Chọn miền tham số cho đường cong Elliptic sử dụng làm mã bảo mật cho hệ thống DNS

Selecting Domain Parameters for Elliptic Curve in Enscrypting Codes for DNS System

Trần Minh Tân và Nguyễn Văn Tam

Abstract: *Besides RSA algorithms are widely used, elliptic curve cryptography (ECC) has been currently studied and just applied in security with outstanding advantages of shorter key length. To enhance the safety in using ECC, a list of domain parameters has been applied for minimizing attack possibilities. In this paper, we introduce algorithm creating domain parameters and elliptic curves that meet security requirements, preventing scan-based attacks on elliptic curve cryptography for application in DNS system's security.*

Keywords: *Elliptic Curve Cryptography, ECC, ECDLP.*

I. GIỚI THIỆU

Sau khi Neal Koblitz và Victor Miller đưa ra những công bố về hệ mật dựa trên đường cong Elliptic (Elliptic Curve Cryptography - ECC) vào năm1985, ECC đã được các nhà khoa học quan tâm nghiên cứu và bước đầu triển khai ứng dụng thực tế, đặc biệt là trên các thiết bị di động. Với cùng một mức độ bảo mật như nhau so với RSA nhưng ECC yêu cầu độ dài khóa ngắn hơn nhiều [1]. Ngoài các hệ thống di động, việc nghiên cứu mở rộng ứng dụng ECC trong các hệ thống khác và trong việc xây dựng các lược đồ chữ ký số cũng đang được tiến hành song song. Nhằm đáp ứng các nhu cầu mở rộng ứng dụng ECC nêu trên, hàng loạt các nghiên cứu, cải tiến hệ mật dựa trên đường cong Elliptic đã được triển khai trong thời gian vừa qua.

Trong [2,14], các tác giả đã trình bày những cải tiến thuật toán về phép nghịch đảo và nhân vô hướng để giảm thời gian tính toán, phòng tránh các tấn công về phía kênh, dò tìm khoá mã ECC. Trong [3], Yan Hu, Yan-yan Cui và Tong Li đã trình bày thuật toán chọn điểm cơ sở G để áp dụng cho đường cong Elliptic. Bên cạnh đó, việc sử dụng dạng không kề cận (NAF) và phương pháp cửa sổ trượt để cải tiến tốc độ của phép nhân trong ECC đã được trình bày bởi các tác giả Shouzhi Xu, Chengxia Li, Fengjie Li và Shuibao Zhang[4]. Việc cải tiến, đơn giản hoá các thuật toán tạo khoá, trao đổi khoá, mã hoá, giải mã trên ECC cũng đã được đề cập trong [5] để làm giảm số bước tính toán, tăng tốc độ ký xác thực, mã hoá, giải mã mà vẫn đáp ứng các yêu cầu về mức bảo mật.

Tuy nhiên, ngoài các kết quả nghiên cứu đã nêu ở trên, để làm tăng khả năng bảo mật của ECC thì bản thân việc chọn được một đường cong tốt với miền các tham số phù hợp đã đảm bảo loại trừ được phần lớn những nguy cơ bị tấn công có thể xảy ra. Và thực tế, bước đầu tiên trong việc ứng dụng hệ mật dựa trên đường cong Elliptic cho mỗi hệ thống bao giờ cũng là việc hai bên gửi, nhận phải thống nhất được đường cong Elliptic sẽ sử dụng, có nghĩa là cần phải xác định các tham số phù hợp của đường cong, sau đó mới đến tạo đường cong Elliptic đạt mức bảo mật xác định.

Có hai loại miền tham số khác nhau, một loại gắn với đường cong Koblitz, còn loại kia chọn có thể kiểm tra ngẫu nhiên. Trong [7], các tác giả cũng đã đưa ra một số khuyến nghị về lựa chọn các tham số cụ thể cho đường cong Koblitz. Theo các công bố của Viện Tiêu chuẩn quốc gia Hoa Kỳ [9], miền tham số của đường cong Elliptic có thể kiểm tra được với các đặc điểm về khả năng tự bảo vệ, các tham số có thể chọn

theo ANSIX962. IEEE cũng đã đưa ra bản nháp tiêu chuẩn IEEE1363 về miền tham số Elliptic sử dụng trong Internet[8]. Về cơ bản, các cách lựa chọn miền tham số cho đường cong Elliptic hiện tại đang được áp dụng theo phương pháp lặp ngẫu nhiên và đếm số điểm trên đường cong tương ứng cho đến khi tìm được các tham số thích hợp [7,8].

