BG Bài 5.3 Sơ đồ chữ ký trên đường cong Elliptic

1. Thuật toán ký trên đường cong Elliptic (ECDSA)

Thuật toán chữ ký số Elliptic Curve [6] lần đầu tiên được đề xuất vào năm 1992 bởi Scott Vanstone trong phản hồi đề xuất của NIST về DSS.

Sau đó, nó đã được chấp nhận vào năm 1998 như là một tiêu chuẩn ISO (ISO 14888-3), và như là một tiêu chuẩn ANSI (ANSI X9.62) vào năm 1999, và như là một tiêu chuẩn của IEEE (IEEE 1363-2000) và như một tiêu chuẩn NIST (Trin 186-2) vào năm 2000.

Thuật toán chữ ký số đường cong Elliptic thực hiện theo 3 giai đoạn:

1. Tạo khóa,
2. Tạo chữ ký ,
3. Xác minh chữ ký.

Một giai đoạn thiết lập phải thực hiện trước giai đoạn tạo khóa để tạo miền tham số của hệ mật .

Miền tham số của một đường cong elliptic mô tả một tả đường cong Elliptic E được xác định trên một trường hữu hạn Fp, một điểm cơ sở g ∈E (Fp) có cấp là n. Các các tham số nên được chọn cẩn thận để ECDLP chống lại tất cả các cuộc tấn công đã biết.

Các đường cong elip được chọn bằng cách chọn (a, b) thuộc Z_p* và thay vào trong phương trình. Vì vậy, miền các tham số có thể được định nghĩa là p, E_p(a, b), g, n.

a) Tạo cặp khóa dùng trong ECDSA:

Giả sử A là người ký trên bản rõ M. Khi đó A thực hiện các bước sau để tạo ra cặp khóa công khai và khóa riêng:

(1) Chọn ngẫu nhiên 1 số nguyên d nằm trong khoảng [1, n-1]

(2) Tính Q = dg

(3) Khóa riêng của người gửi là d

(4) Khóa công khai của người gửi là tổ hợp (E_p(a, b), g, n, Q)

b) Tạo chữ ký bằng ECDSA

A sử dụng khóa riêng của mình để tạo chữ ký trên bản tin M bằng các bước sau:

(1) Chọn ngẫu nhiên một số nguyên k thuộc [1, n-1]

(2) Tính kg = (x_1 , y_1), trong đó x_1 là số nguyên

(3) Tính r = x_1 mod n; Nếu r = 0, thì quay lại bước 1

(4) Tính h = H (M), trong đó H là SHA-512

(5) Tính s = (h + d*r)* (k ^(- 1)) mod n; Nếu s = 0, thì quay lại bước 1

(6) Chữ ký của A trên bản tin M là cặp số nguyên (r, s).

C) Xác thực chữ ký bằng ECDSA

Người nhận B có thể xác minh tính xác thực của chữ ký của A là (r, s) trên bản tin M bằng cách thực hiện tiếp theo:

(1) Nhận được chữ ký trên Khóa công khai (E, g, n, Q) của A.

(2) Xác minh rằng các giá trị r và s nằm trong khoảng [1, n-1]

(3) Tính w = s ^(- 1) mod n.

(4) Tính h = H (M), trong đó H là thuật toán băm an toàn tương tự được sử dụng bởi A.

(5) Tính $u_1 = hw \bmod n$

(6) Tính $u_2 = rw \bmod n$

(7) Tính $u_1 g + u_2 Q = (x_0, y_0)$

(8) Tính $v = x_0 \bmod n$

(9) Chữ ký cho tin nhắn M chỉ được xác minh nếu v = r

d) Tính an toàn của ECDSA

Khóa công khai được tạo bằng cách tính điểm Q, trong đó Q = dg. Để phá vỡ khóa đường cong elip elliptic, Eve (người thám mã) có thể khám phá ra khóa bí mật d khi Q và g được công bố. Bậc của đường cong Elliptic, E là số nguyên tố n, sau đó tính toán d từ dg và g sẽ mất khoảng

2^(2n + 2) phép tính [7]. Ví dụ: nếu độ dài khóa n là 192 bit (khóa nhỏ nhất kích thước mà NIST đề xuất cho các đường cong được xác định trên GF (p)), khi đó Eve sẽ thực hiện khoảng 2^296 phép tính. Nếu Eve có một siêu máy tính và có thể thực hiện một tỷ phép tính mỗi giây, anh ta sẽ mất khoảng hai nghìn tỷ năm để tìm ra khóa bí mật.

