VỀ MỘT PHƯƠNG PHÁP TRAO ĐỔI KHÓA MÃ AN TOÀN

Nguyễn Nam Hải[1*], Nguyễn Thị Thu Nga[2]

Tóm tắt: *Sự phát triển nhanh chóng của mật mã trong những năm gần thúc đẩy các kỹ thuật bảo mật dữ liệu và xác thực người dùng, bảo mật thông tin trên đường truyền…. Bài viết trình bày một phương pháp trao đổi khóa mã an toàn và những ứng dụng mới của hệ mật sử dụng cơ chế cộng điểm trên đường cong elliptic.*

Từ khóa: Đường cong elliptic, Bảo mật thông tin, Bảo mật dữ liệu, Diffie-Hellman, Song tuyến.

1. GIỚI THIỆU

Bài toán logarit rời rạc (DLP) được quan tâm nghiên cứu kể từ khi xuất hiện mật mã khóa công khai năm 1975. Vấn đề được đặt ra là với nhóm cyclic G = <P> bậc *n,*tìm kiếm một số x ∈ [*0, n - 1*], thỏa mãn phương trình:

$$Q = xP.$$

Bài toán này khó tính toán và các nhóm như vậy thường là nhóm nhân trên trường hữu hạn và nhóm các điểm của đường cong elliptic trên trường hữu hạn.

Bài toán Diffie-Hellman liên quan đến bài toán logarit rời rạc. Đó là tìm kiếm đại lượng *abP* trên cơ sở *P, aP, và bP*. Có thể chỉ ra rằng đối với bất kỳ nhóm nào, bài toán logarit rời rạc có thể rút gọn về bài toán Diffie-Hellman. Bài toán ngược đã được chứng minh chỉ đúng trong một số trường hợp nhất định.

Độ khó của bài toán Diffie-Helman là cơ sở cho độ an toàn của giao thức thỏa thuận khóa. Giả sử chúng ta có một nhóm cho G = <P> bậc *n*, quá trình thỏa thuận khóa như sau:

1. Bên A chọn ngẫu nhiên số $a \in [0, n - 1]$ và tính *aP*, gửi cho Bên B.
2. Bên B chọn ngẫu nhiên số $b \in [0, n - 1]$ và tính *bP*, gửi cho Bên A.

	Bên A	Bên B
Đã có	*a, bP*	*b, aP*
Cần tính	$K = a(bP) = abP$	$K = b(aP) = abP$

Giá trị khóa thỏa thuận được là $K = abP = a(bP) = b(aP)$. Giao thức này được gọi một vòng, vì mỗi bên nhận dữ liệu từ đối tác của mình chỉ một lần.

Thỏa thuận về một khóa chung bởi ba bên thì phức tạp hơn và đòi hỏi một giao thức thỏa thuận khóa hai vòng. Dưới đây là các bước thực hiện:

1. Vòng đầu tiên.

(a) Bên A chọn ngẫu nhiên số $a \in [0, n - 1]$ và tính *aP*, gửi cho Bên B.

(b) Bên B chọn ngẫu nhiên số $b \in [0, n - 1]$ và tính *bP*, gửi cho Bên C.

(c) Bên C chọn ngẫu nhiên số $c \in [0, n - 1]$ và tính *cP*, gửi cho Bên A.

2. Vòng thứ hai.

(a) Bên A dựa vào giá trị *a* và *cP* tính *acP*, sau đó sẽ gửi cho Bên B.

(b) Bên B dựa vào giá trị *b* và *aP* tính *baP*, sau đó sẽ gửi cho Bên C.

(c) Bên C dựa vào giá trị *c* và *bP* tính *bcP*, sau đó sẽ gửi cho Bên A.

	Bên A	Bên B	Bên C
Vòng 1	*a, cP*	*b, aP*	*c, bP*

Vòng 2	*a, cP, bcP*	*b, aP, acP*	*c, bP, abP*
Cần tính	*K = a(bcP)*	*K = b(acP)*	*K = c(abP)*

Giá trị khóa thỏa thuận được sẽ là K = abcP.

Ở đây, nảy sinh một câu hỏi tự nhiên là: có tồn tại giao thức một vòng nào phù hợp với ba bên? Câu hỏi vẫn mở cho đến khi Joux đề xuất giải pháp sử dụng biến đổi song tuyến [3]. Sau đó, xuất hiện đề xuất thú vị dựa trên ánh xạ song tuyến mà cụ thể là kết hợp các cặp điểm trên đường cong elliptic. Những đề xuất nổi tiếng nhất cho đến nay là sơ đồ mã hóa dựa trên định danh (Boneh và Franklin) [4] và sơ đồ chữ ký số ngắn (Boneh, Lynn và Shacham) [5].

