Nâng cao hiệu quả bảo mật cho hệ thống tên miền

Security Enhancement for Domain Name System

Tần Minh Tân và Nguyễn Văn Tam

Abstract: *Domain Name Server (DNS) system, a root source providing answers with IP addresses for any request for domain names, is regarded as the most important part of Internet. DNS system also plays a very important part of cryptography analytic infrastructure of Internet. Any change made to DNS system can make the system fall into malfunction, boosting complexity levels in dealing with triggered issues [2,11]. Therefore, security for DNS is a vital must. For the time being, RSA algorithm [6,12] has become the de factor standard for DNS security. However, RSA requires a longer key length of more than 1000 bits [10,15], affecting performance efficiency of DNS system. Hence, elliptic curve cryptography or ECC is regarded as an alternative mechanism for implementing public-key cryptography. The ECC is expected to be used not only in new generation mobile devices [13] but also in DNS system in the near future as ECC requires shorter key length than RSA but providing the same security level. This paper focuses on introducing ECC and new findings related to this mechanism such as key pair generation algorithms, key transfer, encryption and decryption in ECC, as well as findings of the trial on the Vietnam national domain name system dot VN; these findings aims to apply for certification domain name data transfer for the DNS system of a country and compare with the same method in RSA algorithm.*

I. GIỚI THIỆU

Bảo mật cho các hệ thống mạng Internet nói chung và hệ thống tên miền nói riêng là một nhiệm vụ hết sức quan trọng và cấp bách trong hoàn cảnh hiện nay. Tiến triển theo thời gian, các cuộc tấn công vào mạng Internet ở Việt Nam và trên thế giới đang diễn ra ngày càng nhiều với hình thức ngày một tinh vi, phạm vi ngày càng lớn hơn. Thực tế đã có những trường hợp, những thời điểm tin tặc thông qua việc tấn công vào hệ thống máy chủ tên miền (DNS) đã làm tê liệt mạng Internet trên diện rộng trong nhiều giờ gây thiệt hại lớn về an ninh cũng như kinh tế. Để giải quyết vấn đề an toàn cho hệ thống DNS, công nghệ bảo mật DNSSEC (DNS Security Extensions) đã được nghiên cứu và đang được đưa vào áp dụng trong thời gian qua [6].

Năm 1976, Whifield Diffie và Martin Hellman đã đưa ra khái niệm mã bảo mật khóa công khai (PKC - Public Key Cryptography). Từ đó, nhiều ứng dụng của nó đã ra đời và nhiều thuật toán đã được phát triển để giải quyết các bài toán bảo mật. Mức độ bảo mật yêu cầu càng cao thì cỡ khóa phải càng lớn. Với hệ mật mã RSA đang được áp dụng trong hầu hết các ứng dụng, trong đó bao gồm cả bài toán bảo mật cho DNS qua công nghệ DNSSEC [2,6,9] đã nói ở trên, để đảm bảo yêu cầu bảo mật, hiện phải cần cỡ khóa lớn hơn 1000 bit [10,15]. Thực tế, tháng 3 năm 2010, tại hội nghị DATE 2010 - Dresden Đức, các nhà khoa học Andrea Pellegrini, Valeria Bertacco và Todd Austin thuộc trường Đại học Michigan đã công bố kết quả phát hiện một kẽ hở trong hệ mật mã RSA, cách phá vỡ hệ thống, lấy khoá bí mật của RSA 1024 bit chỉ trong vòng 104 giờ thay vì vài năm nếu tấn công theo cách dò tìm lần lượt thông thường [15]. Công bố này cũng đồng nghĩa với tuyên bố rằng, với RSA để đảm bản an toàn sẽ phải tiếp tục tăng độ dài khóa (công nghệ DNSSEC cho hệ thống DNS hiện tại thường sử dụng RSA với độ dài khóa 2048 bit). Điều này kéo theo việc phải tăng năng lực tính toán của thiết bị; làm tăng đáng kể kích thước các file dữ liệu được ký xác thực; tăng thời gian xử lý và lưu lượng dữ liệu phải truyền