Có được điều này do độ khó của bài toán logarithm rời rạc ở phía sau ECDSA. Các tham số của đường cong nên được chọn rất cẩn thận để bảo đảm đường cong Elliptic tránh khỏi các cuộc tấn công như Pollard rho [1] và PohligHellman.

e) **Chứng minh tính hợp thức của thuật toán ký trên đường cong elliptic ECDSA**

Chữ ký được A gửi đến B là (r, s) và s chỉ có thể được tạo bởi A vì chỉ A biết khóa riêng d:

s = (k^(-1)) (h + dr) mod n.

- K = (s^(-1)) (h + dr)
- Kg = (s^(-1)) (h + dr) g
- Kg = (s^(-1))hg + (s^(-1))drg

- r = hwg + rwdg
- r = u1g + u2Q

f) Cuộc tấn công có thể lên ECDSA

Nếu số bí mật k được sử dụng để ký hai hoặc nhiều tin nhắn thì sự độc lập của các chữ ký trên các tin nhắn có thể bị phá vỡ. Cụ thể, nếu số bí mật k được sử dụng để ký lên hai tin nhắn khác nhau thì khóa riêng d có thể được phục hồi.

Tuy nhiên, nếu một số k ngẫu nhiên hoặc giả ngẫu nhiên an toàn được sử dụng, thì cơ hội xảy ra số trị k lặp lại là không đáng kể. Nếu cùng số bí mật k được sử dụng để tạo chữ ký của hai thông điệp khác nhau m1 và m2, sau đó nó sẽ dẫn đến hai chữ ký (r, s1) và (r, s2).

- s1 = k-1(h1 + dr)
- s2 = k-1(h2 + dr) ; where h1 = SHA512 (m1) and h2 = SHA512 (m2).
- ks1- ks2 = h1+dr-h2-dr

  $k=(h_1-h_2)/(s_1 - s_2)$

  $d = (ks - h)/r.$

2. **Sơ đồ chữ ký số kiểu Đức trên đường cong Elliptic (Elliptic Curve German Digital Signature Algorithm - ECGDSA)**

Một trong những nhược điểm của sơ đồ ECDSA là phải tính nghịch đảo trong giai đoạn ký. Tính nghịch đảo là một trong những hoạt động tốn kém trong

Số học mô-đun, vì vậy để giảm chi phí và thời gian, trong ECGDSA phép tính nghịch đảo được thực hiện trong giai đoạn tạo cặp khóa và không phải trong giai đoạn ký.

Một khóa sẽ không đổi trong một khoảng thời gian ổn định để việc ký được thực hiện nhiều hơn, thường xuyên hơn bản chính. ECGDSA sẽ tiết kiệm thời gian và chi phí hơn ECDSA.

a) Sinh ra cặp khóa khi sử dụng ECGDSA:

Giả sử A là người ký trên bản tin M. Thực thể A thực hiện các bước sau để tạo ra cặp khóa riêng và khóa công khai.

(1) Chọn ngẫu nhiên và duy nhất môt số nguyên, d, trong khoảng [1,n-1]

(2) Q ← (d^-1 mod n)*g

(3) Khóa riêng của người gửi A là d

(4) Khóa công khai của người gửi A là tổ hợp (E_p(a, b), g, n, Q).

b) Thực hiện thủ tục tạo ra chữ ký khi sử dụng ECGDSA

A dùng khóa riêng của mình để tạo ra chữ ký trên bản tin M khi thực hiện các bước sau:

(1) Chọn ngẫu nhiên và duy nhất số nguyên k trong khoảng [1,n-1]

(2) $kg \leftarrow (x_1, y_1)$, ở đây x_1 là một số nguyên

(3) r ← x_1 mod n; nếu r = 0, thì quay lại bước 1

(4) h ← H(M), ở đây H là hàm băm SHA-512

(5) s ← (kr-h) d mod n; nếu s = 0, thì quay lại bước 1

(6) Chữ ký của A trên bản tin M là cặp số (r,s).

