MỘT SỐ KHUYẾN NGHỊ VỀ VIỆC SỬ DỤNG AN TOÀN LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN ĐƯỜNG CONG ELLIPTIC

ThS. Hoàng Thu Phương, ThS. Trần Thị Xuyên

Học viện Kỹ thuật mật mã

Trong lĩnh vực chữ ký số, lược đồ ký số dựa trên đường cong Elliptic (ECDSA) được đánh giá là một trong những lược đồ chữ ký số có độ an toàn cao, dù ra đời sau nhưng ECDSA đang dần được thay thế cho lược đồ ký số RSA. Bài báo này tập trung giới thiệu lược đồ ECDSA, ứng dụng của ECDSA trong thực tế và các tham số an toàn được khuyến nghị dùng cho ECDSA.

GIỚI THIỆU VỀ CHỮ KÝ SỐ

Chữ ký số là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng, theo đó, người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác:

- Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa;

- Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

Bên cạnh đó, nếu hiểu theo tính ứng dụng thì chữ ký số có thể thay thế hoàn toàn chữ ký thường bằng tay và sử dụng trên các thiết bị điện tử, nó được hiểu như là một chữ ký tay của cá nhân hay một con dấu của cơ quan, doanh nghiệp và được pháp luật thừa nhận về mặt pháp lý khi thực hiện giao dịch trên môi trường điện tử. Tiêu biểu như ký kê khai thuế, hợp đồng điện tử, giao dịch tài chính,...

Lược đồ ECDSA

Tham số miền cho ECDSA có dạng $(q,FR,h,n,Type,a,b,G,\{domain\_parameter\_seed\})$ [1], trong đó:

- p: là số nguyên tố lẻ, đường cong elliptic E xác định trên trường hữu hạn F_p

- Một chỉ báo FR (Field representation) được sử dụng cho các phần tử của F_p

- Domain_parameter_seed: Một chuỗi bit seedF tùy chọn, nếu đường cong E được tạo theo các phương pháp tạo ngẫu nhiên có thể kiểm chứng được.

- Điểm sinh $G=(x_G, y_G) \in F_p$ có bậc n (nguyên tố) trong $E(F_p)$.

- Hai phần tử a và b trong F_p xác định phương trình của đường cong elliptic E trên F_p

- Type: loại đường cong elliptic được sử dụng.

- Phần phụ đại số h thỏa mãn $h = \#E(F_p)/n$. Với $\#E(F_p)$ là số các điểm thuộc đường cong $E(F_p)$.

Tạo khóa

Cặp khóa của Alice được gắn với một bộ tham số miền EC cụ thể D $(q,FR,h,n,Type,a,b,G,\{domain\_parameter\_seed\})$ - theo FIPS 186-5 (2023). Các bước tạo khóa như sau:

- Chọn ngẫu nhiên một số nguyên d trong khoảng $[1, n-1]$

- Tính $Q = dG$

Khóa công khai của Alice là Q và khóa riêng của Alice là d.

Tạo giá trị bí mật k cho mỗi thông điệp

Một số ngẫu nhiên bí mật mới k, $0 < k < n$ sẽ được tạo trước khi tạo mỗi chữ ký số. Giá trị k^{-1} là nghịch đảo của k theo phép modulo n. Đối với ECDSA không tất định (non-deterministic ECDSA), cả k và k^{-1} có thể được tính trước và khi đó tính bí mật và tính toàn vẹn của chúng sẽ được bảo vệ theo cách tương tự như khóa riêng.

ECDSA tất định (deterministic ECDSA) là một biến thể của ECDSA trong đó giá trị bí mật trên mỗi thông điệp là một hàm của thông điệp đã được ký và khóa riêng, do đó dẫn đến ánh xạ xác định của thông điệp đến chữ ký. Điều này bảo vệ chống lại các cuộc tấn công phát sinh từ việc tạo chữ ký với giá trị bí mật không đủ ngẫu nhiên trên mỗi thông điệp sẽ tiết lộ khóa riêng.

Tạo chữ ký

Đầu vào:

- Thông điệp M (chuỗi bit)

- Khóa riêng d trong khoảng giá trị $[1, n-1]$ và bộ các tham số miền D

- Hàm băm được phê duyệt hoặc XOF với độ dài đầu ra là hashlen bít.

