Kryptography for Dummies

Michael Wacenovsky (2016)

How does ECDSA work ?

Elliptic curves are sets of tuples (x,y), with x and y related by a cubic equation. For ECDSA $x,y \in GF(p)$, with a large prime p.
A special binary operation $\oplus$ imposes a group property onto the set of tuples:

In particular:

- With $A, B \in EC$ $A \oplus B = C \in EC$
- There is a neutral Element $\varnothing \in EC$
- For each $A \in EC$ there is an inverse Element A^{-1}, so that $A \oplus A^{-1} = \varnothing$
- The scalar multiple is defined as the sum of k A's: $kA = \underbrace{A \oplus A \oplus \ldots \oplus A}_{k}$

It is possible to find a cyclic subgroup EC(G;n) of group order n, whose elements are scalar multiples of a single generating point G: $X = kG$, $k < n$; $nG = \varnothing$.

Cryptographic operations are executed within this subgroup. The order of the subgroup EC(G;n) is typically equal or of the same order of the original group, which is about p.

Similar to the discrete logarithm problem, for big group order n it is practically infeasable to calculate k back from a known kG. This is the hearth of ECDSA.

How does ECDSA work ?

signing process

$d < n$ … private key

$Q = dG$ … public key (x, y)

she chooses $k < n$ … random number

$kG = (x_1, y_1) \longrightarrow r = x_1 \bmod n$

hash from message: $e \longrightarrow s = k^{-1}(e \oplus dr) \bmod n$

signature = (r,s)

verification process

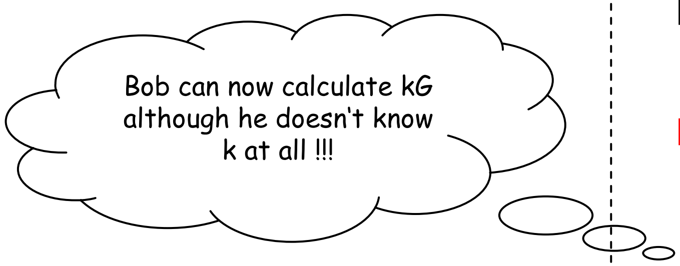
he knows that: $k = s^{-1}(e \oplus dr) \bmod n$

$$kG = (s^{-1} e \bmod n \oplus s^{-1} dr \bmod n)G =$$

$$= (s^{-1} e \bmod n)\ G \oplus (s^{-1} dr \bmod n)\ G$$

$$= (s^{-1} e \bmod n)\ G \oplus (s^{-1} r \bmod n)\ Q := (x_2, y_2)$$

$r == x_2 \bmod n$??



GF(q) …q prime
G … generator of sub group with
prime order $n < q$

Michael Wacenovsky (2016)

How does ECC Diffie-Hellman work ?

Alice chooses $a < n$ … private key

$aG = A$ → Alice's Public key A

Bob chooses $b < n$ … private key

$bG = B$ → Bob's Public key B

she calculates : $s_a = aB = abG = (x_a \mid y_a)$

he calculates : $s_b = bA = baG = (x_b \mid y_b)$

because G is generator of an abelian group,

$x_a = x_b, y_a = y_b$

→ Alice and Bob share the same secret !!

GF(q) …q prime
G … generator of sub group with
prime order $n < q$

Michael Wacenovsky (2016)