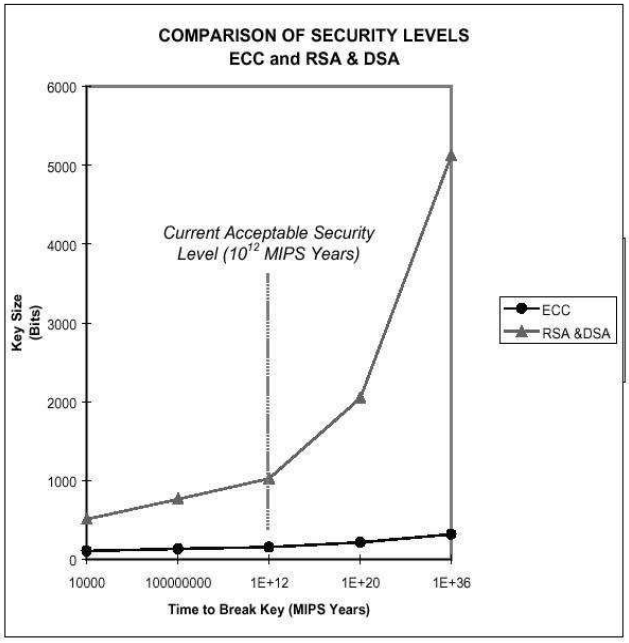
tải trên mạng; đòi hỏi dung lượng lưu trữ của bộ nhớ lớn hơn, nguồn tiêu thụ nhiều hơn,... Và như vậy cũng có nghĩa là sẽ không đảm bảo hiệu quả về mặt kinh tế.

Năm 1985, Neal Koblitz và Victor Miller đã nghiên cứu và đưa ra những công bố về hệ mật mã bảo mật dựa trên đường cong Elliptic (Elliptic Curve Cryptography - ECC) có những đặc tính đặc biệt [3,4,8]: Yêu cầu năng lực tính toán thấp; tiết kiệm bộ nhớ; tiết kiệm băng thông; tiết kiệm năng lượng; tính bảo mật cao. Từ những đặc điểm nổi trội ấy, nhiều nhà khoa học đã đi sâu vào nghiên cứu hệ mật mã bảo mật đường cong Elliptic [1,7,10,11] và bước đầu đã có các ứng dụng vào một số lĩnh vực bảo mật, đặc biệt cho các thiết bị thông tin di động [13], thiết bị USB[9].

Phát triển các kết quả này, Công ty Certicom - Công ty đi đầu trong lĩnh vực nghiên cứu hệ mật mã bảo mật ECC [16], đã nghiên cứu, triển khai một số ứng dụng và công bố các số liệu so sánh về mức độ bảo mật giữa các hệ mật mã RSA và ECC. Theo đó với độ dài khóa 160 bit, hệ mật mã ECC đã có độ bảo mật tương đương với hệ mật mã RSA-1024 bit; và với độ dài khóa 224 bit, hệ mật mã ECC có độ bảo mật tương đương với hệ mật mã RSA-2048 bit [3].

Bảng 1. So sánh độ dài khóa của các hệ mật mã với cùng mức độ bảo mật [3]

Hệ mật mã	**Kích thước khóa (tính theo bit)**					
Khóa đối xứng	56	80	112	128	192	256
RSA/ DSA	512	1024	2048	3072	7680	15360
ECC	112	160	224	256	384	512



Hình 1. So sánh mức độ bảo mật giữa ECC với RSA/DSA [13]

Do kích thước khóa nhỏ và khả năng bảo mật cao nên trong giai đoạn vừa qua, ECC chủ yếu được nghiên cứu để bước đầu áp dụng cho các ứng dụng trên môi trường mạng có giới hạn về thông lượng truyền dữ liệu, các thiết bị có giới hạn về năng lực xử lý, khả năng lưu trữ (đặc biệt là với các thiết bị di động) [13]. Tuy nhiên với các lợi thế về mức độ bảo mật và kích thước khóa nhỏ như đã nói ở trên, ECC hoàn toàn có thể được áp dụng cho các hệ thống lớn như DNS để thay thế, khắc phục các nhược điểm về độ dài khóa của RSA. Bài báo này chúng tôi sẽ đề xuất phương pháp cài đặt hệ mật mã ECC lên các giao dịch trao đổi dữ liệu giữa các máy chủ trong hệ thống DNS để nâng cao tính bảo mật và hiệu năng cho hệ thống này.

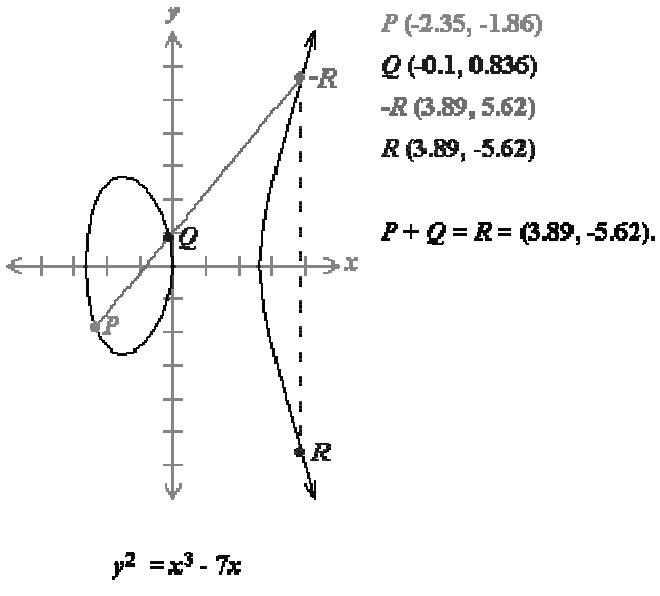
Trong [1], tác giả đã chỉ ra những bước cơ bản để xây dựng thuật toán bảo mật bằng đường cong Elliptic, tuy vậy mới dừng lại ở công thức tổng quan hoặc ở ví dụ cụ thể bằng số. Ở đây, chúng tôi sẽ xây dựng chi tiết các thuật toán tạo khóa, chuyển khóa, mã hóa và giải mã trên ECC một cách đơn giản và rõ ràng hơn nhằm giảm số bước thực hiện. Đây là nền tảng để xây dựng hệ mật mã ECC.

