leq 2\sqrt{p}$ và t được gọi là vết của ánh xạ Frobenius tại p.

Ta có $(\sqrt{p} - 1)^2 \leq |E(\mathbb{F}_p)| \leq (\sqrt{p} + 1)^2$. Khi đó, lực lượng của đường cong elliptic là khá gần với giá trị p. Giá trị $|E(\mathbb{F}_q)|$ có thể được tính nhờ sử dụng thuật toán đếm điểm SEA (Schoof Elkies Atkin) [2].

Trong hệ tọa độ affine khi thực hiện công thức cộng điểm, nếu phải tính thêm phép nghịch đảo thì thời gian và chi phí tính toán sẽ tăng lên, để tránh điều này ta sẽ biểu diễn các điểm thông qua hệ tọa độ xạ ảnh. Trong hệ tọa độ xạ ảnh thuần nhất, điểm xạ ảnh $(x : y : z), z \neq 0$ tương ứng với điểm $(x/z, y/z)$ trong hệ tọa độ affine. Phương trình xạ ảnh của đường cong elliptic là: $y^2 z = x^3 + axz^2 + bz^3$. Điểm vô cực $\mathcal{O} = (0 : 1 : 0)$ và điểm đối của $(x : y : z)$ là $(x : -y : z)$.

Định nghĩa 6 (về xoắn) [6]. *Gọi E là đường cong elliptic trên $\mathbb{F}_p$ và $\lambda \in \mathbb{F}_p^*$ không là thặng dư bậc hai trong $\mathbb{F}_p$, khi đó đường cong E' xác định bởi $y^2 = x^3 + \lambda^2 ax + \lambda^3 b$, được gọi là xoắn (hoặc xoắn bậc hai) của E.*

Xét $E: y^2 = x^3 + ax + b = g(x)$.

Đặt $g_\lambda(x) = \lambda^3 g(x/\lambda)$ với $\lambda \in \mathbb{F}_p^*$ không là thặng dư bậc hai trong $\mathbb{F}_p$, ta có:

$$E': y^2 = x^3 + \lambda^2 ax + \lambda^3 b = g_\lambda(x),$$

Vì $j(E) = j(E')$ nên theo Mệnh đề 4, ta có E đẳng cấu với E' trên bao đóng đại số $\overline{\mathbb{F}}_p$. Tuy nhiên, nếu λ là một thặng dư bậc hai, thì tồn tại $u \in \mathbb{F}_p^*$ sao cho $\lambda = u^2$. Khi đó, ta có $\lambda^2 a = u^4 a$, $\lambda^3 b = u^6 b$ và theo Định lý 3, E và E' đẳng cấu với nhau trên $\mathbb{F}_p$. Do vậy, E và E' là giống nhau trên $\mathbb{F}_p$.

Ta thấy E và xoắn bậc hai E' không đẳng cấu với nhau trên $\mathbb{F}_p$ nên chúng là các đường cong khác nhau khi được xét trên trường nền $\mathbb{F}_p$.

Lớp đẳng cấu của xoắn E' không phụ thuộc vào việc chọn λ. Thật vậy, giả sử chọn $\lambda_1 \neq \lambda_2$ ($\lambda_1, \lambda_2 \in \mathbb{F}_p^*$ không là thặng dư bậc hai trong $\mathbb{F}_p$). Khi đó xác định được hai xoắn như sau:

$$E_{\lambda_1} : y^2 = x^3 + \lambda_1^2 ax + \lambda_1^3 b$$
$$E_{\lambda_2} : y^2 = x^3 + \lambda_2^2 ax + \lambda_2^3 b.$$

Xét ánh xạ:

$$\phi(x, y) = ((\lambda_1 / \lambda_2)x, (\lambda_1 / \lambda_2)^{3/2} y).$$

Ánh xạ này sẽ biến E_{λ_1} thành E_{λ_2}, do tác động của ϕ lên E_{λ_1}, ta có:

$$(\lambda_1 / \lambda_2)^3 y^2 = (\lambda_1 / \lambda_2)^3 x^3 + \lambda_1^2 (\lambda_1 / \lambda_2) ax + \lambda_1^3,$$

suy ra, $y^2 = x^3 + \lambda_2^2 ax + \lambda_2^3 b$.