2. MỘT SỐ KHÁI NIỆM VÀ KIẾN THỨC CƠ BẢN LIÊN QUAN

2.1. Ánh xạ song tuyến

Giả sử rằng *n* là số nguyên tố. Cho $G_1 = <P>$ là một nhóm cyclic bậc *n* có tính chất cộng và một phần tử trung hòa ∞, G_T là một một nhóm cyclic bậc *n* có tính chất nhân và phần tử đơn vị 1. Khi đó, biến đổi song tuyến có thể định nghĩa như sau:

Định nghĩa 1: Biến đổi song tuyến trên (G_1, G_T) được gọi là biến đổi

$$\hat{e}: G_1 \times G_1 \rightarrow G_T,$$

thỏa mãn các điều kiện sau đây:

1. (Song tuyến tính - bilinear) Cho mỗi $R, S, T \in G_1$, ta có:

$\hat{e}(R + S, T) = \hat{e}(R, T)\,\hat{e}(S, T)$ và $\hat{e}(R,S + T) = \hat{e}(R, S)\,\hat{e}(R, T)$.

2. (Không suy biến Non-degeneracy) $\hat{e}(P,P) \neq 1$.

3. (Khả năng tính toán) Giá trị $\hat{e}(P,R)$ có thể được xác định một cách hiệu quả.

Có thể chứng minh rằng ánh xạ song tuyến có các tính chất sau:

1. $\hat{e}(S, \infty) = 1$, và $\hat{e}(\infty, S) = 1$.
2. $\hat{e}(S,-T) = \hat{e}(-S,T) = \hat{e}(S,T)^{-1}$.
3. $\hat{e}(aS,bT) = \hat{e}(S,T)^{ab}$ với mọi $a, b \in \mathbb{Z}$
4. $\hat{e}(S,T) = \hat{e}(T,S)$.
5. Nếu $\hat{e}(S,R) = 1$ thì đối với tất cả $R \in G_1$ thì $S = \infty$.

Một trong những kết quả từ một ánh xạ song tuyến là bài toán logarit rời rạc trong nhóm G_1 có thể được đơn giản hóa một cách hiệu quả thành bài toán logarit rời rạc trong một nhóm G_T. Bởi vì nếu chúng ta tìm kiếm một lời giải của phương trình $Q = xP$ nhóm G_1, số *x* cần tìm cũng là nghiệm của phương trình $\hat{e}(P,Q) = \hat{e}(P,xP) = \hat{e}(P,P)^x$ trong nhóm G_T.

Độ an toàn của nhiều giao thức dựa trên các ánh xạ song tuyến dựa vào độ khó tính toán của bài toán sau

Định nghĩa 2: Nếu $\hat{e}$ là ánh xạ song tuyến, thì bài toán song tuyến Diffie-Hellman ba bên được định nghĩa như sau: Với *P, aP, bP* và *cP* cho trước cần tính $\hat{e}(P, P)^{abc}$.

Độ khó của việc tính toán bài toán song tuyến Diffie-Hellman dẫn đến độ khó của bài toán Diffie-Hellman cả trong nhóm G_1 và nhóm G_T. Giả thiết chúng ta có thể giải bài toán Diffie-Hellman một cách hiệu quả trong nhóm G_1, trên cơ sở *aP* và *bP* và ta có thể tính *abP*, dẫn đến việc tìm $\hat{e}(abP,cP) = \hat{e}(P,P)^{abc}$. Nếu biết

phương pháp giải bài toán Diffie-Hellman hiệu quả trong nhóm G_T, thì tính toán $g = \hat{e}(P,P)$, $g^{ab} = \hat{e}(aP,bP)$,$g^c = \hat{e}(P,cP)$, có thể xác định $g^{abc} = \hat{e}(P,P)^{abc}$.