Bài báo này chúng tôi đưa ra thuật toán chọn miền tham số đường cong Elliptic và xây dựng đường cong Elliptic trên trường số nguyên tố hữu hạn, khắc phục việc đếm ở trên mà vẫn đảm bảo mức bảo mật đã cho đồng thời hạn chế được các nguy cơ bị tấn công đã được liệt kê, áp dụng vào việc bảo mật trong quá trình trao đổi dữ liệu tên miền (zone transfer) giữa máy chủ tên miền DNS chính (Primary DNS) và các máy chủ DNS phụ (secondary DNS) trong hệ thống DNS.

Các nội dung tiếp theo của bài báo: Phần 2 chúng tôi trình bày phát biểu bài toán và đề xuất thuật toán cải tiến chọn miền tham số cho đường cong Ellitic và tạo đường cong Elliptic trên trường số nguyên tố. Phần 3 trình bày kết quả thực nghiệm áp dụng các thuật toán cải tiến đã đề xuất vào quá trình mã hoá, giải mã trên các file dữ liệu tên miền trên máy chủ DNS cấp quốc gia ".vn". Cuối cùng, phần 4 là một số kết luận.

II. PHÁT BIỂU BÀI TOÁN

1. Đường cong Elliptic

1.1. Đường cong Elliptic (E) trong trường nguyên tố hữu hạn

Đường cong Elliptic trong trường nguyên tố hữu hạn $E(F_q)$ được biểu diễn dưới dạng:

$$y^2 = x^3 + ax + b \qquad (1)$$

trong đó:

1. Đồng nhất: $P + \infty = \infty + P = P$ với $\forall P \in E(k)$

2. Nếu $P= (x, y) \in E(k)$ thì $(x, y) + (x, -y)= \infty$

Điểm $(x, -y)$ ký hiệu là $-P$ gọi là điểm âm của P.

3. Cộng điểm:

Nếu $P= (x_1, y_1) \in E(k)$ và $Q= (x_2, y_2) \in E(k)$,

ở đây $P \neq \pm Q$ thì $P + Q = (x_3, y_3)$ với:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

4. Nhân đôi điểm:

Giả sử $P= (x_1, y_1) \in E(k)$, ở đây $P \neq -P$ thì

$2P= (x_3, y_3)$, với:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

1.2. Đường cong Elliptic trong trường nhị phân $E(F_2^m)$

Đường cong Elliptic trong trường nhị phân được biểu diễn dưới dạng:

$$y^2 + xy = x^3 + ax^2 + b \qquad (2)$$

trong đó:

1. Đồng nhất: $P + \infty = \infty + P = P$ với $\forall P \in E(F_2^m)$

2. Nếu $P= (x, y) \in E(F_2^m)$ thì $(x, y)+(x, x+y)= \infty$. Điểm $(x, x+y)$ ký hiệu là $-P$ và gọi là điểm âm của P.

3. Cộng điểm:

Giả sử $P= (x_1, y_1) \in E(F_2^m)$

và $Q= (x_2, y_2) \in E(F_2^m)$,

ở đây $P \neq \pm Q$ thì $P + Q = (x_3, y_3)$ với:

$$x_3= \lambda^2 + \lambda + x_1 + x_2 + a$$

$$y_3= \lambda(x_1 + x_3) + x_3 + y_1$$

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}$$

4. Nhân đôi điểm:

Giả sử $P= (x_1, y_1) \in E(F_2^m)$, ở đây $P \neq -P$ thì: $2P= (x_3, y_3)$, với:

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2}$$

$$y_3 = x_1^2 + \lambda x_3 + x_3$$

$$\lambda = \frac{x_1 + y_1}{x_1}$$

1.3. Miền tham số của đường cong Elliptic

Miền tham số của đường cong Elliptic [6] được xác định bởi:

D= (q, FR, S, a,b, P, n, h) (3)

Với:

- q là bậc của trường.
- FR: biểu diễn trường mà đường cong E được xác định trên đó.
- S: tham số phù hợp với thuật toán chọn ngẫu nhiên đường cong E.
- a, b là các hệ số của phương trình đường cong (1).
- P = (x_P, y_P) ∈ E(F_q) trong tọa độ Affine. P còn gọi là điểm cơ sở.
- n là bậc của P
- h: hệ số h= #E(F_q)/n

Trong phạm vi của bài báo, chúng tôi sẽ tập trung vào xét đường cong Elliptic trong trường số nguyên tố. Theo đó, các tham số mô tả đường cong E được xác định trên trường hữu hạn F_q với điểm cơ sở P ∈ E(F_q) và bậc của nó là n.