Đầu ra: Cặp số nguyên (r, s), với r, s thuộc khoảng $[1, n-1]$

Quá trình ký:

1. Tính H = Hash(m) bằng cách sử dụng hàm băm đã thiết lập hoặc XOF với xâu bit H đầu ra có hashlen bít

2. Chuyển giá trị này sang số nguyên e:

- Nếu len(n) ≥ hashlen, đặt $E = H$. Nếu không, đặt $E = [log_2(n)]$ bit của H.

- Chuyển xâu bit E sang số nguyên e

3. Chọn ngẫu nhiên một số nguyên bí mật k, $0<k<n$

4. Tính k^{-1} mod n

5. Tính $R = kG = (x_R, y_R)$

6. Đặt x_R là biểu diễn affine tọa độ x của điểm $R=(x_R, y_R)$

7. Chuyển x_R thành số nguyên r_1

8. Tính $r = r_1$ mod n.

9. Tính $s = k^{-1}(e+r.d)$ mod n.

10. Hủy một cách an toàn giá trị k và k^{-1}

11. Nếu $r = 0$ hoặc nếu $s = 0$ và k được tạo một cách xác định, thì đầu ra là "Failure". Mặt khác, nếu $r = 0$ hoặc $s = 0$ thì quay lại bước 3.

12. Chữ ký của Alice cho thông điệp m là (r, s)

Xác minh chữ ký

Để xác minh chữ ký của Alice trên thông điệp m, Bob sẽ thực hiện như sau:

Đầu vào:

- Thông điệp M

- Cặp số nguyên (r, s)

- Khóa xác minh chữ ký Q và các tham số miền D

Đầu ra: "Chấp nhận" hoặc "Từ chối" chữ ký trên M có nguồn gốc từ người sở hữu khóa công khai Q

Quá trình xác minh chữ ký:

1. Xác minh rằng cả r và s đều là số nguyên trong khoảng $[1, n-1]$. Đầu ra "Từ chối" nếu xác minh không thành công.

2. Tính H = Hash(M) sử dụng hàm băm đã thiết lập hoặc XOF trong đó chuỗi bit H có hashlen bít.

3. Lấy số nguyên e từ H như sau:

- Nếu $[log_2(n)] \geq$ hashlen, đặt $E = H$. Ngược lại, đặt E bằng $[log_2(n)]$ các bít ngoài cùng bên trái của H.

- Chuyển chuỗi bit E thành số nguyên e.

4. Tính s^{-1} mod n.

5. Tính $u = e.s^{-1}$ mod n và $v = r.s^{-1}$ mod n.

6. Tính $R_1 = [u]G + [v]Q$. Đầu ra "Từ chối" nếu R_1 là điểm vô cực.

7. Đặt x_R là tọa độ x của biểu diễn affine của $R_1=(x_R, y_R)$.

8. Chuyển đổi x_R thành số nguyên r_1.

9. Xác minh $r = r_1 \mod n$ (*). Nếu (*) đúng thì đầu ra là "Chấp nhận", ngược lại thì là "Từ chối".

ỨNG DỤNG ECDSA TRONG THỰC TẾ

Hiện có nhiều nghiên cứu đã chỉ ra khả năng sử dụng ECDSA hiệu quả hơn trong các môi trường có tài nguyên hạn chế (bộ nhớ, năng lượng và khả năng CPU). Wander và cộng sự [8] đã thực hiện một nghiên cứu về năng lượng cho mật mã khóa công khai (ECC/ECDSA, RSA). Họ đã phân tích chữ ký trong ECDSA với khóa 160-bit và RSA với khóa 1024-bit và kết luận rằng ECC/ECDSA hiệu quả hơn RSA và khả thi trên các thiết bị có tài nguyên hạn chế vì nó tạo ra các khóa và chứng chỉ nhỏ với cùng mức độ bảo mật như RSA. Gần đây, các nhà nghiên cứu đã áp dụng thuật toán ECDSA như một hệ thống xác thực nhẹ trong WSN (mạng cảm biến không dây). Điều này chứng minh tính hiệu quả của việc sử dụng ECDSA trong WSN về mặt bảo mật và hiệu suất.

