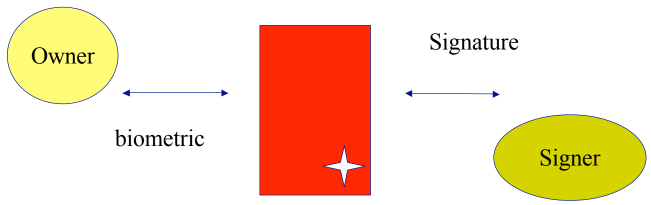
Open Source Is Not Enough

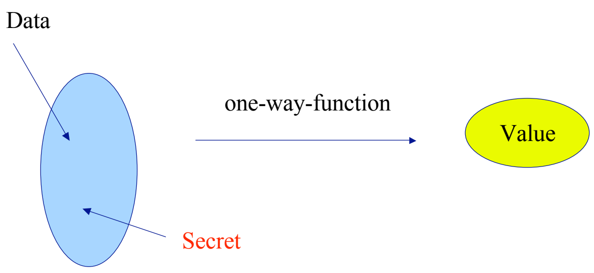
An Attack on BouncyCastle ECC

Daniel Mall

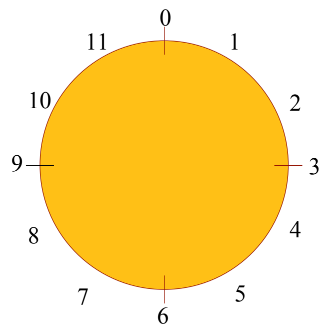
Passports



Signature



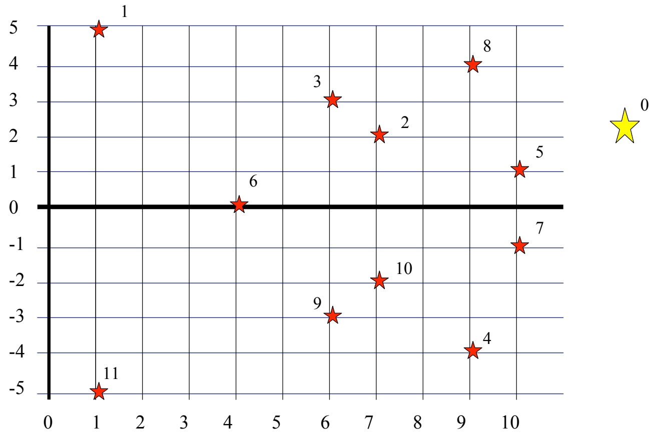
Discrete Logarithm



Cyclic Group G = (Z_{12}, +, 0)

1. G = <1>
   X * 1 = 7 mod 12
2. G = <5>
   X * 5 = 7 mod 12
   Euclidean Alg: Fast
3. After a permutation ?

Another Representation



Elliptic Curves

Z_p a prime field , $p > 3$

$a , b \in Z_p$

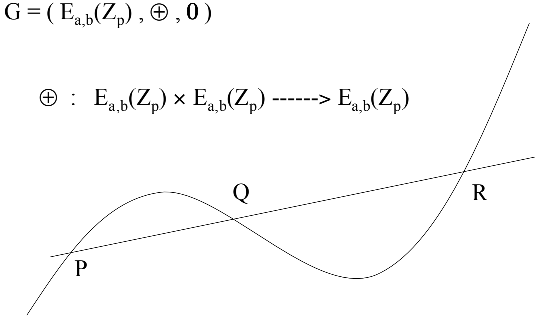
$E_{a,b}(Z_p) = \{ (x,y) \in Z_p \times Z_p : y^2 = x^3 + ax + b \} \cup \{0\}$

Our example: $p = 11$, $a = 0$, $b = 2$

Group Structure

$G = (E_{a,b}(Z_p) , \oplus , \mathbf{0})$

$\oplus$: $E_{a,b}(Z_p) \times E_{a,b}(Z_p)$ ------> $E_{a,b}(Z_p)$



$P \oplus Q \oplus R = \mathbf{0}$

Group Structure

$G = (E_{a,b}(Z_p) , \oplus , \mathbf{0})$

$\oplus$: $E_{a,b}(Z_p) \times E_{a,b}(Z_p)$ ------> $E_{a,b}(Z_p)$

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E_{a,b}(Z_p) \setminus \{0\}$