2. Phương pháp chọn đường cong Elliptic ngẫu nhiên - Neal Koblitz [15]

Để xác định được đường cong Elliptic sử dụng làm mã bảo mật, Neal Koblitz đã đưa ra thuật toán lựa chọn đường cong phù hợp với phương trình đường cong đã nêu ở trên. Theo Neal Koblitz, việc chọn ngẫu nhiên đường cong Elliptic trên trường F_q (với q lớn) được thực hiện như sau:

1. Chọn ngẫu nhiên 3 phần tử từ F_q là x, y, a.
2. Tính b = y^2 - (x^3 + ax).
3. Kiểm tra $4a^3 + 27b^2 \neq 0$ để đảm bảo phương trình x^3 + ax + b = 0 không có nghiệm kép.
4. Nếu điều kiện trên không thoả mãn thì quay lại bước 1.
5. Còn lại, đặt P = (x,y) và đường cong $y^2 = x^3 + ax + b$ là đường cong cần chọn.

3. Yêu cầu chọn các tham số cho đường cong Elliptic

Mặc dù phương pháp chọn ngẫu nhiên nêu ở trên đảm bảo là chọn được một đường cong Elliptic và sử dụng chính tính ngẫu nhiên là một yếu tố bảo mật. Tuy nhiên với các yêu cầu cao hơn, ta sẽ phải chọn các tham số sao cho ECDLP (Elliptic Curve Discrete Logarithm Problem) hạn chế được các tấn công thông thường đã biết [10]. Các tham số bao gồm một nhóm các thực thể, trừ một số trường hợp đặc biệt mỗi người dùng có thể xác định riêng. Theo [10] thì các yêu cầu để hạn chế những tấn công đã được liệt kê như sau:

- Để tránh dạng tấn công Pohlig- Hellman và tấn công Pollard's rho, đối với ECDLP cần chọn #E(F_q) có thể chia hết được cho một số nguyên tố *n* đủ lớn, tối thiểu cũng thỏa mãn $n > 2^{160}$. Với trường F_q cố định, để hạn chế đến mức cao nhất các tấn công Pohlig- Hellman và Pollard's rho thì phải chọn *E* sao cho số #E(F_q) chia hết cho một số nguyên tố lớn, #E(F_q) = *hn* với *n* là số nguyên tố lớn và *h* là nhỏ (*h*= 1, 2, 3 hoặc 4).
- Để tránh tấn công đối với các đường cong kỳ dị của trường số nguyên tố, người ta chọn #E(F_q)≠ q.
- Để tránh tấn công cặp Weil và Tate thì phải đảm bảo rằng *n* không chia hết cho q^k-1 với 1≤k≤*c* trong đó *c* là một số đủ lớn sao cho DLP trong $F_q^* c$ có thể coi là khó giải; nếu $n > 2^{160}$ thì *c*= 20 là đủ.
- Để chống lại các cuộc tấn công đối với một số lớp đường cong đặc biệt thì nên chọn ngẫu nhiên *E* với điều kiện #E(F_q) có thể chia hết cho một số nguyên tố lớn.

Mặc dù vậy, các yêu cầu nêu trên chỉ mới là những khuyến cáo chi tiết cho tham số cần chọn lựa, chưa

phải là thuật toán chọn tham số hay chọn miền tham số cho đường cong Elliptic.

Ngoài phương pháp chọn đường cong Elliptic của Neal Koblitz (nguyên bản năm 1985 và phiên bản mới năm 2008 theo tài liệu [15]), năm 2003 các tác giả Yasuyuki Nogami, Yoshitaka Morikawa mới đề cập đến việc tạo đường cong elliptic trên trường Fq^m với số mũ bậc chẵn [16], năm 2004 có thêm các tác giả Mykola Karpynskyy, Ihor Vasyltsov, Ihor Yakymenko và Andrij Honcharyk trình bày về cách tạo tham số cho đường cong Elliptic dựa trên đặc trưng Jacobi và phép bình phương [17], nhưng chưa có một phương án chọn miền tham số cho đường cong kế thừa toàn bộ các kết quả nghiên cứu phương thức chống tấn công thường gặp đã nêu ở trên. Trong [5], chúng tôi đã đề cập một số cải tiến trong các thuật toán tạo khoá, trao đổi khoá, mã hoá và giải mã trên đường cong Elliptic, tuy nhiên vẫn chưa đề cập đến các bước lựa chọn miền tham số, tạo đường cong Elliptic mà hai bên sẽ thống nhất áp dụng cho các thuật toán tạo khoá, trao đổi khoá, mã hoá và giải mã này. Sau đây chúng tôi trình bày các thuật toán cải tiến chọn miền tham số cho đường cong Elliptic sử dụng làm mã bảo mật, thỏa mãn các yêu cầu chọn tham số nói trên.