B. Thuật toán nhân điểm thang Montgomery

Đầu tiên, thang Montgomery [9] được đề xuất với ý định tăng tốc phép nhân vô hướng trên đường cong elliptic dạng Montgomery. Sau đó, Brier và Joye [4] đã tổng quát hóa thuật toán cho đường cong elliptic trên $\mathbb{F}_p$.Theo đó, đối với đường cong elliptic, tung độ y là không cần thiết trong phép cộng điểm và nhân đôi điểm. Hoành độ của $P + Q$ có thể được tính từ hoành độ của P, Q, và $Q - P$.

Cụ thể, gọi $P = (x_1, y_1)$, $Q = (x_2, y_2)$ và $Q - P = (x_3, y_3)$ là các điểm thuộc E, khi đó, hoành độ của $P + Q = (x_4, y_4)$ và $2P = (x_5, y_5)$ có thể được tính như sau:

$$x_4 = \frac{2(x_1 + x_2)(x_1 x_2 + a) + 4b}{(x_1 + x_2)^2} - x_3,$$

$$x_5 = \frac{(x_1^2 - a)^2 - 8bx_1}{4(x_1^3 + ax_1 + b)}.$$

Từ đó, kết quả kP có thể được tìm bằng cách tính toán một dãy các cặp (Q, H) mà có tính chất $H - Q = P$.

Thuật toán 1. Thang Montgomery

INPUTS: $P \in E(\mathbb{F}_p)$, $d = (1, d_{l-2}, \ldots, d_0)_2$.

OUTPUTS: hoành độ x của dP.

1. $R[0] \leftarrow P$, $R[1] \leftarrow 2P$.
2. **for** $i = l - 2$ **downto** 0 **do**
   - 2.1. $R[1 - d_i] \leftarrow R[0] + R[1]$
   - 2.2. $R[d_i] \leftarrow 2R[d_i]$
3. **end for**

Return $R[0]$.

Theo [4], tung độ của dP có thể suy ra từ hoành độ của dP, P và $(d-1)P$. Cụ thể, gọi $dP = (x_1, y_1)$, $P = (x_P, y_P)$, $(d-1)P = (x_2, y_2)$, ta có

$$y_1 = \frac{2b + (a + x_P x_1)(x_P + x_1) - x_2 (x_P - x_1)^2}{2y_P}.$$

Ta thấy rằng, việc tính toán chỉ sử dụng hoành độ x giúp tiết kiệm nhiều phép nhân, dẫn tới thuật toán nhanh hơn so với các thuật toán nhị phân cổ điển. Hơn nữa, vì tung độ y không cần xử lý trong tính toán, nên yêu cầu bộ nhớ ít hơn. Thuật toán thang Montgomery cũng đưa ra lợi thế cho việc phát hiện lỗi bằng cách kiểm tra $R[1] - R[0] = P$ tại mỗi bước lặp của vòng lặp chính.

III. TẤN CÔNG GÂY LỖI TRÊN ĐƯỜNG CONG XOẮN VÀ CÁCH KHÔI PHỤC GIÁ TRỊ VÔ HƯỚNG BÍ MẬT

Trong tài liệu [2], các tác giả đã phát biểu và giải thích về công thức liên hệ giữa cấp của đường cong elliptic và xoắn của nó. Ở đây, chúng tôi phát biểu lại dưới dạng mệnh đề và trình bày chứng minh một cách tường minh. Trong chứng minh, chúng tôi sử dụng ký hiệu Legendre. Trong đó, với p là số nguyên tố lẻ, thì ký hiệu Legendre $(\frac{a}{p})$ bằng 1 (tương ứng -1) nếu a là thặng dư bậc hai (tương ứng, không là thặng dư bậc hai) theo $\bmod p$.