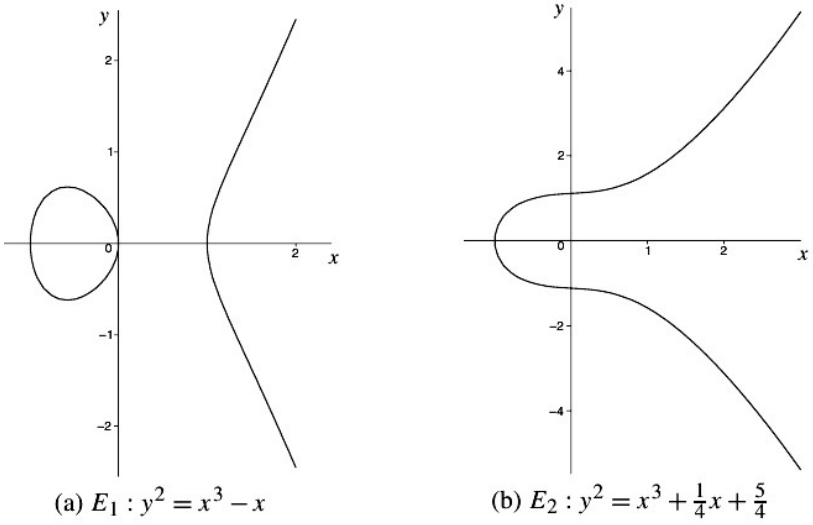
Sự tồn tại của một ánh xạ song tuyến cho phép giải chính xác bài toán Diffie-Hellman trong nhóm G_1. Liên quan đến câu hỏi liệu bốn phần tử P, aP, bP và cP có thỏa mãn đẳng thức $abP = cP$. Sử dụng ánh xạ song tuyến có thể viết $\gamma_1 = \hat{e}(P,cP) = \hat{e}(P,P)^c$, và $\gamma_2 = \hat{e}(aP,bP) = \hat{e}(P,P)^{ab}$. Điều này có nghĩa đẳng thức $abP = cP$ xảy ra khi và chỉ khi $\gamma_1 = \gamma_2$.

2.2. Đường cong Elliptic

Đường cong elliptic E trên trường K được xác định bởi phương trình Weierstrass không suy biến:

$$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

trong đó, $a_1, a_2, a_3, a_4, a_6 \in K$. Tập $E(K)$ là tập hợp các điểm K hữu tỷ của đường cong và bao gồm một điểm ở vô cực ∞, và những điểm $(x, y) \in K \times K$ mà thỏa mãn phương trình đường cong.



Hình 1. *Đường cong elliptic trên mặt phẳng thực.*

Nếu K là một trường hữu hạn $\mathbb{F}q$ với đặc trưng p, thì định lý Hasse cho một giới hạn về số lượng các điểm K hữu tỷ:

$$\left(\sqrt{q}-1\right)^2 \le \left|E(K)\right| \le \left(\sqrt{q}+1\right)^2$$

Do đó, chúng ta có thể giả định rằng $|E(K)| = q + 1 - t$, với $|t| \le 2\sqrt{q}$. Nếu $p \mid t$, chúng ta nói rằng đường cong E là siêu kỳ dị.

Trong trường hợp khi $p > 3$, phương trình Weierstrass có thể đơn giản hóa bằng cách sử dụng biến đổi tuyến tính các biến về dạng:

$$E : Y^2 = X^3 + aX + b,$$

Ví dụ, cho p=5, thì $2 \le \left|E(F_5)\right| \le 10$, như vậy, số điểm của đường cong Elliptic trên trường hữu hạn F_5là trong khoảng từ 2 đến 10. Thực tế, tất các các đường cong Elliptic có thể có trên F_5 và số điểm tương ứng được mô tả như trong bảng 1.

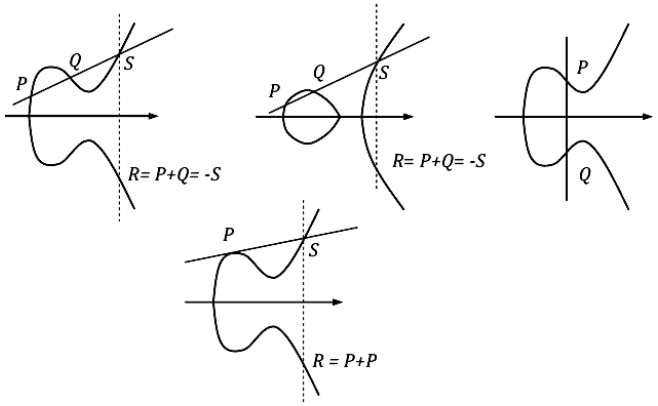
Bảng 1. *Số điểm của các đường cong Elliptic tương ứng trên trường F_5.*

STT	Đường cong Elliptic	Số điểm
1	$y^2=x^3+2x$	2
2	$y^2=x^3+4x+2$	3
3	$y^2=x^3+x$	4
4	$y^2=x^3+3x+2$	5
5	$y^2=x^3+1$	6
6	$y^2=x^3+2x+1$	7
7	$y^2=x^3+4x$	8
8	$y^2=x^3+x+1$	9
9	$y^2=x^3+3x$	10