c) Kiểm thử chữ ký khi sử dụng ECGDSA

Người nhận B có thể kiểm thử tính xác thực chữ ký của A là (r, s) trên bản tin M bởi việc thực hiện các bước sau:

(1) Nhận được khóa công khai của A là (E, g, n, Q)

(2) Kiểm thử xem các giá trị r và s có thuộc khoảng [1,n-1]

(3) w ← r^-1 mod n

(4) h ← H(M), ở đây H cùng là

hàm băm an toàn được A sử dụng

(5) $u_1 \leftarrow hw \bmod n$

(6) $u_2 \leftarrow sw \bmod n$

(7) $(x_0,y_0) \leftarrow u_1g + u_2Q$

(8) $v \leftarrow x_0 \bmod n$

(9) Chữ ký trên bản tin M chỉ được xác nhận nếu $v = r$

d) Chứng minh tính hợp thức của Sơ đồ

Người gửi A gửi chữ ký tới B là (r, s) và s chỉ có thể tạo bởi chỉ có A mới biết khóa riêng d: s =(kr – h)d (modn)

- s = (kr-h) d
- s * r^-1*d^-1 = (kh * r^-1)
- sw*d^-1g = kg – hw* g
- kg = hw*g + sw*Q
- r = u1g+u2Q

Nếu cùng số bí mật (k) được

dung để ký lên hai bản tin khác nhau, nó sẽ tạo ra 2 chữ ký khác nhau (r, s_1) và (r, s_2).

- $s1 = (kr-h1)\ d$
- $s2 = (kr-h2)\ d$, ở đây $h1 = SHA512\ (m1)$ và $h2 = SHA512\ (m2)$
- $s1-s2= h2-h1$

Khi đó không thể xác định được k mặc dầu cùng một số bí mật được dùng để ký lên hai bản tin khác nhau. Bởi vậy, sơ đồ này không dễ bị tấn công khi dùng cùng một số bí mật.

Ví dụ của ECGDSA trên GF(p) với hàm băm RIPEMD - 160

Ví dụ ECGDSA trên GF(p) với đường cong elliptic 192 bit brainpoolP192r1 và hàm băm RIPEMD – 160 .

Đường cong brainpoolP192r1 có số nguyên tố p là:

p = C302F41D 932A36CD A7A34630 93D18DB7 8FCE476D E1A86297

gồm 192 bit.

Phương trình đương cong elliptic E: y2 = x3 + ax + b, với a, b được cho:

a = 6A911740 76B1E0E1

9C39C031 FE8685C1

CAE040E5 C69A28EF

và

b = 469A28EF 7C28CCA3

DC721D04 4F4496BC

CA7EF414 6FBF25C9.

Số phần tử của nó là: #E(GF(p))

= q,

ở đây

q = C302F41D 932A36CD

A7A3462F 9E9E916B

5BE8F102 9AC4ACC1

là một số nguyên tố 192-bit. G

= (x(G), y(G)) với

x(G) = C0A0647E AAB6A487

53B033C5 6CB0F090

0A2F5C48 53375FD6

và

y(G) = 14B69086 6ABD5BB8

8B5F4828 C1490002

E6773FA2 FA299B8F

là một điểm có bậc q trên E.

Khóa riêng và khóa công khai của người ký là:

Để làm khóa riêng, người ký A chọn ngẫu nhiên số nguyên dA $\in \{1, . . . , q - 1\}$:

dA = 80F2425E 89B4F585

F27F3536 ED834D68

E3E492DE 08FE84B9.

Như là khóa công khai của A là

điểm PA = (d_A $^{-1}$ mod q) · G

vcowsi các tọa độ:

x(PA) = BCAD67EA E3563528

FEDCBDD8 FC5DA1EE

64123AE0 8BD476B0

và

y(PA) = A9ED7D6B

7B9D2929 5DEA48BA

01D3C8B5 6E736885 22A28A04.