Trong các nội dung tiếp theo, Phần 2 chúng tôi sẽ trình bày phát biểu bài toán hệ mật mã đường cong Elliptic (ECC) và kết quả xây dựng một số thuật toán trong ECC để áp dụng cho việc xác thực trong quá trình trao đổi dữ liệu trên mạng Internet; Phần 3 trình bày kết quả thực nghiệm ECC, ứng dụng các thuật toán nói trên trong việc xác thực dữ liệu tên miền trong hệ thống DNS cấp quốc gia, so sánh với cách sử dụng phương pháp tương tự bằng RSA; cuối cùng là phần kết luận.

II. PHÁT BIỂU BÀI TOÁN

Đường cong Elliptic trên GF(p) hoặc Zp với số nguyên tố p được xác định bằng phương trình Cubic: $y^2 = (x^3 + ax + b) \bmod p$, với các hệ số a và b và các biến x và y là các phần tử của Zp thỏa mãn ràng buộc $(4a^3 + 27b^2) \bmod p \neq 0$ [14].

Như vậy ta dễ dàng nhận thấy đường cong Elliptic ***(E)*** có phương trình là hàm chẵn đối với biến y, do đó đồ thị của ***(E)*** nhận trục hoành Ox là trục đối xứng.



Hình 2. Một dạng đường cong Elliptic

Tập các điểm trên đường cong Elliptic ***(E)*** có các đặc điểm sau:

- Điểm **Θ** là điểm thuộc (***E***) nằm ở vô cùng, được gọi là phần tử trung hòa.
- Với mỗi điểm P=(x,y), phần tử đối của P là điểm -P=(x,-y), ta định nghĩa tổng hai điểm P+(-P) = P-P = **Θ**. Hay -P là điểm đối xứng của P qua trục Ox.
- Với 2 điểm $P=(x_P, y_P)$ và $Q=(x_Q, y_Q)$ với $x_P \neq x_Q$, một đường thẳng đi qua hai điểm P, Q sẽ giao với (***E***) tại một điểm duy nhất. Ta định nghĩa điểm R = -(P+Q). Nếu đường thẳng này là tiếp tuyến của (***E***) tại điểm P hoặc Q thì tương ứng R≡P hoặc R≡Q. Điểm đối xứng của R là -R được gọi là điểm tổng của P và Q.
- Đường thẳng đi qua P và -P (tức P và Q có cùng hoành độ), sẽ giao với (***E***) tại điểm vô cùng, do vậy R = P+(-P) = **Θ**.
- Để nhân đôi điểm P, ta vẽ tiếp tuyến của (***E***) tại P, tiếp tuyến này sẽ giao với (***E***) tại điểm Q, ta có Q= -(P+P)=-2P. Hay -Q=2P

Với những đặc điểm trên, tập các điểm thuộc đường cong (***E***) tạo thành một nhóm Abel.

Hệ mật mã đường cong Elliptic (ECC) được xây dựng trên cơ sở bài toán logarith trên đường cong Elliptic. Độ bảo mật ECC phụ thuộc vào độ khó của bài toán logarith rời rạc đường cong Elliptic. Giả sử P và Q là hai điểm trên đường cong Elliptic sao cho k*P=Q trong đó *k* là một đại lượng vô hướng với P và Q đã cho, bằng cách tính toán suy luận để thu được *k* trên cơ sở thuật toán rời rạc của Q đối với P.

Với một điểm P cho trước và hệ số *k*, ta có thể dễ dàng tính ra được điểm Q tương ứng trên đường cong Elliptic. Tuy nhiên theo chiều ngược lại, để tìm ra hệ số *k* (khóa *k*) từ điểm Q và điểm P lại là một bài toán "rất khó" nếu như hệ số *k* là một số đủ lớn (có độ dài 224 bit chẳng hạn). Dựa trên cơ sở bài toán logarit rời rạc xét trên tập các điểm thuộc đường cong Elliptic này, hệ mật mã ECC cung cấp đầy đủ cả 4 dịch vụ an ninh: mã hóa, xác thực, ký số và trao đổi khóa; đảm

bảo cho việc xây dựng một hạ tầng xác thực khóa công khai trên Internet. Do đó một trong những thuật toán chủ yếu trong ECC là tạo khóa, chuyển khóa, mã hóa và giải mã [14].