Phương pháp cát tuyến và tiếp tuyến cho thấy cách thực hiện phép toán trên các điểm của đường cong elliptic. Phép toán trên các điểm của đường cong trên trường số thực được minh họa trong hình 2. Cụ thể:

i) Với 2 điểm *P*, *Q* bất kỳ, kẻ một đường thẳng đi qua *P* và *Q* thì sẽ cắt đường cong Elliptic tại một điểm thứ 3 là điểm *S*. Phép cộng *P* và *Q* sẽ là $R = P + Q = -S$. Trong trường hợp *P* và *Q* đối xứng nhau qua trục hoành, hay nói cách khác *Q* = -*P* thì đường thẳng nối *P* và *Q* sẽ cắt đường cong tại một điểm thứ 3 ở vô cực, hay *P*+ -(*P*)=∞.

ii) Để tính *P*+*P*, ta vẽ đường thẳng tiếp tuyến với đường cong Elliptic tại điểm P, đường thẳng này sẽ cắt đường cong Elliptic tại điểm S, lúc đó $R = P + Q = -S$.



Hình 2. *Phép toán trên các điểm của đường cong elliptic.*

Giả sử điểm $P \in E(\mathbb{F}q)$ thỏa mãn các điều kiện sau đây:

1. Là một điểm bậc *n*,
2. Bậc của *P* là một số nguyên tố,
3. Hai số *n* và *q* là các số nguyên tố cùng nhau.

Khi đó, bài toán logarit rời rạc trong nhóm <P> được định nghĩa như sau:

Cho trước một điểm *P* và điểm *Q* ∈<*P*> cần phải tìm số nguyên *l*, thỏa mãn phương trình *lP* = *Q*.

Hiện nay, phương pháp tốt nhất để giải bài toán này là thuật toán Pollard [7], thời gian thực hiện dự kiến khoảng O($\sqrt{n}$).Nếu n ≈ q, thì thời gian thực hiện của thuật toán trên theo cấp số nhân đối với log *q*. Cần lưu ý rằng, cũng có những

phương pháp khác trong việc giải bài toán logarit rời rạc, mà áp dụng cho từng loại đường cong cụ thể. Đặc biệt, có thể sử dụng phép nhân Weil và Tate để chuyển bài toán từ các nhóm điểm của đường cong sang nhóm nhân trên trường hữu hạn $\mathbb{F}_q^k$ *[6]*. Số *k* được gọi là mức độ nhúng của đường cong và được định nghĩa như sau.

Định nghĩa 3: Giả sử *E* là một đường cong elliptic xác định trên trường *𝔽q*, và *P ∈ E (𝔽q)* là điểm có bậc là số nguyên tố *n*. Nếu *USCLN (n, q) = 1*, thì mức độ nhúng của <*P*> là số nguyên *k* nhỏ nhất sao cho *n* $|q^k - 1$.

Nếu độ nhúng thấp, thì sử dụng phép nhân Weil, chúng ta có thể sử dụng các thuật toán tiểu hàm mũ cho việc tìm kiếm logarit rời rạc (phương pháp chỉ số), trong đó có thể tính nhanh trong $\mathbb{F}_q^k$ so với thuật toán Pollard trong <P>. Vì lý do này, trong mật mã bài toán logarit rời rạc trên đường cong elliptic chỉ sử dụng những đường cong có độ nhúng lớn.

Với đường cong elliptic với độ nhúng thấp cho phép thực hiện hiệu quả phép nhân Weil và Tate, điều đó dẫn đến các ánh xạ song tuyến.

2.3. Phép nhân Tate và thuật toán Miller

Cho *E* là một đường cong elliptic với hệ số thuộc trường $K = \mathbb{F}_q$ mô tả bởi phương trình Weierstrass *r(X,Y) = 0*. Hơn nữa, cho $\overline{K}$ là bao đóng đại số của trường *K*.

Một ước số trên *E* được gọi là tổng của các điểm trên đường cong $D = \sum_{P \in E} n_P(P)$ trong đó có nhiều nhất số lượng hữu hạn các hệ số n_p khác không. Tập hợp các điểm $P \in E$ với hệ số n_p khác không được gọi là giá của *D*. Ước được gọi là không nếu thỏa mãn điều kiện $\sum_{P \in E} n_P(P) = 0$. Chúng ta nói rằng một ước được xác định trên trường *K* nếu $D^\sigma = \sum_P n_p\left(P^\sigma\right) = D$ với mọi tự đồng cấu σ trường $\overline{K}$ sẽ đồng nhất trên *K*. Chúng ta chấp nhận rằng $P^\sigma=(\sigma(x)\sigma(y))$ nếu *P = (x, y)* và $\infty^\sigma=\infty$. Tập hợp tất cả các ước xác định trên trường *K* được ký hiệu là $\mathrm{Div}_K(E)$.