Khởi tạo chữ ký:

Giả sử m là bản tin được mã theo ASCII sau “Example of ECGDSA with the hash function RIPEMD-160”. Khi đó, giá trị băm theo RIPEMD-160 hash của m (với việc cộng thêm 0 vào phần cuối) là

RIPEMD-160(m) = 00000000

577EF842 B32FDE45

79727FFF 02F7A280

74ADC4EF.

Người ký A chọn ngẫu nhiên số

nguyên k ∈ {1, . . . , q - 1}:

k = 22C17C2A 367DD85A

B8A365ED 06F19C43

F9ED1834 9A9BC044.

Khi đó, r = x(k · G) mod q là

r = 2D017BE7 F117FF99

4ED6FC63 CA5B4C7A

0430E9FA 095DAFC4.

Giá trị s = (k · r - RIPEMD-

160(m)) · dA mod q bằng

s = C02B5CC5 C51D5411

060BF024 5049F824

839F671D 78A1BBF1.

Cặp (r, s) là chữ ký của A trên

bản tin m.

Kiểm thử chữ ký:

r và s như ở trên thuộc vào tập

{1, . . . , q - 1}.

Giá trị băm bởi RIPEMD-160

trên bản tin “Example of

ECGDSA with the hash

function RIPEMD-160” là

RIPEMD-160(m) = 00000000

577EF842 B32FDE45

79727FFF 02F7A280

74ADC4EF.

Giá trị u1 = $r^{-1} \cdot$ RIPEMD-160(m) mod q là

u1 = 06664D48 33E54C21 58B4275E D63DE697 B8101E9B C5718A8A.

u2 = $r^{-1} \cdot s$ mod q bằng

u2 = 240B83FE 9A1DA756 D2C68A06 43EC2052

74F085A6 BFA868D2.

x(u1 · G + u2 · PA) mod q là

2D017BE7 F117FF99

4ED6FC63 CA5B4C7A

0430E9FA 095DAFC4,

nó bằng với r, như vậy cặp số

(r, s) được chấp nhận là chữ ký

của A trên bản tin m.

Ví dụ và Bài tập

Computations on Elliptic Curves – Example 1

- Example: Given $E: y^2 = x^3+2x+2 \bmod 17$ and point $P=(5,1)$
  Goal: Compute $2P = P+P = (5,1)+(5,1)= (x_3, y_3)$

$$s = \frac{3x_1^2 + a}{2y_1} \bmod p = (2\cdot 1)^{-1}(3\cdot 5^2+2) = 2^{-1}\cdot 9 \equiv 9\cdot 9 \equiv 13 \bmod 17$$

$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \bmod 17$$
$$y_3 = s(x_1-x_3) - y_1 = 13(5-6) - 1 = -14 \equiv 3 \bmod 17$$

Finally $2P = (5,1) + (5,1) = (6,3)$

Verify that (6,3) is a point on the curve:

$3^2 = 9,\ 6^3 + 12 + 2 = 36\cdot 6 + 14 \equiv 2\cdot 6 + 14 = 26 \equiv 9 \bmod 17$

$P+2P=(5,1)+(6,3)=(10,6)$ since

$$s = \frac{y_2 - y_1}{x_2 - x_1} \bmod p = (3-1)/(6-5) = 2\,(1)^{-1} \equiv 2 \bmod 17$$
$$x_3 = s^2 - x_1 - x_2 = 4 - 11 = -7 \equiv 10 \bmod 17;$$
$$y_3 = s(x_1 - x_3) - y_1 = -10 - 1 = -11 \equiv 6 \bmod 17$$

ECE597/697 Koren Part.9 .9

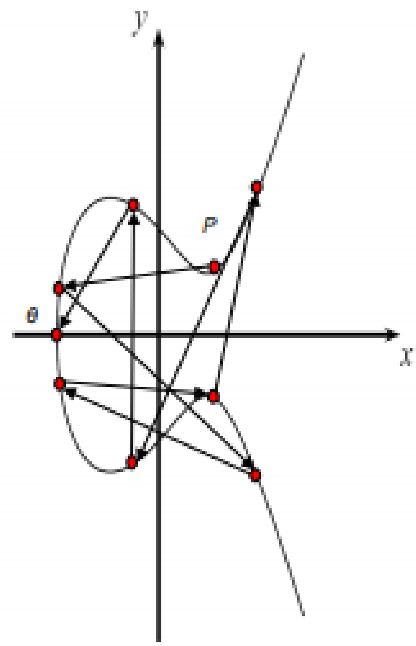
Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources

Example 1 (ctd.)