Trên cơ sở bài toán này, chúng tôi đề xuất các thuật toán cụ thể:

1. Tạo khóa:

Đường cong Elliptic trên trường GF(p) có dạng:

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

đã nói ở trên với các tham số p, a và b đã chọn. Lấy điểm cơ sở G từ nhóm Ep(a,b) trên đường cong Elliptic, bậc của nó phải là một giá trị n lớn [14]. Bậc n của điểm G trên đường cong Elliptic được xác định bằng số nguyên dương bé nhất n sao cho n*G = 0 [14].

Tham số hệ mật mã ECC trên trường nguyên tố hữu hạn Fp.[4]:

$$T = (p, a, b, G, n, h) \qquad (2)$$

Trong đó: p là số nguyên dương xác định trường nguyên tố hữu hạn Fp và chọn $[\log_2 P] \in \{192, 224, 256, 384, 512\}$; a,b là các hệ số $\in$Fb xác định đường cong trên Elliptic E(Fb) trên trường Fb(1); h là phần số thập phân, h= #E(Fb)/n với #E(Fb) là số các điểm thuộc đường cong E(Fb).

Theo các bước tạo khóa được xác định tại [14], chúng tôi xây dựng thuật toán như Hình 3.

Thuyết minh thuật toán:

- Đầu vào: Bên gửi A và Bên nhận B thống nhất đường cong Elliptic và tham số hệ mật mã đường cong Elliptic T.
- Đầu ra: Khóa công khai của A: P_A và khóa công khai của B: P_B cần được thiết lập.

Các bước thuật toán:

1. A chọn ngẫu nhiên một số nguyên dương $n_A < n$.

2. A xác lập tích $P_A = n_A*G = (x_A, y_A)$

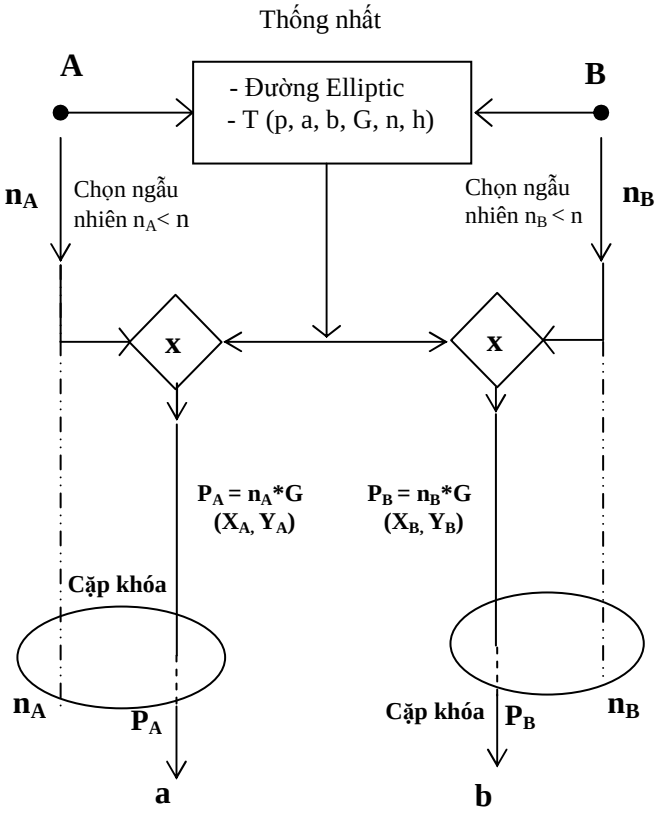
Cặp khóa công khai và khóa riêng của A là (P_A, n_A)

3. B chọn ngẫu nhiên số nguyên $n_B < n$ và tính

$$P_B = n_B * G = (x_B, y_B)$$

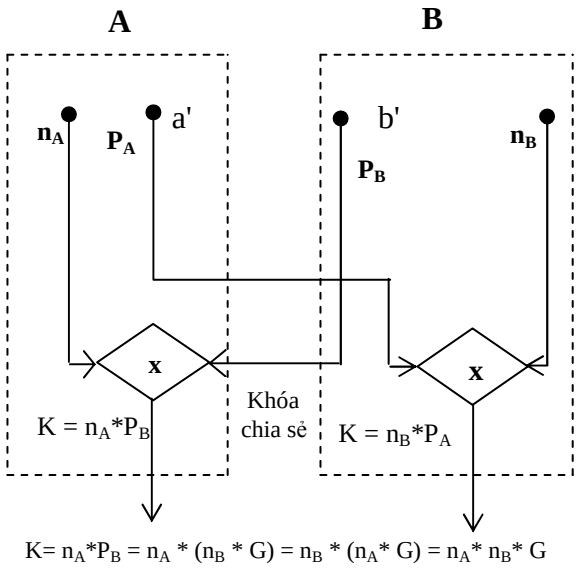
Cặp khóa công khai, khóa riêng của B là (P_B, n_B).