Mệnh đề 7 [2]. *Gọi E là đường cong elliptic trên trường $K = \mathbb{F}_p$ và E' là xoắn bậc hai của E. Khi đó,* $|E(K)| + |E'(K)| = 2p + 2$.

Chứng minh. Ta có $g_\lambda(\lambda x) = \lambda^3 g(\lambda)$. Gọi $z = x\lambda$, bởi vì có thể khôi phục được x từ

$x = z/\lambda$, nên khi x duyệt qua tất cả các điểm thuộc $\mathbb{F}_p^*$ thì z cũng duyệt qua tất cả các điểm thuộc $\mathbb{F}_p^*$ nhưng với cấp khác nhau.

Với $x \in K$, nếu $g(x) = 0$ thì $g_\lambda(\lambda x) = 0$, dẫn tới mỗi đường cong đóng góp duy nhất một điểm.

Nếu $g(x) \neq 0$ là thặng dư bậc hai, thì có hai điểm $(x, \pm y) \in E(K)$. Hơn nữa, vì λ không là thặng dư bậc hai trong K^*, nên:

$$\left(\frac{(\lambda x)^3 + a\lambda^2(\lambda x) + b\lambda^3}{p}\right) = \left(\frac{\lambda}{p}\right)\left(\frac{x^3 + ax + b}{p}\right) = -1,$$

Suy ra, $\lambda^3 g(x) = g_\lambda(\lambda x)$ không là thặng dư bậc hai. Do vậy, không có điểm thuộc $E'(K)$ với tọa độ đầu tiên λx. Khi đó, E nhận hai điểm và E' không nhận điểm nào.

Nếu $g(x) \neq 0$ không là thặng dư bậc hai, thì không có điểm thuộc $E(K)$ với hoành độ là x, nhưng khi đó:

$$\left(\frac{(\lambda x)^3 + a\lambda^2(\lambda x) + b\lambda^3}{p}\right) = \left(\frac{\lambda}{p}\right)\left(\frac{x^3 + ax + b}{p}\right) = 1,$$

Nên suy ra $\lambda^3 g(x) = g_\lambda(\lambda x)$ là thặng dư bậc hai. Vì vậy, có hai điểm $(\lambda x, \pm y) \in E'(K)$. Khi đó, E' đóng góp hai điểm còn E không đóng góp điểm nào.

Do đó, với mỗi $x \in K, g(x) \neq 0$ sẽ cho hai điểm, hoặc trên E hoặc trên E'.

Xét tổng $|E(K)| + |E'(K)|$, mỗi phần tử thuộc K được tính hai lần và có p phần tử $x \in K$, cộng thêm hai điểm vô cùng của hai đường cong, nên ta thu được tổng $2p + 2$ □

Trong [5], các tác giả đã chỉ ra cách biểu diễn tập các điểm chứa dạng xoắn của đường cong elliptic. Ở đây, chúng tôi phân tích các bước xây dựng của các tác giả.

Vì thuật toán thang Montgomery không sử dụng toạ độ y của các điểm, nên thuật toán này cũng hợp lệ đối với các điểm $(x : y : z) \in E$ với $y \in \mathbb{F}_{p^2}$ thay vì $y \in \mathbb{F}_p$. Từ đó, ta xét tập các điểm (x, y) với $x \in \mathbb{F}_p$ và $y \in \mathbb{F}_{p^2}$ và sẽ chỉ ra rằng tập các điểm này có chứa dạng xoắn của E. Điều đó được thực hiện thông qua tập S được định nghĩa như sau:

$$S = \{(0:1:0)\} \cup \{(x:y:1) \in E(\mathbb{F}_{p^2}) : x \in \mathbb{F}_p, y \in \mathbb{F}_{p^2}\}.$$

Nhằm biểu diễn đường cong E và đường cong xoắn E', chúng ta thực hiện phân hoạch tập S như sau: $S = \{\mathcal{O}\} \cup S^0 \cup S^1 \cup S^2$, trong đó:

$$S^0 = \{(x:0:1) \in E(\mathbb{F}_{p^2}) \mid \quad x \in \mathbb{F}_p\},$$

$$S^1 = \{(x:y:1) \in E(\mathbb{F}_{p^2}) \quad \mid x \in \mathbb{F}_p, y \in \mathbb{F}_p^*\},$$

$$S^2 = \{(x:y:1) \in E(\mathbb{F}_{p^2}) \quad \mid x \in \mathbb{F}_p, y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p\}.$$

Ta thấy, S^0 là tập các điểm cấp 2.