$P_3 = (x_3,y_3) := P_1 \oplus P_2$

1. $P_1 \neq P_2$: $\lambda = (y_2 - y_1) / (x_2 - x_1)$

   $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda (x_1 - x_3) - y_1$

2. $P_1 = P_2$: $\lambda = (3x_1^2 + a) / (2y_1)$

   $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda (x_1 - x_3) - y_1$

ECDLP

Given: $P \in E_{a,b}(Z_p)$

$Q \in \langle P \rangle$

Problem: Find $k \in IN$ with $Q = k\,P$

Diffie-Hellman-Protocol

Parameter: $E_{a,b}(Z_p)$ and $P \in E_{a,b}(Z_p)$

d_A // private key of Alice

d_B // private key of Bob

Alice -----> Bob : $Q_A = d_A\,P$ // Bob : $K_B = d_B\,Q_A$

Bob -----> Alice : $Q_B = d_B\,P$ // Alice: $K_A = d_A\,Q_B$

$$K_A = d_A\,Q_B = d_A\,d_B\,P = d_B\,d_A\,P = d_B\,Q_A = K_B$$

Implementation (BouncyCastle)

class ECPoint

Methods

P. add (Q) // $P \oplus Q$ // without contract

P. twice ( ) // $P \oplus P$

P. multiply(k) // $k\,P$ // with NAF

Non-Adjacent Form (NAF)

Remark:

Let $P = (x,y) \in E_{a,b}(Z_p)$, p>3, ==> $-P = (x, -y)$

$R \oslash P := R \oplus (-P)$

Subtraction of points on an elliptic curve is as efficient as addition

Naf: $n = \Sigma_{0 \le i \le l-1}\ k_i\,2^i$ // $k_i \in \{ -1, 0, 1 \}$

$k_i\,k_{i+1} = 0$, $i = 0, \ldots, l-2$

30 P

Double-and-Add

$30 = (11110)_2$

$30\,P = 16\,P \oplus 8\,P \oplus 4\,P \oplus 2\,P$ // $\# \oplus = 7$

Naf

naf (30) = (1 0 0 0 –1 0) // 30 = 32 – 2

$30\,P = 32\,P \oslash 2\,P$ // $\# \oplus \oslash = 6$

Implementation (BouncyCastle)

Representation of **0** : virtual

$\mathbf{0} = P \oplus (-P) = (x, y) \oplus (x, -y)$

==> $\lambda = ((-y) - y) / (x - x)$

==> Java throws an ArithmeticException

0 is represented by the occurrence of an ArithmeticException

BouncyCastle v. 1. x_132

$E_{2,1}(Z_7) = \{ (0, 1), (0, -1), (1, 2), (1, -2) \} \cup \{0\}$

$P = (1, 2)$ // $ord(P) = 5$

$2\,P = (0, 1)$, $3\,P = (0, -1)$, $4\,P = (1, -2)$

P.multiply(3): naf (3) = (1 0 –1)

P. twice( ) = $P \oplus P$, 2P. twice( )= $2\,P \oplus 2\,P$

4P. add(–P) = $4\,P \oslash P = 3\,P$

But $4\,P = -P$. Hence $3\,P = (-P)$. add(–P)

==> ArithmeticException

Result

Let $E_{a,b}(Z_p)$ be an elliptic curve

and $P \in E_{a,b}(Z_p)$ with $n = ord(P) \equiv 1 \bmod 4$.

Then calling

P.multiply(n – 2)

BouncyCastle version 1.x_132 throws an

ArithmeticException.

Hence, we can claim that $ord(P) = n - 2$

A Dangerous Curve

$E_{a,b}(Z_p)$ with $p = 48611$

$a = -3, \quad b = 38351$

numberOfPoints = 48613 = 173 * 281 ≡ 1 mod 4

P = (39565 , 18995) // a point on the curve

ord(P) = 48613

ord(P) – 2 = 48611 ∈ IP

Faked Domain Parameters

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

n = ord (P)

h = numberOfPoints / n

D = (48611 , - , - , -3 , 38351 , (39565 , 18995) , 48611 , 1)

EC Validation

D = (q , FR , S , a , b , P = (x, y) , n , h) ...

$P \in E_{a,b}(Z_p) \setminus \{0\}$

...

----> n P = **0** // point counting is difficult

$n \mid (p^k - 1)$ ==> $20 < k$

$n \neq p$

A real example: –– / Qing Zhong: Open Source is not enough