4. Thuật toán 1: Chọn miền tham số cho đường cong Elliptic

Đầu vào: Bậc của trường q, FR với F_q, mức bảo mật L thỏa mãn đồng thời $2^L \geq 4\sqrt{q}$ và $160 \leq L \leq \lfloor \log_2 q \rfloor$ (để đảm bảo rằng $n>2^{160}$, $2^L \leq q$).

Đầu ra: Miền tham số D= (q, FR, S, a, b, P, n, h)

1. Chọn a, b $\in F_q$ (có thể kiểm tra ngẫu nhiên bằng cách sử dụng thuật toán 2 đề cập bên dưới).

2. Tính

- N= $\#E(F_q)$ = q+1-t; t là mức bảo mật yêu cầu.
- Hoặc N= $\#E(Fq^m)= q^m +1-V_m$ trong Fq^m, $\forall m\geq 2$; trong đó $V_0=2$, $V_1= t$, $V_m=V_1V_{m-1} - qV_{m-2}$ được xác định với $m\geq 2$.

3. Kiểm tra N có thể chia hết cho số nguyên tố lớn *n* không (với $n > 2^L$). Nếu không, quay lại bước 1.

4. Kiểm tra $n \neq q-1$ (để đảm bảo rằng *n* không chia hết cho q^k -1 với $1\leq k\leq 20$ (tránh trường hợp đặc biệt khi mức bảo mật t=2, k=1 dẫn đến n=N=q-1)).

Nếu điều kiện không thỏa mãn thì quay lại bước 1.

5. Kiểm tra $n \neq q$. Nếu không thì quay lại bước 1.

6. Đặt $h \leftarrow N/n$.

7. Chọn điểm bất kỳ $P' \in E(F_q)$ và đặt P= h. P', lặp lại cho đến khi $P \neq \infty$.

8. Đưa ra (q, FR, S, a, b, P, n, h).

Tiếp theo, chúng tôi đưa ra thuật toán tạo đường cong E trên trường số nguyên tố.

5. Thuật toán 2: Tạo đường cong Elliptic trên trường số nguyên tố

Đầu vào: Số nguyên tố p > 3, hàm băm H- *l* bit.

Đầu ra: S, a, b $\in F_p \Rightarrow$ xác định đường cong E

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

1. Đặt $t \leftarrow \lceil log_2 p \rceil$, $s \leftarrow \lfloor (t-1)/l \rfloor$, $v \leftarrow t- sl$

2. Chọn chuỗi bít bất kỳ S có độ dài $g \geq l$ bit.

3. Tính h= H(S) và đặt r_0 là chuỗi bit dài *v* bit bằng cách lấy *v* bit tận cùng bên phải của h.

4. Đặt R_0 là dãy bit có được bằng cách lấy bit tận cùng bên trái từ r_0 đến 0.

5. Đặt z là số nguyên mà biểu diễn nhị phân của nó là S.

6. Với i từ 1 đến s, thực hiện:

   a. Đặt S_i là biểu diễn nhị phân bit g của số nguyên (z+ i) mod 2^g

   b. Tính $R_i = H(s_i)$

7. Đặt $R = R_0||R_1||\ldots||R_s$.

8. Đặt r là số nguyên mà biểu diễn nhị phân của nó là R.

9. Nếu r= 0 hoặc nếu $4r + 27 \equiv 0 \pmod p$ thì trở lại bước 2.

10. Chọn a, b $\in$ Fb bất kỳ, không đồng thời bằng 0 sao cho $r. b^2 = a^3 \pmod p$.

11. Đưa ra (S, a, b).

Nhận xét: Với các thuật toán đã đề xuất, cách tạo miền tham số, tạo đường cong đã nêu ở trên đáp ứng yêu cầu các tham số được tạo ra là ngẫu nhiên, đảm bảo tính bí mật. So với các phương pháp đã có [15,16,17] thì phương pháp này đã được cải tiến bằng cách đưa thêm việc kiểm tra, loại trừ các miền tham số có khả năng dẫn đến dễ bị tấn công đối với hệ mật dựa trên đường cong Elliptic và khắc phục việc phải đếm số điểm trên đường cong như đã nêu trong [7], [8] bằng cách chỉ tính một lần duy nhất tổng số điểm trên đường cong elliptic thông qua công thức đã xác định trước. Bằng cách kiểm tra, loại trừ những miền tham số không phù hợp, chọn ra các tham số thỏa mãn yêu cầu chống tấn công như đã nói ở mục 3, hệ mật dựa trên đường cong Elliptic chọn được không những hạn chế được tấn công cặp Weil và Tate mà còn hạn chế được các dạng tấn công Pohlig- Hellman, tấn công Pollard's rho, tấn công đối với một số lớp đường cong đặc biệt và với các đường cong kỳ dị của trường số nguyên tố.