Thật vậy, xét $P = (x:y:1)$ là một điểm cấp 2. Khi đó, $2P = \mathcal{O}$, suy ra $P = -P$. Do đó, $(x:y:1) = (x:-y:1)$, hay $y = 0$.

Sau đây ta sẽ chỉ ra rằng số lượng các điểm phân biệt của tập S được biểu diễn thông qua số lượng các điểm cấp 2. Cụ thể, ta chỉ ra S chứa $2p + 1 - \alpha$ điểm phân biệt, tức là, $|S| = 2p + 1 - \alpha$.

Thật vậy, đặt $|S^0| = \alpha$. Ta thực hiện phép đếm điểm như sau: xét $S^1 \cup S^2$, với mỗi $x \in S^1 \cup S^2$ sẽ cho ta chính xác hai điểm phân biệt (x, y_1) và (x, y_2). Do tính rời nhau của các tập S^1, S^2 và đã có α các điểm cấp 2. Cho nên:

$$|S^1| + |S^2| = 2p - 2\alpha = 2(p - \alpha).$$

Khi đó bằng cách phân hoạch tập S, ta thu được kết quả như sau:

$$|S| = 1 + \alpha + |S^1| + |S^2| =$$
$$= 1 + \alpha + 2(p - \alpha) = 2p + 1 - \alpha.$$

Theo phép đếm điểm ở trên, ta thấy rằng dường như việc phân hoạch S^1 và S^2 không đóng góp nhiều ý nghĩa vào việc tính số điểm phân biệt trong S. Tuy nhiên, sau đây sẽ chỉ ra rằng việc phân hoạch các tập S^1 và S^2 giúp thấy rõ biểu diễn của đường cong E và đường cong xoắn E' trong tập S.

Ta có, $E(\mathbb{F}_p) = \{\mathcal{O}\} \cup S^0 \cup S^1$. Giả sử rằng $|E(\mathbb{F}_p)| = p + 1 - c$.

Khi đó,

$$|S^2| = |S| - E(\mathbb{F}_p) =$$
$$(2p + 1 - \alpha) - (p + 1 - c) = p + c - \alpha.$$

Suy ra:

$$|\{\mathcal{O} \cup S^0 \cup S^2\}| = p + c - \alpha + \alpha + 1 = p + 1 + c.$$

Theo Mệnh đề 7, ta có

$$|E'| = 2(p+1) - |E| = p + 1 + c.$$

Do đó, $|E'| = |\{\mathcal{O} \cup S^0 \cup S^2\}|$. Từ đó thấy rằng, biểu diễn của E và E' là khác nhau ở tập S^1 và S^2. Rõ ràng, nếu x không phải là hoành độ của một điểm thuộc E, thì x sẽ đưa ra λx là hoành độ của một điểm thuộc E'. Do đó, các điểm thuộc $\mathcal{O} \cup S^0 \cup S^2$ có thể dễ dàng được ánh xạ tới các điểm trên xoắn E'.

Do vậy, ta sẽ thực hiện tính toán trên tập S chứa đường cong E và dạng xoắn của đường cong E. Từ các phân tích ở trên cũng như trong [5], rút ra các nhận xét sơ bộ như sau:

1. Cấp nhóm của E và E' có độ lớn như nhau (cỡ $\mathcal{O}(p)$).

2. Xét đường cong elliptic E xác định trên $\mathbb{F}_p$, một giá trị ngẫu nhiên $x \in \mathbb{F}_p$ tương ứng với hoành độ của một điểm hoặc trên E hoặc trên xoắn E' với xác suất xấp xỉ ½ (theo nhận xét trên).