K(E) là ký hiệu trường các phân số *K[X,Y]/r(X,Y)*. Ước của hàm $f \in K(E)$ là tổng hình thức $div(f) = \sum_{P \in E} m_P(P)$, trong đó, m_p là số lần mà *P* tham gia vào phân bố *f* như là một hệ số (giá trị âm được áp dụng trong trường hợp của các cực). Các ước của hàm số thuộc *K(E)* được gọi là các ước chính. Định lý sau đây cho phép chính xác xác định chúng.

Định lý 1: Ước $D = \sum_{P \in E} n_P(P)$ là ước chính khi và chỉ khi:

$$\sum_{P \in E} n_P = 0 \text{ và } \sum_{P \in E} n_P(P)$$

Chúng ta nói rằng hai ước $D_1, D_2 \in Div_K(E)$ là tương đương nhau $D_1 \sim D_2$ nếu tồn tại một hàm hữu tỷ $f \in K(E)$ và $D_1=D_2+div(f)$. Nếu $f \in K(E)$ và $D = \sum n_P(P) \in Div_K(E)$ cùng có giá phân biệt, thì có thể định nghĩa *f(D)* là

$$f(D) = \prod_{P \in E} f(P)^{n_P}$$

2.3.1. Phép nhân Tate

Giả sử $|E(F_q)| = hn$, trong đó n là một số nguyên tố mà *UCLN (n, q) = 1*. Cho k là số nguyên nhỏ nhất khi $n \mid q^k - 1$. Tập hợp tất cả các điểm P ∈ E($\overline{K}$) thỏa mãn biểu thức $nP = \infty$ (các điểm bậc n) sẽ được ký hiệu là $E[n]$ (có thể chỉ ra rằng $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$). Ngoài ra, μ_n chúng ta ký hiệu nhóm con bậc n của nhóm $F_{q^k}^{\times}$.

Trước khi định nghĩa phép nhân Tate, chúng ta sẽ bổ sung thêm một vài giả định để đơn giản hóa cách mô tả. Cho $n \nmid q - 1$ (nghĩa là, $k>1$). Bởi vì $E[n] \subset E\left(\mathbb{F}_{q^k}\right)$ và $\left|E[n]\right| = n^2$, thì $n^2 \mid \left|E\left(\mathbb{F}_{q^k}\right)\right|$ và $n \nmid \left|E\left(\mathbb{F}_{q^k}\right)\right| / n^2$.

Định nghĩa 4: Cho $P,Q \in E[n]$, và cho f_p là một hàm thỏa mãn điều kiện $div(F_p) = n(P) - n(\infty)$ (f có n lần zero tại P và n lần cực tại ∞). Giả sử thêm rằng $R \in E[n]$ là điểm đáp ứng các điều kiện $R \notin \{\infty, P, -Q, P-Q\}$ và D_Q là ước được định nghĩa như sau $D_Q = (Q + R) - (R)$. Khi đó phép nhân Tatea được hiểu là phép ánh xạ

$$e : E[n] \times E[n] \to \mu_n$$

được định nghĩa như sau:

$$e(P,Q) = f_P(D_Q)^{(q^k-1)/n} = \left(\frac{f_P(Q+R)}{f_P(R)}\right)^{(q^k-1)/n}$$

Có thể chỉ ra rằng ánh xạ trên được lựa chọn đúng và không phụ thuộc vào sự lựa chọn của hàm $f_p$và điểm R. Ngoài ra, ánh xạ trên còn là ánh xạ song tuyến không suy biến.

2.3.2. Thuật toán Miller

Trong phần này, chúng ta mô tả các thuật toán Miller [9], cho phép tính toán một cách hiệu quả phép nhân Tate. Điều quan trọng của thuật toán này là cách thức tính hàm f_p với ước $n(P) - n(\infty)$.

Đối với mỗi $i \geq 1$, cho f là một hàm mà ước của nó bằng $div(f_i) = i(P) - (iP) - (i - 1)(\infty)$.

Với định nghĩa như vậy, chúng ta có $f_1 = 1$ và $f_n = f_P$. Bổ đề sau đây chỉ ra cách thức tính f_n một cách hiệu quả.