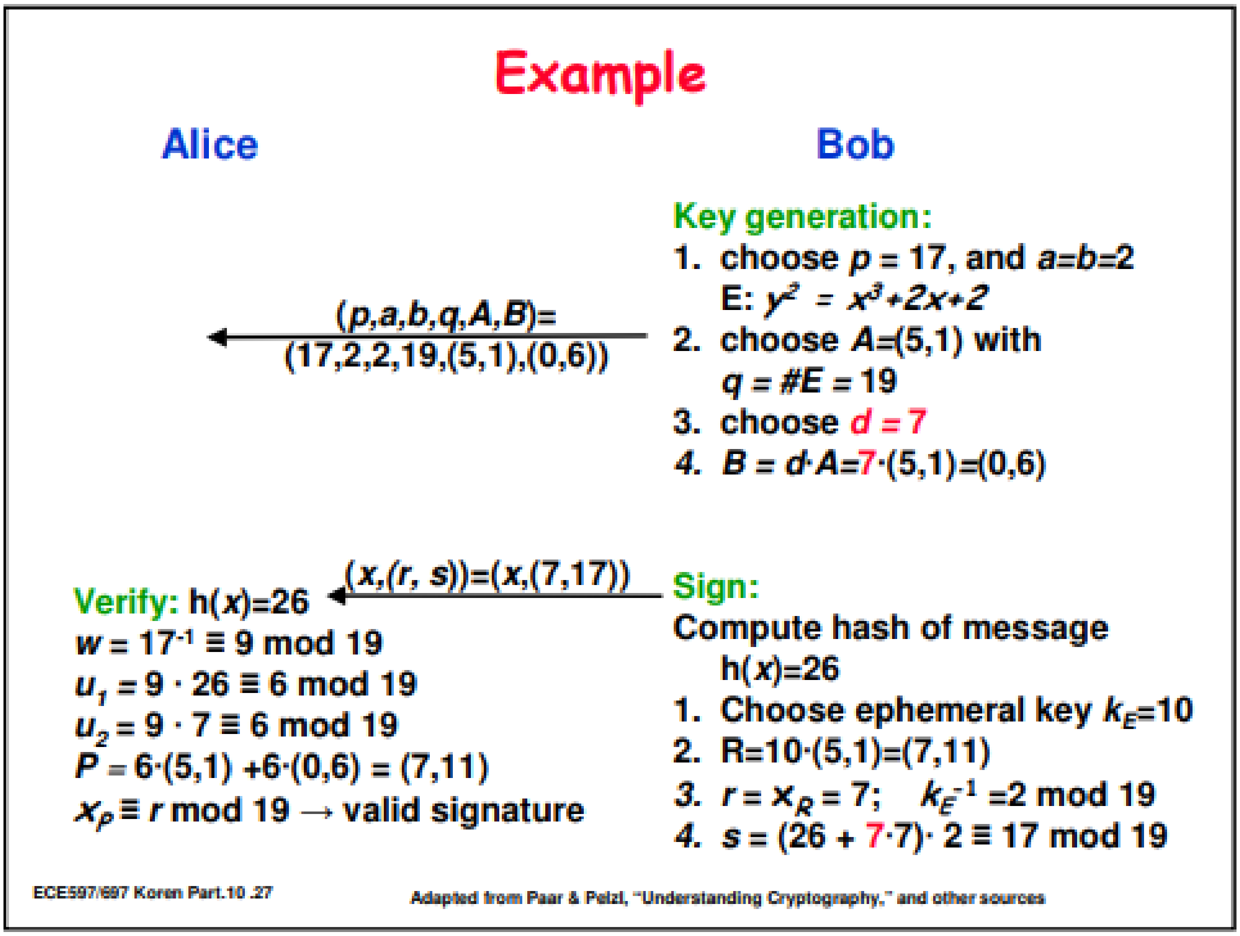
- The points on an elliptic curve and the point θ form cyclic subgroups