Thuật toán tạo khóa: Hai bên gửi A và nhận B.



Hình 3. Thuật toán tạo khóa

2. Thuật toán trao đổi khóa



Hình 4. Thuật toán trao đổi khóa

Thuyết minh thuật toán:

Thuật toán trao đổi khóa được hình thành sau khi bên A và bên B đã được tạo khóa P_A và P_B thể hiện ở điểm a, b tương ứng trên hình 3 như đã nói ở trên.

Thuật toán được diễn đạt như sau:

- Đầu vào: Cặp khóa P_A và P_B
- Đầu ra: $P_A \rightarrow B$; $P_B \rightarrow A$

Xác nhận đúng đối tượng cần kết nối thông tin bằng kết quả hai bên tìm được khóa chia sẻ chung K.

Các bước thực hiện :

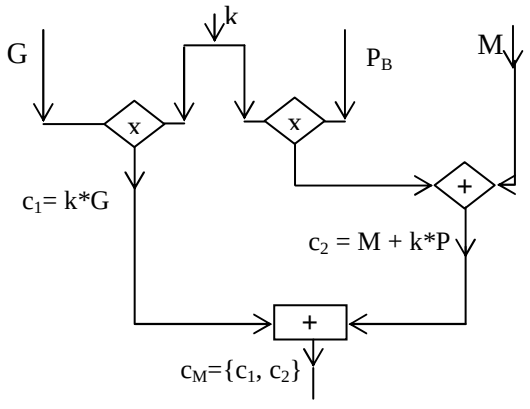
1. A truyền khóa P_A cho B; B truyền khóa P_B cho A.
2. Cả A và B tính khóa chia sẻ:
   - Phía A: Lấy n_A của mình nhân với khóa P_B nhận được từ B tạo ra:
     $K= n_A*P_B = n_A*(n_B*G) = n_A* n_B* G$
   - Phía B: Lấy n_B của mình nhân với khóa P_A nhận được từ A tạo ra:
     $K= n_B*P_A = n_B*(n_A*G) = n_A*n_B* G$

Như vậy cả A và B đều nhận được K giống nhau.

3. Thuật toán mã hóa và giải mã

Thuật toán mã hóa và giải mã Elliptic được Bellaer và Rogaway đề xuất [3], thực chất là một biến thể của hệ mật mã công khai Elgamal. Ở đây chúng tôi cụ thể hơn dưới dạng lưu đồ thuật toán và đơn giản hơn bằng cách bỏ qua thủ tục tính cặp khóa, tính bản mã sử dụng.

Thuật toán mã hóa:

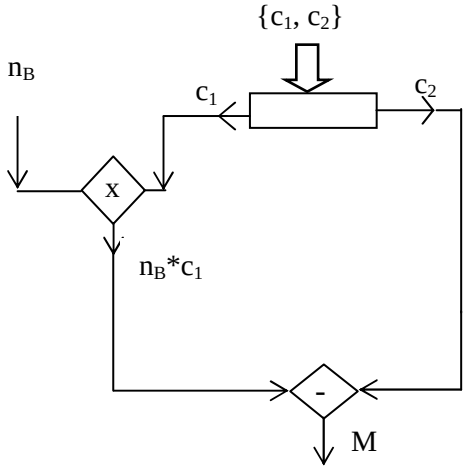


Hình 5. Lưu đồ thuật toán mã hóa

- Đầu vào: A muốn gửi bản tin M cho B.
- Đầu ra : Văn bản mã c_M
- Các bước thực hiện:

1. A chọn ngẫu nhiên một số nguyên dương thỏa mãn $0 < k < n$ và tính: $c_1 = k*G$ và $c_2 = M + k*P_B$ trong đó P_B là khóa công khai của B.
2. A gửi văn bản đã mã hóa $c_M = \{ c_1, c_2\}$ cho B.

Thuật toán giải mã



Hình 6. Lưu đồ thuật toán giải mã

- Đầu vào ở B:

  B nhận được văn bản mã $C_M = \{ c_1, c_2\}$
- Đầu ra:

  Khôi phục lại văn bản M do A gửi đến.
- Các bước thực hiện :

B tách c_1 và nhân c_1 với khóa riêng n_B của nó và lấy c_2 trừ đi kết quả đó:

$$c_2 - n_B*c_1 = M + k*P_B - n_B * (k*G)$$
$$= M + k*(n_B*G) - n_B*(k*G)$$
$$= M$$

Vậy đã thực hiện xong giải mã.