Bổ đề 1: Nếu $P \in E[n]$, l là một đường thẳng nối các điểm iP, jP, và v là đường thẳng đứng đi qua điểm $iP + jP$ thì $f_{i+j} = f_i f_j \frac{l}{\upsilon}$

Chứng minh: Bởi vì các đường thẳng l và v thể hiện các phép tính nhóm trên các điểm của đường cong E, do đó, chúng ta có thể viết

$$\begin{aligned}
&div\left(f_i f_j \frac{l}{\upsilon}\right) = div(f_i) + div(f_j) + div(l) - div(\upsilon)\\
&= (i(P) - (iP) - (i-1)(\infty)) + (j(P) - (jP) - (j-1)(\infty))\\
&\quad + ((iP) + (jP) + (-(i+j)(P)) - 3(\infty)) - (((i+j)(P)) + (-(i+j)(P)) - 2(\infty))\\
&= (i+j)(P) - (i+j)(P) - (i+j-1)(\infty)\\
&= div(f_{i+j})
\end{aligned}$$

Cho n = $(n_t, ..., n_1, n_0)_2$ sẽ là biểu diễn nhị phân của *n*. Hàm f_p có thể được tính toán hiệu quả bằng phép cộng và nhân hai khi dịch chuyển các bit liên tiếp số *n* từ trái sang phải.

Khi xác định phép nhân Tate chỉ cần tìm giá trị hàm f_p ở các điểm $Q+R$ và R. Do đó, thuật toán Miller chỉ xác định tại mỗi lần lặp giá trị f_i ở những điểm trên.

1. Cho $n = (n_t, ..., n_1, n_0)_2$ sẽ là biểu diễn nhị phân của *n*.
2. Chọn điểm $R \in E[n] \setminus \{\infty, P, -Q, P-Q\}$.
3. Giả định $f \leftarrow 1$, $T \leftarrow P$.
4. Đối với *i* từ *t* đến *0* thực hiện:
   (a) Xác định đường thẳng *l* tiếp tuyến với đường cong tại điểm *T*.
   (b) Kẻ đường thẳng đứng v dọc đi qua điểm *2T*.
   (c) $T \leftarrow 2T$.
   (d) $f \leftarrow f^2 \cdot \frac{l(Q+R)}{\upsilon(Q+R)} \cdot \frac{\upsilon(R)}{l(R)}$
   (e) Nếu $n_i = 1$ thì
      i. Thiết lập đường thẳng *l* đi qua các điểm *P* và *Q*.
      ii. Thiết lập đường thẳng đứng *v* đi qua điểm $T + P$.
      iii. $T \leftarrow T + P$.
      iv. $f \leftarrow f \cdot \frac{l(Q+R)}{\upsilon(Q+R)} \cdot \frac{\upsilon(R)}{l(R)}$
5. Tính $f^{(q^k-1)/n}$

Ví dụ: Giả sử chọn đường cong E: $y^2 = x^3 + 1$ trên F_{101}. Khi đó, $\left|E\left(F_{101}\right)\right| = 101+1 = 2 \cdot 3 \cdot 17$. Với*n*=17 ta có*k* = 2. Ta viết $F_{101^2} = F_{101}(\theta)$, trong đó, $\theta^2 = -2$. Cho $P = (87, 61)$ (bậc của nó bằng*n* = 17) vàQ = (48, θ) (bậc của Q bằng 102). Đặt $D = \left([2]Q\right) - (Q)$. Ta tính các giá trị sau:

i	$f_i(D)$	*i*	$f_i(D)$
1	1	8	$46+18\theta$
2	$52+56\theta$	16	$22+43\theta$
4	$53+3\theta$	17	$74+62\theta$

Như vậy, $\langle P,Q\rangle_{17} = 74 + 62\theta$. Tính được $\left(q^k - 1\right)/n = (101^2 - 1)/17 = 600$. Vậy giá trị *f* cuối cùng tính được là $93+25\theta \in \mu_{17}$.

Đáng tiếc là phép nhân Tate không thỏa mãn một trong các giả thiết mà chúng ta yêu cầu đối với ánh xạ song tuyến - nhóm *E [n]* không phải là nhóm cyclic. Để giải quyết vấn đề này, hãy tìm các tự đồng cấu: $\Psi : E \to E$ mà $\Psi(P) \notin \langle P \rangle$. Khi đó, ánh xạ $\hat{e}(Q,P) = e(Q, \Psi(Q))$ sẽ thỏa mãn các điều kiện đặt ra cho một ánh xạ song tuyến.

3. CÁC GIAO THỨC MẬT MÃ SỬ DỤNG ÁNH XẠ SONG TUYẾN

3.1. Thoả thuận khóa mã một vòng dùng cho ba bên

Giả sử rằng có thể tính toán một cách hiệu quả ánh xạ song tuyến trên nhóm G_1 và G_T, trong đó, bài toán song tuyến Diffie-Hellman là bài toán khó. Ánh xạ đó là cơ sở để thực hiện giao thức thỏa thuận khóa mã một vòng cho ba bên:

1. Bên A chọn ngẫu nhiên một số $a \in [0, n - 1]$, tính aP và gửi cho các bên B, C.

2. Bên B chọn ngẫu nhiên một số $b \in [0, n - 1]$, tính bP và gửi cho các bên A, C.

3. Bên C chọn ngẫu nhiên một số $c \in [0, n - 1]$, tính cP và gửi cho các bên A, B.

Có thể thấy rằng sau vòng này, tất cả những người tham gia có thể tự mình tạo ra một khóa mã bí mật chung.