3. Thuật toán Montgomery khi không sử dụng tọa độ y, thì khi hoạt động hoặc trên đường cong E hoặc E' không có sự khác nhau.

4. Khi cấp của E là nguyên tố, thì không có nghĩa là cấp của E' cũng là nguyên tố.

Tiếp theo, chúng tôi trình bày tóm tắt ý tưởng tấn công gây lỗi dựa trên đường cong xoắn của Fouque cùng cộng sự [5] và giải bài toán tìm $d \bmod ord(E)$ khi đã biết $d \bmod ord(E')$.

Mô hình tấn công gây lỗi dựa vào đường cong xoắn E'

- Kẻ tấn công sửa đổi tọa độ x của điểm P tạo thành điểm P' sao cho $\hat{P} \in E'$.
- Mục tiêu tấn công hướng tới là cài đặt phép nhân vô hướng thang Montgomery khi tọa độ y không được sử dụng. Thực hiện phép nhân vô hướng với $P' \in E'$ cho ta kết quả lỗi $\hat{Q} = d\hat{P} \in E'$.
- Tính được $d \bmod ord(\hat{P})$ bằng cách giải bài toán DLP trong nhóm $\langle \hat{P} \rangle$.

Trong [5], Fouque cùng cộng sự đã trình bày hai tấn công dựa trên đường cong xoắn. Tấn công cơ bản không tính đến biện pháp đối phó là khi đối phương có khả năng chọn điểm đầu vào P và cài đặt không sử dụng xác minh điểm tại cuối thuật toán nhân vô hướng. Tấn công thứ hai giả thiết rằng kẻ tấn công không thể chọn P và cài đặt xác minh điểm kết quả tại cuối phép nhân vô hướng. Trong trường hợp này, kẻ tấn công cần chèn hai lỗi. Thứ nhất, một lỗi được chèn vào hoành độ x của điểm cơ sở P tạo thành P'. Khi đó, $P' \in E'$ với xác suất ½. Thứ hai, tại cuối tính toán, một lỗi được chèn vào hoành độ x của dP' ngay trước khi xác minh điểm. Khi đó, kẻ tấn công vượt qua bước xác minh điểm với xác suất ½ . Có thể thu được đầu ra lỗi và vượt qua xác minh điểm với xác suất ¼.

Cũng giống như ý tưởng về tấn công đường cong yếu, khi thu được $Q' = dP'$ trên E', với $ord_{E'}(P')$ trơn hoặc nhỏ thì kẻ tấn công có thể giải bài toán logarit rời rạc sử dụng các thuật toán như phân tích Pohlig-Hellman, phương pháp baby-step-giant-step của Shank, phương pháp Pollar-ρ để tính $d \bmod ord(P')$. Lặp lại quá trình với đủ nhiều các điểm P' khác nhau và sử dụng Định lý thặng dư Trung Hoa, ta tính được giá trị $d \bmod ord(E')$ với độ phức tạp thời gian là căn bậc hai của nhân tử lớn nhất của cấp của xoắn. Với giả thiết rằng $ord(E)$ là số nguyên tố.

Bài toán: *Cho trước* $d \bmod ord(E')$ *và* $0 < d < ord(E)$, *khi đó ta tính được khóa bí mật* $d \bmod ord(E)$.

Lời giải: Gọi $ord(E) = a_1$ và $ord(E') = a_2$, như ta đã biết $0 < d < a_1$. Ta xét hai trường hợp như sau:

Trường hợp 1: $a_1 \le a_2$. Khi đó, $d < a_2$ nên $d \bmod a_2 = d$. Do đó, ta khôi phục được $d \bmod ord(E)$ từ $d \bmod ord(E')$.

Trường hợp 2: $a_2 < a_1$. Ta sẽ chỉ ra $\frac{a_1}{a_2} < 2$.