III. KẾT QUẢ THỰC NGHIỆM

Trên cơ sở những cải tiến theo các thuật toán 1 và thuật toán 2 đã đề xuất, chúng tôi sử dụng ngôn ngữ lập trình Java để cài đặt chương trình chọn miền tham số, tạo đường cong Elliptic sau đó áp dụng vào quá trình tạo khoá và mã hoá, giải mã đã được đề cập trong [5]. Chương trình được chạy thử nghiệm trên các dữ liệu tên miền ".vn" lấy trực tiếp về từ hệ thống máy chủ DSN quốc gia (các zone file lưu giữ những bản ghi tên miền ".vn"). Đồng thời, chúng tôi cũng cài đặt thêm thuật toán chọn đường cong Elliptic theo phương pháp ngẫu nhiên của Neal Koblitz và triển khai các thuật toán tạo khoá, mã hoá, giải mã trong [5] trên đường cong chọn được theo phương pháp này trên cùng bộ dữ liệu tên miền đã được đem ra thử nghiệm theo thuật toán cải tiến nêu trên, so sánh thời gian thực hiện đã thu được bằng cả hai phương pháp. Mục tiêu của thực nghiệm nhằm đánh giá tính khả thi về thời gian xử lý thực của giải pháp mới là có thể chấp nhận được hay không để áp dụng vào quá trình trao đổi dữ liệu tên miền (zone transfer) giữa máy chủ DNS chính (Primary DNS) và các máy chủ DNS phụ (secondary DNS).

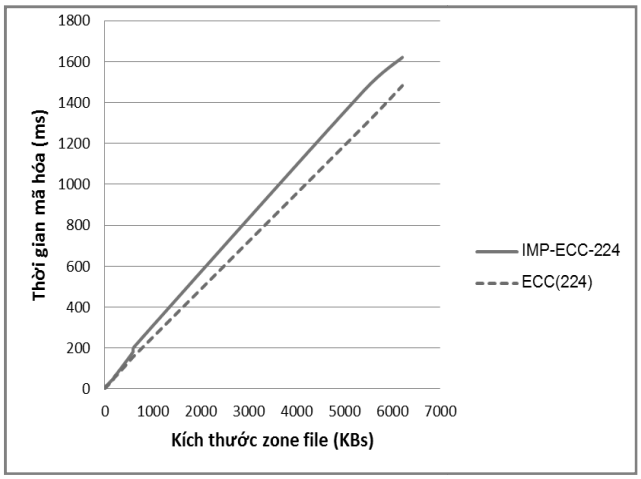
Chương trình được thực hiện trên máy tính Intel(R) Core (TM) i5, 3.10 GHz, 3.2 GB RAM, chạy hệ điều hành Window 7.0, 32 bit. Dữ liệu thử nghiệm trên 16 loại zone file tên miền thực tế, được lấy về từ hệ thống máy chủ DNS quốc gia ".vn" với các kích thước khác nhau. Độ dài khoá mã thử nghiệm cho cả hai phương pháp được chọn là 224 bit. Kết quả chi tiết được so sánh trong Bảng 1, theo đó tổng thời gian thực hiện bằng phương pháp sử dụng thuật toán ECC cải tiến chênh lệch lâu hơn không đáng kể so với thuật toán cũ. Độ trễ này là chấp nhận được khi đổi lại là việc đáp ứng được yêu cầu tăng mức độ bảo mật cho hệ mật dựa trên đường cong Ellitic, chống các tấn công dò tìm khoá.

Để đánh giá, so sánh tổng thể với các giải pháp bảo mật hiện có đang được áp dụng trên hệ thống DNS, chúng tôi thử nghiệm thêm quá trình mã hoá, giải mã bằng mã bảo mật RSA trong công nghệ DNSSEC hiện tại, độ dài mã khóa thử nghiệm được đặt là 2048 bit cho đảm bảo có cùng một mức bảo mật với ECC-224 bit (ECC-224 và RSA-2048 có cùng một mức độ bảo mật [6]). Kết quả thời gian mã hóa, giải mã bằng RSA-2048 thu được được đem so sánh với tổng thời gian thực hiện cả quá trình chọn miền tham số cho đến tạo đường cong, mã hoá, giải mã bằng thuật toán ECC cải tiến đã thử nghiệm ở trên. Chi tiết nêu trong Bảng 1.