Trên thế giới, thực tế đã có một số doanh nghiệp, công ty hàng đầu của Mỹ đã đưa ECDSA vào sử dụng như dùng xác thực cho các trình quyệt web an toàn qua SSL/TLS cụ thể hơn nếu truy cập các trang web như Google.com, Amazon.com, Facebook.com, sau đó truy cập vào chứng chỉ an toàn ta sẽ thấy được.

Ngoài ra ECDSA còn được sử dụng để bảo vệ thông tin liên lạc nội bộ để giúp đảm bảo ẩn danh, nó cũng được dùng để chứng minh quyền sở hữu trong bitcoin, cung cấp chữ ký số trong dịch vụ iMessage của Apple, và dùng để mã hóa thông tin DNS với DNSCurve.

Ở nước ngoài, thuật toán ECDSA đã và đang được đưa vào sử dụng trong các doanh nghiệp, còn ở Việt Nam hiện các doanh nghiệp sử dụng thuật toán RSA cũng đang dần chuyển sang ECDSA vì những thế mạnh của nó và dự trong tương lai thuật toán này sẽ nhanh chóng thay thế RSA để trở thành phổ biến.

KHÍA CẠNH AN TOÀN VÀ CÁC KHUYẾN NGHỊ AN TOÀN ĐƯỢC DÙNG TRONG ECDSA

Bài toán logarit rời rạc trên đường cong elliptic

Bài toán logarit rời rạc đường cong elliptic (ECDLP) là: cho một đường cong elliptic E được xác định trên một trường hữu hạn F_p, biết trước một điểm $G \in E(F_p)$ có cấp n, và một điểm $Q = lG$ với $0 \leq l \leq n-1$. Hãy tìm giá trị l.

Cho đến nay có rất nhiều công trình công bố cách giải bài toán này tuy nhiên thuật toán tốt nhất được biết đến để giải bài toán ECDLP là phiên bản song song hóa thuật toán Pollard's rho với thời gian chạy kì vọng là $(\sqrt{\pi n})/(2r)$ bước thực hiện, trong đó n là cấp của điểm sinh G và r là số lượng bộ xử lý được sử dụng [2].

Bảng 2 được tham khảo từ ANS X9.62 [5] minh họa độ khó của ECDLP. Nó chứa các ước tính theo MIPS năm của khả năng tính toán cần thiết để giải ECDLP trên một đường cong chung trong phần mềm sử dụng phương pháp Pollard-ρ cải tiến.

Bảng 2. Khả năng tính toán cần để giải ECDLP dùng thuật toán Pollard's rho [5]

Kích thước của *n* tính theo bit	MIPS năm
150	3.8×10^{10}
205	7.1×10^{8}
234	1.6×10^{28}

Yêu cầu hàm băm an toàn

Các hàm băm sử dụng trong lược đồ ký cần phải có khả năng kháng tiền ảnh và kháng va chạm để đảm bảo an toàn. Thường các hàm băm đã được phê duyệt như SHA-256, SHA-384, SHA-512 hoặc các XOF được phê duyệt là SHAKE128 và SHAKE256, được khuyến nghị trong FIPS 202. Khi SHAKE128 hoặc SHAKE256 được sử dụng làm XOF thì đầu ra của nó có độ dài tương ứng là 256 hoặc 512 bit [1].

Yêu cầu bảo mật với giá trị k

Mỗi giá trị k trong quá trình tạo chữ ký số ECDSA có yêu cầu bảo mật giống như khóa riêng d. Điều này là do nếu kẻ tấn công biết được giá trị k được bên gửi sử dụng để tạo chữ ký (r, s) trên thông điệp m thì kẻ tấn công có thể khôi phục khóa riêng của bên gửi vì $d = r^{-1}(ks - e) \mod n$. Do đó giá trị k này phải được tạo, lưu trữ và hủy an toàn sau khi chúng được đã sử dụng.

Giá trị k bí mật trên mỗi thông điệp được sử dụng để ký nên được tạo độc lập với nhau. Cụ thể, một giá trị bí mật k khác nên được tạo cho mỗi thông điệp khác nhau; nếu không, khóa riêng d có thể được khôi phục. Lưu ý rằng nếu bộ tạo số ngẫu

nhiên hoặc giả ngẫu nhiên an toàn được sử dụng thì cơ hội tạo một giá trị k lặp đi lặp lại là không đáng kể.