Thật vậy, theo định lý Hasse và Mệnh đề 7, kết hợp với điều kiện $a_2 < a_1$, ta có biểu diễn a_1, a_2 như sau: $a_1 = p + 1 + t$ và $a_2 = p + 1 - t$, với $0 < t \le 2\sqrt{p}$. Khi đó:

$$\frac{a_1}{a_2} = \frac{p+1+t}{p+1-t} = 1 + \frac{2t}{p+1-t} < 1 + \frac{4\sqrt{p}}{p+1-2\sqrt{p}}$$

Ta thấy, nếu $p > 6\sqrt{p}$, thì ta có đánh giá sau:

$$p > 6\sqrt{p} \Leftrightarrow p^2 > 36p \Leftrightarrow p > 36$$

Do đó, với $p > 36$ thì $p + 1 > 6\sqrt{p}$. Khi đó:

$$\frac{a_1}{a_2} < 1 + \frac{4\sqrt{p}}{p+1-2\sqrt{p}} < 1 + \frac{4\sqrt{p}}{6\sqrt{p}-2\sqrt{p}} = 2$$

Gọi $d \bmod a_2 = r$, ta có biểu diễn $d = d_2 a_2 + r, d_2 \in \mathbb{N}$. Như đã biết $0 < d < a_1$, khi đó ta có:

$$0 < d = d_2 a_2 + r < a_1 \Rightarrow 0 \le d_2 < \frac{a_1 - r}{a_2} < \frac{a_1}{a_2} < 2.$$

Do vậy, $d_2 \in \{0,1\}$, hay chỉ có duy nhất một hoặc hai khả năng cho d như sau:

Với $d_2 = 0$, ta có $d \bmod a_2 = d \bmod a_1 = r$.

Với $d_2 = 1$, ta thu được $d = d \bmod a_2 + a_2$.

Khi đó, với duy nhất một thông điệp, kẻ tấn công đã có thể khôi phục vô hướng bí mật d.

Ví dụ: Đối với đường cong *secp256k1*, cấp của xoắn là:

$$3 \times 197 \times 1559 \times 96769 \times 146849 \times$$
$$2587814237219 \times 375925338294461779 \times$$
$$1010091789365275595885630233 59$$

Vì vậy, trong cài đặt mà không có biện pháp bảo vệ, kẻ tấn công có thể tính logarit rời rạc trên xoắn với chi phí 2^{50} và khôi phục được vô hướng bí mật cho $n = 256$.

Thực tế, trong số 5 đường cong được đề xuất bởi NIST trên trường nguyên tố, chỉ có duy nhất đường cong ký hiệu P-384 là có xoắn với cấp nguyên tố. Đối với những đường cong còn lại, cấp nhóm của đường cong xoắn là hợp số và do đó dễ bị tấn công hơn.

IV. ĐỀ XUẤT MỘT SỐ TIÊU CHÍ AN TOÀN

Từ việc phân tích tấn công ở trên, chúng tôi đề xuất các tiêu chí an toàn đối phó với tấn công gây lỗi dựa trên đường cong xoắn như sau:

- *Xác minh điểm (khi cài đặt):* kiểm tra các điểm đã tác động có thuộc đường cong E và không thuộc đường cong xoắn E' hay không trong mỗi giai đoạn trước và sau thực hiện phép nhân vô hướng. Điều này sẽ làm giảm xác suất thành công của kẻ tấn công.
- *Thuật toán nhân vô hướng (khi cài đặt):* thực hiện thuật toán nhân vô hướng có sử dụng tọa độ y.
- *Lựa chọn đường cong (khi sinh bộ tham số miền):* Khó có thể giải bài toán DLP trên đường cong xoắn E' để có thể suy về việc giải bài toán DLP trên đường cong E. Cần chọn đường cong E mà có xoắn bậc hai E' an toàn theo nghĩa cấp của đường cong xoắn hoặc là số nguyên tố hoặc có ít nhất một ước nguyên tố lớn hơn 2^{200} theo tiêu chí của SafeCures [13].