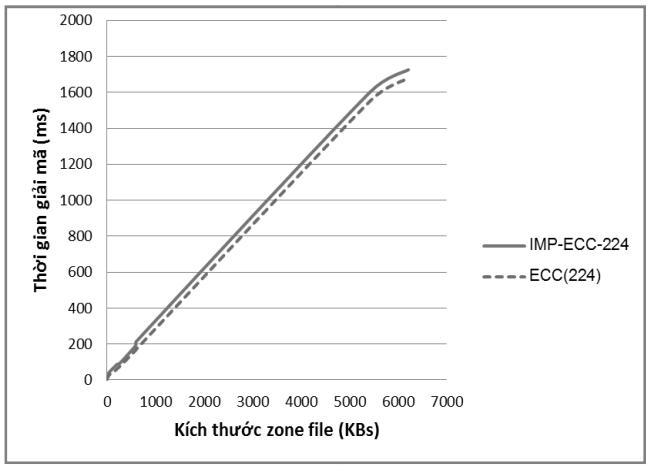
Tổng hợp kết quả thực nghiệm về thời gian mã hoá, giải mã bằng thuật toán ECC cải tiến (IMP-ECC-224 bit) và mã hoá, giải mã bằng ECC-224 sau khi chạy chương trình trên những zone file có biến động kích thước được lấy trên máy chủ DNS quốc gia liên tiếp với tần suất 02 lần/ngày trong 30 ngày liên tục được thể hiện chi tiết trên các biểu đồ trong Hình 1 và Hình 2. So sánh thời gian mã hóa, giải mã bằng ECC cải tiến (IMP- ECC-224 bit) và bằng RSA-2048 bit cùng mức độ bảo mật được thể hiện trên các biểu đồ trong Hình 3 và Hình 4.

Bảng 1. Tổng hợp số liệu so sánh tổng thời gian thực hiện mã hoá và giải mã các zone file tên miền .VN bằng ECC-224 bit, ECC cải tiến (IMP-ECC-224 bit) và bằng RSA-2048 bit.

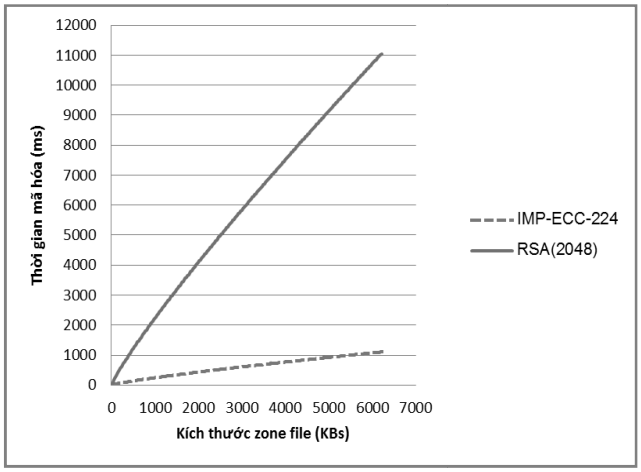
Zone File	Kích thước zone file (bytes)	Thời gian mã hoá (ms)			Thời gian giải mã (ms)		
		ECC 224 bit	IMP-ECC 224 bit	RSA- 2048 bit	ECC 224 bit	IMP-ECC 224 bit	RSA-2048 bit
.int.vn	2 948	2	4	10	4	6	130
.vinhlong.vn	3 521	3	5	20	5	8	159
.danang.vn	3 598	3	6	24	6	8	170
.health.vn	5 356	4	8	37	10	13	230
.ac.vn	9 867	7	10	40	13	17	420
.hanoi.vn	13 628	8	13	63	16	21	570
.biz.vn	26 280	9	15	70	17	26	1 080
.pro.vn	30 263	10	16	70	19	30	1 270
.info.vn	37 757	11	17	90	27	41	1 570
.gov.vn	175 234	45	50	420	54	79	7 461
.org.vn	204 457	57	62	480	62	86	8 761
.net.vn	268 805	71	80	630	77	95	11 750
.name.vn	594 418	158	183	1 390	167	193	29 560
.edu.vn	605 695	160	204	1 400	185	215	30 200
.com.vn	5 423 158	1 290	1 463	12 481	1 553	1 603	1 035 543
vn.root	6 208 944	1 483	1 621	14 200	1 679	1 726	1 446 351