Nhân xét:

Thuật toán này không yêu cầu kiểm tra điểm R có thuộc đường cong Elliptic hay không; không cần tính điểm Z = k*k*R như trong [1,3,14] làm cho tốc độ tính nhanh hơn.

Bảng 2. Tổng hợp số liệu về thời gian ký xác thực và kích thước các zone file tên miền .VN trước và sau khi ký bằng DNSSEC với RSA-2048 bit và ký bằng ECC-224 bit.

Zone	Kích thước zone file ban đầu (Bytes)	Kích thước zone file sau khi ký xác thực (bytes)		Thời gian ký (giây)		Số tên miền được ký
		Với DNSSEC sử dụng RSA-2048 bit	Với ECC-224 bit	Với DNSSEC sử dụng RSA-2048 bit	Với ECC-224 bit	
.vn	3 520 683	27 126 822	6 337 230	171,135	21,942	69 530
.com.vn	3 495 013	24 357 519	5 941 522	145,342	18,633	59 483
.net.vn	120 257	840 584	198 424	5,094	0,621	2 069
.org.vn	142 423	1 078 018	243 544	6,668	0,877	2 684
.edu.vn	263 367	1 749 856	442 456	10,464	1,291	4 232
.ac.vn	5 765	42 885	10 492	0,269	0,038	108

III. KẾT QUẢ THỰC NGHIỆM

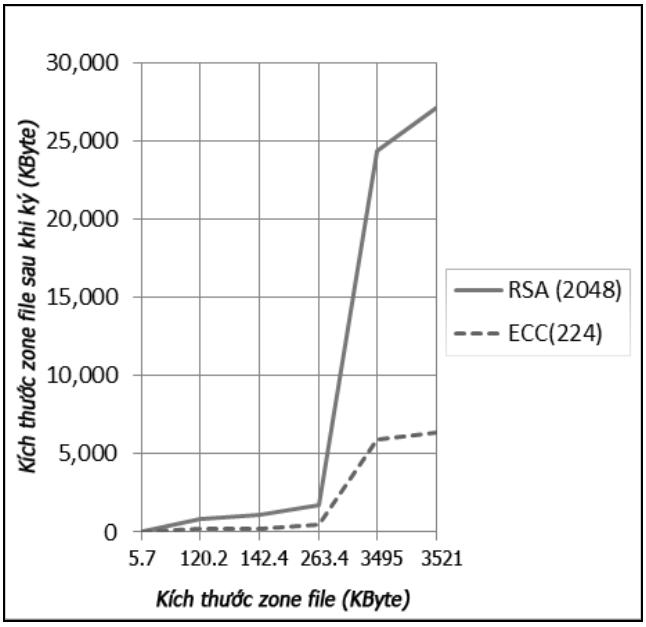
Trên cơ sở các thuật toán đề xuất ở trên, chúng tôi đã sử dụng ngôn ngữ lập trình Java để cài đặt các thuật toán, áp dụng vào quá trình xác thực trong các giao dịch trao đổi dữ liệu tên miền giữa máy chủ DNS chính (Primary DNS Server) và các máy chủ phụ (Secondary DNS Server). Thí nghiệm được thực hiện trên các zone file dữ liệu tên miền được lấy trực tiếp về từ hệ thống DSN quốc gia.

Để đảm bảo an toàn và dự phòng bổ sung, san tải cho nhau, hệ thống DNS được thiết kế theo quy định sẽ gồm một máy chủ DNS chính và nhiều máy chủ DNS phụ. Theo các mốc thời gian định kỳ tùy thuộc vào cơ chế khai báo trên máy chủ DNS chính, các máy chủ DNS phụ sẽ tự động kết nối với máy chủ DNS chính để tải các file dữ liệu tên miền đã có sự thay đổi trên máy chủ chính về máy chủ phụ để đáp ứng việc cập nhật kịp thời các thay đổi nhằm trả lời chính xác các truy vấn về tên miền từ các máy tính trên mạng Internet được hỏi đến nó. Quá trình này được gọi là cơ chế zone transfer trong quy trình quản lý hệ thống DNS. Để bảo mật cho quá trình đồng bộ dữ liệu này, ngoài giải pháp phần cứng (khai báo cấu hình mạng chỉ cho phép các máy chủ phụ có địa chỉ IP từ trong một danh sách đã được định nghĩa trước mới có quyền kết nối vào máy chủ chính), hiện chỉ mới có công nghệ bảo mật DNSSEC sử dụng RSA đang được áp dụng là có triển khai việc ký xác thực, mã hóa dữ liệu tên miền trong quá trình trao đổi giữa các máy chủ DNS với nhau. Ở đây, chúng tôi đã xây dựng chương trình ký xác thực, mã hóa, giải mã bằng ECC tương tự như các bước làm của DNSSEC sau đó lần lượt sử dụng ECC để thực hiện việc ký xác thực, mã hóa dữ liệu trên các zone tên miền quốc gia bao gồm .vn, .com.vn, .net.vn, .org.vn, .edu.vn và .ac.vn và so sánh với các kết quả đã thu được bằng phương pháp sử dụng DNSSEC.