Các tiêu chí 1 và 2 được thực hiện trong quá trình cài đặt thuật toán, còn tiêu chí 3 phải được thực hiện khi lựa chọn đường cong elliptic. Dựa vào kết quả của Mệnh đề 7 và Bài toán giải quyết ở trên, chúng tôi đã đưa ra bảng đánh giá theo tiêu chí 3 đối với một số đường cong elliptic trong các chuẩn của GOST, NIST, Brainpool,…

BẢNG 1. ĐÁNH GIÁ TIÊU CHÍ AN TOÀN CỦA MỘT SỐ ĐƯỜNG CONG ELLIPTIC TRONG CÁC CHUẨN

Đường cong	**Tham số** p, ord(E), ord(E') = $2p$+2-ord(E) = $\prod q_i$, q' = max{ q_i }	$q' > 2^{200}$ **(60 digits)**
NIST P-224	p = 2^224 - 2^96 + 1 ord(E) = 26959946667150639794667015087019630673557916260026308143510066298881 ord(E') = 269599466671506397946670150870196259404578077144243917216827223680612 65337410229703 (68 digits) = $3^2 \times 11 \times 47 \times 3015283 \times 40375823 \times 267983539294927 \times$p36 p36 = 177594041488131583478651368420021457	False
brainpoolP256t1	p = 76884956397045344220809746629001649093037950200943055203735601445031516197751 ord(E) = 76884956397045344220809746629001649092737531784414529538755519063063536359079 ord(E') = 76884956397045344220809746629001649093338368617471580868715683826999496036425 (77 digits) = $5^2 \times 175939 \times 492167257 \times 8062915307 \times 2590895598527 \times 4233394996199 \times$p27 p27 = 401601867518226318515439169	False
ANSSI FRP256v1	p = 109454571331697278617670725030735128145969349647868738157201323556196022393859 ord(E) = 109454571331697278617670725	False

	0307351281460045468114024126530722032077260795632330rd(E') =1094545713316972786176707250307351281459341524843350636613304439040466596522448778 digits) =7×439×11760675247×3617872258517821×p48p48 =8371164146303769607029157826141789376993385558370	
NIST P-256	p=2^256 - 2^224 + 2^192 + 2^96-1115792089210356248762697446949407573530086143415290314195533631308867097853951ord(E) =1157920892103562487626974469494075735299969552241357603424222590610685120443690rd(E') =1157920892103562487626974469494075735301753316064448680486450035566656836635358 digits) =3×5×13×179×p73p73 =3317349640749355357762425066592395746459685764401801118712075735758936647	True
GOST R 34.10-2001/2012	p =5789604461865809771178549250434395392663499233282028201972879200395656482104 1ord(E) =5789604461865809771178549250434395392708293458372545062238097359213763106961 9ord(E') =5789604461865809771178549250434395392618705008191511341707661041577549857246 5 (77 digits) = 3^3×5×7×19×p73p73=3224508193743141058857448761032801666732779174709836447623314420260400923	True

Dựa vào kết quả ở Bảng 1 chúng ta có thể kết luận như sau:

- Các đường cong NIST P-224, brainpoolP256t1 và ANSSI FRP256v1 không có tính an toàn xoắn;
- Các đường cong NIST P-256 và GOST R 34.10-2001/2012 là có tính an toàn xoắn.

V. KẾT LUẬN

Trong bài báo này, chúng tôi đã làm rõ về công thức liên hệ giữa cấp của đường cong elliptic ban đầu và xoắn của nó. Đồng thời, diễn giải lại cách thức xây dựng nhóm con các điểm trên E có dạng đường cong xoắn và đưa ra lời giải cho việc tính giá trị vô hướng bí mật d khi biết được giá trị $d \bmod ord(E')$. Từ những phân tích đó, chúng tôi đề xuất các tiêu chí an toàn nhằm kháng lại kiểu tấn công gây lỗi dựa trên đường cong xoắn.