	Bên A	Bên B	Bên C
Đã có	a, bP và cP	b, aP và cP	c, aP và bP
Cần tính	$K = \hat{e}(bP,cP)^a = \hat{e}(P,P)^{abc}$	$K = \hat{e}(aP,cP)^b = \hat{e}(P,P)^{abc}$	$K = \hat{e}(aP,bP)^c = \hat{e}(P,P)^{abc}$

Phân tích sơ đồ trên có thể đặt ra câu hỏi: Liệu có khả năng xây dựng ánh xạ đa tuyến $\hat{e}_l: G^{l-1}{}_l \rightarrow G_T$. Và từ ánh xạ đó có thể tạo lập giao thức thỏa thuận khóa mã một vòng cho l người tham gia. Câu hỏi về sự tồn tại của ánh xạ đa tuyến như vậy hiện nay vẫn còn là bài toán mở.

3.2. Mật mã dựa trên định danh

Trong [10], Shamir đã đề xuất khái niệm về mật mã dựa trên định danh để giải quyết các vấn đề phát sinh trong quản lý chứng chỉ. Đề xuất Shamir giả định:

1. Khóa công khai của người dùng là định danh của họ (ví dụ như địa chỉ email).

2. Sẽ có một bên thứ ba đáng tin cậy chịu trách nhiệm cho việc tạo ra các khóa bí mật cho người sử dụng.

3. Mã hóa có thể được thực hiện ngay cả trước khi tạo khóa riêng của người sử dụng (Phép mã hóa chỉ yêu cầu định danh (ID) của người dùng và khóa công khai của một bên thứ ba tin cậy).

Đề xuất của Shamir đã phải chờ đến khi Boneh và Franklin [4] đề xuất sơ đồ mã hóa định danh (ID) dựa trên ánh xạ song tuyến mới được thực hiện. Sơ đồ này giả định rằng:

1. Chúng ta thực hiện một ánh xạ song tuyến $\hat{e}: G_1 \rightarrow G_T$, mà bài toán song tuyến Diffie-Hellman là bài toán tính toán khó.

2. Tồn tại hàm băm H_1 và H_2, sao cho:

$H_1: \{0, 1\}^* \rightarrow G_1 \setminus \{\infty\}$ và $H_2: G_T \rightarrow \{0, 1\}^l$.

trong đó, l là số bit của bản rõ.

3. Bên thứ ba tin cậy cung cấp khóa riêng $t \in [0, n-1]$ và khóa công khai $T = tP$ (khóa T được phổ biến rộng rãi).

Khi một người dùng cần có một khóa riêng d_A, thì bên thứ ba tin cậy cấp một mã định danh ID_A, tính khóa $d_A = tQ_A = tH_1(ID_A)$ và gửi qua một kênh an toàn cho người dùng. Chú ý rằng khóa riêng d_A có thể được coi là một chữ ký của bên thứ 3 tin cậy vào mã dạng ID_A.

Để mã hóa một thông điệp $m \in \{0, 1\}^l$ sử dụng sơ đồ Boneh-Franklin, phải làm như sau:

1. Thiết lập một khóa công khai dựa trên mã định danh$Q_A = H_1(ID_A)$.

2. Chọn một số ngẫu nhiên $r \in [0, n - 1]$ và tính toán $R = rP$.

3. Tạo bản mã $c = m \oplus H_2(\hat{e}(Q_A,T)^r)$.

4. Gửi cặp (R, c) cho người nhận.

Để giải mã một thông điệp của người dùng sử dụng khóa riêng của mình $d_A$và tính toán ra bản rõ $m = c \oplus H_2(\hat{e}(d_A, R))$. Quá trình giải mã thông điệp đúng nhờ vào đẳng thức sau:

$$\hat{e}(d_A,R) = \hat{e}(tQ_A, rP) = \hat{e}(Q_A, P)^{tr} = \hat{e}(Q_A, tP)^r = \hat{e}(Q_A, T)^r.$$

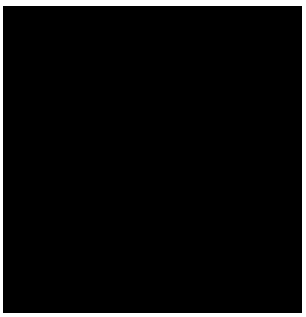
Để nhận được thông điệp từ bản mã (R, c) cần tính $(Q_A, T)^r$ trên cơ sở (P, Q_A, T, R) và đó là bài toán song tuyến DH.