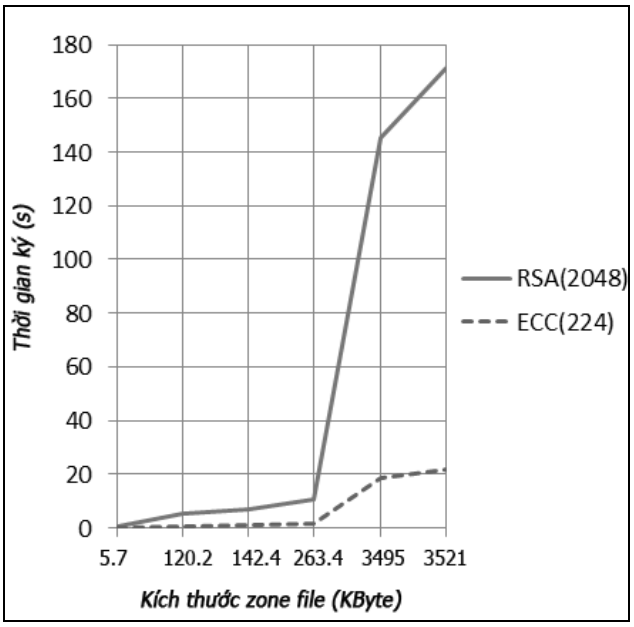
Các kết quả thu bằng hai phương pháp được đem ra so sánh theo các tiêu chí sau: 1/ Thời gian ký xác thực; 2/Kích thước zone file sau khi ký xác thực. Chi tiết được thể hiện trong Bảng 2.

Kết quả so sánh này cho thấy, sau khi ký xác thực bằng RSA-2048 bit với DNSSEC, kích thước các zone file tăng bình quân xấp xỉ 7,31 lần, trong khi đó sau ký xác thực bằng ECC-224 bit kích thước chỉ tăng bình quân 1,74 lần so với file dữ liệu gốc. Về thời gian ký xác thực, khi sử dụng RSA-2048 bit sẽ lâu hơn bình quân 7,8 lần so với việc ký bằng ECC-224 bit theo thuật toán đã đề xuất.

Tổng hợp so sánh kết quả thực nghiệm trên các zone file được lấy liên tiếp mỗi khi có sự thay đổi các bản ghi tên miền trên zone của máy chủ DNS chính trong vòng 24 giờ liên tục (theo cơ chế yêu cầu máy chủ DNS phụ cập nhật toàn bộ nội dung file mỗi khi có thay đổi) được thể hiện trên các sơ đồ sau:



Hình 7. So sánh kích thước zone file tên miền sau khi ký xác thực với RSA-2048 bit và ECC-224 bit



Hình 8. So sánh thời gian ký xác thực bằng RSA-2048 bit và ECC-224 bit trên các zone file gốc

Như vậy, rõ ràng ECC có các ưu điểm vượt trội về thời gian xử lý và đặc biệt là làm giảm đáng kể kích thước các zone file dữ liệu tên miền sau khi được ký xác thực so với phương pháp dùng RSA trong DNSSEC với cùng một mức độ bảo mật. Việc sử dụng ECC đã làm giảm tương đối thời gian, dữ liệu phải truyền tải trên mạng trong quá trình đồng bộ tên miền giữa máy chủ DNS chính và các máy chủ DNS phụ, đồng thời tiết kiệm đáng kể băng thông (hiện tại hệ thống DNS quốc gia đang phải đồng bộ dữ liệu thường xuyên trong ngày giữa máy chủ chính và 26 máy chủ phụ đặt tại các địa điểm khác nhau trên toàn cầu). Việc ứng dụng ECC sẽ nâng cao rõ rệt hiệu năng cho hệ thống máy chủ tên miền.

IV. KẾT LUẬN

Bài báo này nghiên cứu áp dụng mã bảo mật đường cong Elliptic, trong đó đã :

- Xây dựng lưu đồ thuật toán tạo khóa dựa trên đường cong Elliptic và tham số T(p, a, b, G, n, h), giúp cho việc tính toán rõ ràng và đơn giản.

Xây dựng thuật toán trao đổi khóa thống nhất với thuật toán tạo khóa và bỏ qua được các bước A tạo P_A gửi B và B tạo P_B gửi A như trong [3]. Đồng thời thuật toán ở đây đơn giản.