Các tham số miền cho ECDSA

Bảng 3 cung cấp thông tin liên quan tới việc xác định mức an toàn ứng với kích thước khóa của ECC cũng như thời gian đảm bảo an toàn theo SEC1 [4]. Tuy nhiên tùy thuộc mỗi quốc gia, khi triển khai vận dụng có thể có những thay đổi theo hướng nâng cao độ an toàn (Thông tư số 23/2022/TT-BQP của Bộ Quốc phòng có khuyến nghị tham số khóa ≥ 256 bit của ECDSA được sử dụng cho tới năm 2027 [7]).

Bảng 3. Tham số an toàn cho ECDSA [6]

Mức an toàn của một mã đối xứng	Kích thước khóa của ECC	An toàn tới năm
80	160	2010
112	224	2030
128	256	2040
192	384	2080
256	512	2120

Bảng 4 là khuyến nghị của NIST về loại đường cong và mức an toàn tương ứng (xem chi tiết các tham số miền được NIST khuyến nghị cho các loại đường cong elliptic (mục 3.2, 3.3 [3]).

Bảng 4. Độ an toàn của các đường cong khuyến nghị [3]

Mức độ an toàn (tính bằng bít)	Các đường cong khuyến nghị
112	P-224, K-233, B-233
128	P-256, W-25519, Curve25519, Edwards25519, K-283, B-283
192	P-384, K-409, B-409
224	W-448, Curve448, Edwards448, E448
256	P-521, K-571, B-571

Ngoài ra, các tham số miền ECDSA có thể được tạo như được chỉ định trong ANS X9.142; khi các tham số miền ECDSA được tạo (tức là các đường cong khuyến nghị của NIST không được sử dụng), giá trị của G phải được tạo theo quy tắc (ngẫu nhiên có thể kiểm chứng). Một hàm băm đã được phê duyệt (là bắt buộc trong quá trình tạo tham số miền) sẽ được sử dụng trong quá trình tạo tham số miền ECDSA. Khi tạo các tham số miền này, mức độ bảo mật của hàm băm được sử dụng sẽ đáp ứng hoặc vượt quá mức độ bảo mật liên quan đến độ dài bit của n. Nó được khuyến nghị rằng độ an toàn được liên kết với độ dài bit n và mức độ bảo mật của hàm băm là như nhau trừ khi có thỏa thuận giữa các thực thể tham gia sử dụng hàm băm mạnh hơn.

KẾT LUẬN

ECDSA hiện đang được khuyến nghị sử dụng trong rất nhiều tiêu chuẩn cả trong và ngoài nước. Có một số tấn công đối với ECDSA tuy nhiên bài toán ECDLP được xem là bài toán khó, không những vậy, cho tới nay chưa có nghiên cứu nào cho thấy có các cuộc tấn công hiệu quả lên ECDSA vì vậy ECDSA vẫn là lược đồ ký số đảm bảo an toàn và ngày càng được sử dụng nhiều trong thực tiễn. Các tham số miền cũng có tác động tới độ an toàn của ECDSA thường được lựa chọn theo các khuyến nghị của các tiêu chuẩn nổi tiếng trên thế giới như ANSI X9.142, NIST SP 800-186,... tùy theo mức độ an toàn mong muốn trong từng ứng dụng.❖

TÀI LIỆU THAM KHẢO

[1]. *FIPS PUB 186-5, February, 2023, "Digital Signature Standard (DSS)" .*

[2]. *Don Johnsonand Alfred Menezes, and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Dept. of Combinatorics & Optimization, University of Waterloo, Canada.*

[3]. *NIST SP 800-186, February, 2023. "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters".*

[4]. *Daniel R. L. Brown, "SEC 1: Elliptic Curve Cryptography", Certicom Corp, 2009.*

[5]. *Jiaxu Bao, "Research on the Security of Elliptic Curve Cryptography", Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022).*

[6]. *Daniel R. L. Brown, "SEC 1: Elliptic Curve Cryptography", Certicom Corp, 2009.*

[7]. *QCVN 12: 2022/BQP, "Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPSEC và TLS, BQP", 2022.*

[8]. *A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE, 2005, pp. 324-328.*