Cần nhấn mạnh rằng phương pháp mô tả trên chống được tấn công thụ động, nhưng lại dễ bị tấn công bản mã lựa chọn. Tuy nhiên, có thể cải tiến để loại bỏ vấn đề này.

4. MỘT VÀI KẾT QUẢ THỬ NGHIỆM THỰC TẾ

Trên cơ sở các kết quả lý thuyết nói trên chúng tôi đã xây dựng một phần mềm bảo mật thông tin trên đường truyền sử dụng phương pháp trao đổi khóa mã an toàn và một số ứng dụng của Hệ mật trên đường cong elliptic có tích hợp nghiệp vụ mật mã. Các kết quả thử nghiệm thực tế cho thấy phần mềm hoạt động tốt, ổn định, có độ bảo mật cao (hình 3, 4, 5).

Hình 3. *Ảnh gốc trước khi mã hóa.*



Hình 4. *Ảnh giải mã với khóa sai.*

Hình 5. *Ảnh sau khi giải mã.*

5. KẾT LUẬN

Bài viết này trình bày một cơ chế mật mã mới dựa trên ánh xạ song tuyến, trong đó có thể thực hiện bằng cách ghép cặp điểm trên đường cong elliptic. Đã chỉ ra khả năng ghép cặp điểm trên đường cong cho phép xây dựng các giao thức như: thỏa thuận khóa một vòng giữa ba bên và mã hóa dựa trên định danh. Các kết quả trên có sự hợp tác với đề tài VAST01.06/15-16 của Viện Hàn lâm Khoa học và Công nghệ Việt Nam.

Cần nhấn mạnh rằng lĩnh vực mật mã học hiện đang ở một giai đoạn phát triển rất chuyên sâu. Một số lớn kết quả được công bố liên quan đến khả năng sử dụng thực tế phép nhân Tate; thuật toán Miller và phương pháp ghép cặp điểm trên đường cong.

TÀI LIỆU THAM KHẢO

[1]. ANSI X9.62-2005 (2005), *"Public Key Cryptography For The FinancialServicesIndustry: The Elliptic Curve Digital Signature Algorithm(ECDSA)"*, American National Standards Institute.

[2]. ANSI X9.63 (1999), *"Public Key Cryptography For The FinancialServices Industry: Key Agreement and Key Transport Using ECC"*, American National Standard Institute.

[3]. A. Joux, *"A one round protocol for tripartite Diffie-Hellman"*, Algorithmic Number Theory: 4thInternational Symposium, pp. 263–267, 2000.

[4]. D. Boneh, M. Franklin, *"Identity-based encryption from the Weil pairing"*, *Advances in Cryptology– CRYPTO 2001*, pp. 586–615, 2001.

[5]. D. Boneh, B. Lynn, H. Shacham, *"Short signatures from the Weil pairing"*, *Advances in Cryptology– ASIACRYPT 2001*, pp. 297–319, 2001.

[6]. Lawrence C. Washington (2008), *"Elliptic Curves–Number theory and Cryptography"*, CRC Press.

[7]. J. Pollard, *"Monte Carlo methods for index computation mod p"*, Mathematics of Computation, pp.918–924, 1978.

[8]. A. Menezes, T. Okamoto, S. Vanstone, *"Reducing elliptic courve logarithms to logarithms in a finitefield"*, IEEE Transactions on Information Theory, pp. 1639–1646, 1993.

[9]. V. Miller, *"The Weil pairing, and its efficient calculation"*, Journal of Cryptology, pp. 235–261, 2004.

[10]. A. Shamir, *"Identity-based cryptosystems and signature schemes",* Advances in Cryptology ‑CRYPTO 84, pp. 47‑53, 1984.

ABSTRACT

A METHOD FOR SECURITY KEY AGREEMENT

The rapid development of cryptography promotes data security and user authentication techniques, information confidentiality... In the paper, a method for security key agreement and new applications of the Cryptosystem on the elliptic curve is presented.

Keywords: Elliptic curve, Information security, Data security, Diffie-Hellman, Bilinear.

Nhận bài ngày 01 tháng 3 năm 2017
Hoàn thiện ngày 04 tháng 4 năm 2017
Chấp nhận đăng ngày 05 tháng 4 năm 2017

Địa chỉ: [1]Học viện Kỹ thuật Mật mã;
[2]Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam.
[*]Email: nam_haivn@yahoo.com