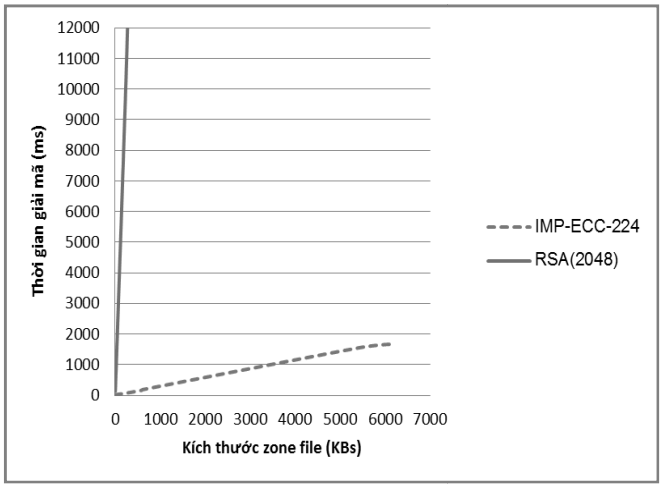
Hình 1. So sánh thời gian mã hoá theo thuật toán ECC cải tiến (IMP-ECC-224 bit) và theo cách chọn đường cong của Neal-Koblitz (ECC-224 bit) trên các zone file tên miền ".vn".



Hình 2. So sánh thời gian giải mã theo thuật toán ECC cải tiến (IMP-ECC-224 bit) và theo cách chọn đường cong của Neal-Koblitz (ECC-224 bit) trên các zone file tên miền ".vn".



Hình 3. So sánh thời gian mã hoá các zone file tên miền ".vn" bằng thuật toán ECC cải tiến (IMP-ECC-224 bit) và bằng RSA-2048 bit.



Hình 4. So sánh thời gian giải mã các zone file tên miền ".vn" bằng thuật toán cải tiến (IMP-ECC-224 bit) và bằng RSA-2048 bit.

Kết quả thu được cho thấy, với cùng một mức bảo mật thì tổng thời gian tạo đường cong Elliptic và mã hoá, giải mã bằng thuật toán ECC cải tiến cài đặt trên cơ sở đường cong thu được từ các thuật toán 1 và 2 đã trình bày ở trên nhanh hơn rất nhiều so với tổng thời gian mã hoá giải mã bằng RSA đang áp dụng cho hệ thống DNS hiện tại, đặc biệt là với các file dữ liệu có kích thước lớn. Việc này rất có lợi khi áp dụng trong thực tế, thay vì phải sử dụng công nghệ DNSSEC với RSA như hiện tại. Đặc biệt là trong khi hệ thống DNS phải thường xuyên trao đổi các file dữ liệu lớn hàng ngày.

IV. KẾT LUẬN

Để tạo điều kiện chọn các tham số cho đường cong Elliptic và tạo đường cong Elliptic dùng trong các hệ mật, nhiều công trình nghiên cứu đã đưa ra những bảng liệt kê các miền tham số để khuyến nghị áp dụng khi xây dựng hệ mật dựa trên đường cong Elliptic. Mặc dù vậy, việc chọn đó là ngẫu nhiên, bị phụ thuộc vào hoàn cảnh và phải đếm số điểm trên đường cong Elliptic. Khắc phục điều đó, bài báo này đưa ra thuật toán chọn miền tham số và tạo đường cong Elliptic trên trường số nguyên tố hữu hạn F_q đáp ứng yêu cầu hạn chế các tấn công Pohlig-Hellman và Pollard's rho, Weil, tấn công cặp Tate và tấn công đối với một số lớp đường cong đặc biệt. Kết quả đánh giá thực nghiệm cho thấy khả năng áp dụng thực tế là khả thi.

TÀI LIỆU THAM KHẢO

[1] JAGDISH BHATTA and LOK PRAKASH PANDEY, *Perfomance Evaluation of RSA Variants and Elliptic Curve Cryptography on Handheld Devices*. IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 11, November 2011.

[2] SHIWEI MA, YUANLING HAO, ZHONGQIAO PAN, HUICHEN, *Fast Implementation for Modular Inversion and Scalar Multiplication in the Elliptic Curve Cryptography*, IITA '08 Proceedings of the 2008 Second International Symposium on Intelligent Information Technology Application - Volume 02, 978-0-7695-3497-8/08©2008 IEEE.

[3] YAN HU, YAN-YAN CUI, TONG LI, *An Optimization Base Point Choice Algorithm of ECC on GF(p)*, 2010 Second International Conference on Computer Modeling and Simulation. 978-0-7695-3941-6/10 ©2010 IEEE.

[4] SHOUZHI XU, CHENGXIA LI, FENGJIE LI, SHUIBAO ZHANG, *An Improved Sliding Window Algorithm for ECC Multiplication*, World Automation Congress (WAC),24-28 June 2012 Page(s): 335 - 338.