- Đưa ra thuật toán mã hóa, giải mã đơn giản hơn so với trước đây.

- Cuối cùng trong bài báo này, chúng tôi đã trình bày kết quả thực nghiệm cài đặt thuật toán, áp dụng thử nghiệm trên các file dữ liệu tên miền được lấy trực tiếp về từ hệ thống DSN quốc gia (các file trên thực tế sẽ tham gia trong quá trình trao đổi dữ liệu tên miền giữa máy chủ DNS quốc gia). So sánh thời gian ký xác thực, kích thước các file dữ liệu sau khi triển khai thử nghiệm bằng ECC-224 bit qua các thuật toán được xây dựng trong bài báo với các kết quả đã thu được khi sử dụng công nghệ DNSSEC sử dụng RSA-2048 bit. Kết quả thực nghiệm đã khẳng định được tính ưu việt của việc ứng dụng các thuật toán trên ECC đã được đề xuất trong bài báo so với phương pháp thông dụng hiện nay là RSA.

Từ những phân tích trên, ta thấy việc nghiên cứu, ứng dụng mã bảo mật đường cong Elliptic - ECC như những kết quả đã đưa ra đã đạt yêu cầu làm tăng tính bảo mật hơn so với RSA, đồng thời với ba thuật toán

đã nêu làm đơn giản số bước tính toán. Đây sẽ là nền tảng cơ sở để giải quyết việc tránh phải tiếp tục nâng độ dài khóa như RSA mà vẫn đáp ứng được yêu cầu về bảo mật (khó phá khóa) với kích thước khóa nhỏ hơn. Việc áp dụng mã bảo mật đường cong Elliptic - ECC trong các hệ thống lớn như DNS là một hướng đi đúng và trọng tâm trong thời gian tới. Trong hướng nghiên cứu sắp tới, chúng tôi sẽ mở rộng xét chọn miền tham số cho đường cong Elliptic để sử dụng làm mã bảo mật.

TÀI LIỆU THAM KHẢO

[1] ANOOP MS, *Elliptic Curve Cryptography. An Implementation Guide*. anoopms@tataelxsi.co.in

[2] B. WELLINGTON, *Domain Name System Security (DNSSEC) signing Authority*, RFC 3008, Internet Engineering Task Force, November 2000 http://www.ietf.org/rfc/rfc3008.txt

[3] CERTICOM RESEARCH, *SEC1: Elliptic Curve Cryptography*, Version 1.0, September 2000, http://www.secg.org/collateral/sec1_final.pdf

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

[5] DARREL HANKERSON, JULIO LÓSPEZ HERNANDERZ, ALFRED MENEZES, *Software Implementation of Elliptic Curve Cryptography over Binary Fields*, CHES 2000.

[6] DANIEL MASSEY, ED LEWIS and OLAFUR GUDMUNDSSON, *Public Key Validation for the DNS Security Extensions*, DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, Print ISBN: 0-7695-1212-7, 2001.

[7] F. HESS, *Generalising the GHS attack on the Elliptic Curve Discrete logarithm problem*, LMS J. Comput, Math 7, 2004.

[8] JACOB SCOTT, *Elliptic Curve Cryptography*, December 14, 2010.

[9] 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.

[10] N. GURA A. PATEL, A. WANDER, H. EBERLE and S.C SHANTZ, *Comparing Elliptic Curve Cryptography and RSA on 8 bit CPUS*, Proccedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004) 6th Internetional Workshop - 2004

[11] M. ABDALLA, M. BELLARE and P.ROGAWAY, *DHAES. An encryption Scheme based on the Difflie - Hellman problem*, Submission to P1363a: Standerd specifications for Public-Key Cryptography, Additional Techniques, 2000.

[12] REZA CURTMOLA, ANIELLO DEL SORBO, GIUSEPPE ATENIESE, *On the Performance and Analysis of DNS Security Extensions*, Cryptology and Network Security, 4th International Conference, CANS 2005.

[13] 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

[14] W. STALLINGS, *Crypotography and Network Security*, Fourth Edition 2009.

[15] ANDREA PELLEGRINI, VALERIA BERTACCO and TODD AUSTIN, *Fault Based Attack of RSA Authentication*, Design, Automation and Test in Europe (DATE) conference in Dresden on March 10. http://web.eecs.umich.edu/~valeria/research/publications/DDTE10RSA.pdf

[16] Certicom Website: http://certicom.com

Nhận bài ngày: 25/05/2012

SƠ LƯỢC VỀ 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, 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. Đang là nghiên cứu sinh tại Viện Công nghệ Thông tin - Viện Khoa học và Công nghệ Việt Nam.

Hiện 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 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

Email: nvtam@ioit.ac.vn