2P = (5,1)+(5,1) = (6,3);	*11P = (13,10)*
3P = 2P+P = (10,6)	*12P = (0,11)*
4P = (3,1)	*13P = (16,4)*
5P = (9,16)	*14P = (9,1)*
6P = (16,13)	*15P = (3,16)*
7P = (0,6)	*16P = (10,11)*
8P = (13,7)	*17P = (6,14)*
9P = (7,6)	*18P = (5,16)*
10P = (7,11)	*19P = θ*

This elliptic curve has order #E = |E| = 19 since it contains 19 points in its cyclic group.



Adapted from Paar & Pelzl, "Understanding Cryptography," and other sources



Bài tập 1 (ECDSA): h(x)=số hóa chữ cái đầu tên của sv+5, d= lấy số cuối ngày sinh + 3, k_E=số cuối tháng sinh + 5.

Ví dụ với Nguyễn Thành Nam 4/4/1999

h(x)=18, d=7. K_E = 9.

Bài tập 2 (ECGDSA): h(x)=số hóa chữ cái đầu tên của sv+5, d= lấy số cuối ngày sinh + 3, k_E=số cuối tháng sinh + 5.

Bài tập về nhà

Bài tập 1. Sơ đồ chữ ký ECDSA

Cho đường cong (E) $y^2 = x^3+ax+b(modp)$, với p là số nguyên tố lớn hơn 29.

a) Chọn p và a, b thích hợp để số phần tử của (E) là 1 số nguyên tố. Ví dụ,

$y^2 = x^3+5x+7(mod29)$, ta có #(E)=37.

Tìm tất cả các điểm của (E)

b) Chọn 1 điểm g trên (E) làm điểm sinh.
   Xây dựng hệ mật khóa công khai trên (E) với khóa mật d= số cuối ngày sinh + 3.
c) Dùng hệ mật ở phần b) để ký trên h(x)=số hóa chữ cái đầu tên của sv+5, d= lấy số cuối ngày sinh + 3, k_E=số cuối tháng sinh + 5.
d) Kiểm thử chữ ký.

Bài tập 2. Sơ đồ chữ ký ECGDSA

Cho đường cong (E) $y^2 = x^3+ax+b(\mathrm{mod}\,p)$, với p là số nguyên tố lớn hơn 29.

a) Chọn p và a, b thích hợp để số phần tử của (E) là 1 số nguyên tố. Ví dụ,

$y^2 = x^3+5x+7(\mathrm{mod}\,29)$, ta có #(E)=37.

Tìm tất cả các điểm của (E)

b) Chọn 1 điểm g trên (E) làm điểm sinh.

Xây dựng hệ mật khóa công khai trên (E) với khóa mật d= số cuối ngày sinh + 3.

c) Dùng hệ mật ở phần b) để ký trên h(x)=số hóa chữ cái đầu tên của sv+5, d= lấy số cuối ngày sinh + 3, k_E=số cuối tháng sinh + 5.

d) Kiểm thử chữ ký.

Bài tập 3. Hai sinh viên hợp vừa gửi vừa nhận với bản tin x = số hóa tên của sv.

Nội dung 1. Ký trên x với h(x)= số hóa tên sv (modp).

Nội dung 2. Mã hóa x và chữ ký (r, s) bằng hệ mật EC - ElGamal và **Massey-Omura** của đối tác và gửi cho đối tác.

Nội dung 3. Giải mã và xác thực chữ ký của đối tác.

Giải

1
4
9
16
25
7
20
6
23
13
5
28
24
22

$A = (7, 11)$, $d=12$, $B= (16, 13)$
Khóa công khai:
$(p, a, b, n, A, B) = (17, 2, 2, 19, (7, 11), (16, 13))$.
Ký: $h(x) = 12$, $k_E = 15$, $R =(6, 14)$,
$k_E^{-1} = 14$, $s = (12 +12*6)*14 \bmod 19 = 17$;
$(r, s) = (6, 17)$
Kiểm thử: $w = s^{-1}=17^{-1}=9 \bmod 19$
$u_1 = 13$, $u_2 = 16$, $P = (6, 14)$