[5] TRẦN MINH TÂN và NGUYỄN VĂN TAM, *Nâng cao hiệu quả bảo mật cho hệ thống tên miền*, Chuyên san "Các công trình nghiên cứu, phát triển và ứng dụng công nghệ thông tin và truyền thông", Tập V-1 Số 8(28) 12-2012.

[6] Standards for Efficient Cryptography, *SEC1: Elliptic Curve Cryptography*, Mar. 2009. Version 2.0. http://www.secg.org/download/aid-780/sec1-v2.pdf

[7] CERTICOM RESEARCH, *SEC2: Recommended Elliptic Curve Domain Parameters*, Version 2.0 January 27, 2010, www.secg.org/download/aid-784/**sec2**-v2.pdf

[8] IEEE. *Specifications for Public-Key Cryptography*, IEEE Standard 1363-2000, Aug.2000. http://standards. ieee.org/ catalog/olis/busarch.html

[9] American National Standards Institute. *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, American National Standard X9.62-2005, 2005. http://webstore.ansi.org/ansidocstore

[10] Guide to Elliptic Curve Cryptography, Springer, 2009.

[11] WENDY CHOU, *Elliptic Curve Crytography and its Applications to Mobile Devices*, University of Maryland, College Park, 2003 http://www.cs.umd.edu/ Honors/reports/ECCpaper.pdf

[12] P. GAUDRY, F. HESS and N. P. SMART, *Constructive and destructive facets of Weil descent on elliptic curves*. J. of Cryptology, 15:19–46, 2002. http://www.loria.fr/gaudry/publis/weildesc vZ.ps.gz.

[13] M. JACOBSON, A. J. MENEZES and A. STEIN, *Solving elliptic curve discrete logarithm problems using Weil descent*. J.of the Ramanujan Mathematical Society,16:231-260, 2001 http://eprint.iacr.org/ 2001/ 041.

[14] SHICHUN PANG, SHOUYU, FUZONG CONG, HAIYAN QIU, *An Efficient Elliptic Curve Scalar Multiplication Algorithm against Side Channel Attacks*, Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010 International Conference on 24-26 Aug 2010.

[15] ANN HIBNER KOBLITZ, NEAL KOBLITZ, AND ALFRED MENEZES, *Elliptic Curve Cryptography: The serpentine course of a paradigm shift*. Cryptology ePrint Archive: Report 2008/390 August 28, 2008; last revised on October 2, 2008.

[16] YASUYUKI NOGAMI, YOSHITAKA MORIKAWA. *Fast generation of elliptic curves with prime order over extension field of even extension degree*. Information Theory, 2003. Proceedings. IEEE International Symposium on Digital. 0-7803-7728-1/03©2003 IEEE.

[17] MYKOLA KARPYNSKYY, IHOR VASYLTSOV, IHOR YAKYMENKO, ANDRIJ HONCHARYK, *Elliptic curve parameters generation*. Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2004. Proceedings of the International Conference. Publication Year: 2004 , Page(s): 294 - 295.

Nhận bài ngày: 06/02/2013

SƠ LƯỢC VỀ CÁC TÁC GIẢ

TRẦN MINH TÂN

Sinh ngày 02/9/1968 tại Hưng Yên.

Tốt nghiệp Đại học Sư phạm Hà Nội I - Khoa Vật Lý năm 1991, tốt nghiệp Đại học Bách khoa Hà Nội - Khoa CNTT năm 1996, nhận bằng Thạc sỹ chuyên ngành CNTT năm 2006 tại Trường Đại học Công nghệ - ĐHQG Hà Nội. Hiện là nghiên cứu sinh tại Viện Công nghệ Thông tin - Viện Khoa học và Công nghệ Việt Nam.

Đang công tác tại Trung tâm Internet Việt Nam - Bộ Thông tin và Truyền thông.

Lĩnh vực nghiên cứu: An toàn, bảo mật trên mạng Internet, công nghệ IPv6, DNS.

Điện thoại: 0913275577, 04.35564944 máy lẻ 512. Email: tantm@vnnic.net.vn

NGUYỄN VĂN TAM

Sinh ngày 21/02/1947.

Tốt nghiệp Đại học CVUT, Praha, Tiệp Khắc năm 1971. Bảo vệ luận án Tiến sĩ tại Viện Nghiên cứu VUMS, Praha, Tiệp Khắc năm 1977.

Được phong hàm Phó Giáo sư năm 1996.

Hiện đang công tác tại Phòng Tin học viễn thông - Viện Công nghệ Thông tin.

Lĩnh vực nghiên cứu: Công nghệ mạng và Quản trị, an toàn mạng.

Điện thoại: 0913390606, 04.38362136