Bên cạnh đó, trong [12], các tác giả đã có đánh giá về việc này như sau: "Nếu sử dụng một biến thể trong kỹ thuật của Galbraith và McKee [11], ta thấy rằng xác suất để một đường cong elliptic ngẫu nhiên trên $\mathbb{F}_p$ và xoắn của nó là an toàn có thể bị chặn dưới bởi $\frac{1}{2\log^2 p}$ và bị chặn trên bởi $\frac{5}{\log^2 p}$". Tuy nhiên, chúng tôi chưa đánh giá được xác suất để tìm được một đường cong elliptic ngẫu nhiên trên $\mathbb{F}_p$ và xoắn của nó là an toàn. Và đây sẽ là hướng nghiên cứu tiếp theo về chủ đề này.

TÀI LIỆU THAM KHẢO

[1]. I. BIEHL, B. MEYER and V. MÜLLER, "Differential fault attacks on elliptic curve cryptosystems, Advances in Cryptology" CRYPTO 2000, Springer, pp. 131-146, 2000.

[2]. I. F. BLAKE, G. SEROUSSI and N. SMART, "Elliptic curves in cryptography", Cambridge university press, 1999.

[3]. D. BONEH, R. A. DEMILLO and R. J. LIPTON, "On the importance of eliminating errors in cryptographic computations", Journal of cryptology 14, pp. 101-119, 2001.

[4]. E. BRIER and M. JOYE, "Weierstraß elliptic curves and side-channel attacks, Public Key Cryptography", Springer, pp. 335-345, 2002.

[5]. P.-A. FOUQUE, R. LERCIER, D. RÉAL and F. VALETTE, "Fault attack on elliptic curve Montgomery ladder implementation, Fault Diagnosis and Tolerance in Cryptography", 2008. FDTC'08. 5th Workshop on, IEEE, pp. 92-98, 2008.

[6]. S. D. GALBRAITH, "Mathematics of public key cryptography", Cambridge University Press, 2012.

[7]. D. HANKERSON, A. J. MENEZES and S. VANSTONE, "Guide to elliptic curve cryptography", Springer Science & Business Media, 2006.

[8]. C. H. LIM and P. J. LEE, "A key recovery attack on discrete log-based schemes using a prime order subgroup, Advances in Cryptology" CRYPTO'97, Springer, pp. 249-263, 1997.

[9]. P. L. MONTGOMERY, "Speeding the Pollard and elliptic curve methods of factorization", Mathematics of computation, 48, pp. 243-264, 1987.

[10]. L. C. WASHINGTON, "Elliptic curves: number theory and cryptography", CRC press, 2008.

[11]. S. D. GALBRAITH and J. MCKEE, "The probability that the number of points on an elliptic curve over a finite field is prime", Journal of the London Mathematical Society, 62, pp. 671-684, 2000.

[12]. J.-P. FLORI, J. PLÛT, J.-R. REINHARD and M. EKERA, "Diversity and Transparency for ECC, NIST workshop on ECC Standards", 2015.

[13]. http://safecurves.cr.yp.to/

SƠ LƯỢC VỀ TÁC GIẢ

TS. Đinh Quốc Tiến

Đơn vị công tác: Viện Khoa học - Công nghệ Mật mã, Ban Cơ yếu Chính phủ, Hà Nội.

Email: tiendq77@gmail.com

Nhận bằng Kỹ sư tại Học viện Kỹ thuật Mật mã năm 2000. Nhận bằng Thạc sĩ mật mã tại Học viện Kỹ thuật Mật mã năm 2007. Nhận bằng Tiến sĩ Toán học tại Viện Khoa học Công nghệ Quân sự Bộ Quốc phòng năm 2015.

Hướng nghiên cứu hiện nay: Mật mã khóa công khai và tiêu chuẩn mật mã.

CN. Đỗ Đại Chí

Đơn vị công tác: Viện Khoa học - Công nghệ Mật mã, Ban Cơ yếu Chính phủ, Hà Nội.

Email: chidd@bcy.gov.vn

Nhận bằng Cử nhân Toán học, Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội năm 2014.

Hướng nghiên cứu hiện nay: Mật mã khóa công khai (Bài toán DLP).