The Elliptic Curve Digital Signature Algorithm (ECDSA)

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it

1

ECDSA

INTRODUCTION

2

- Conceptually, ECDSA is closely related to DSA
  - DLP is constructed in the group of EC
  - Arithmetic is performed in Zp* and GF(2^m)
  - We focus on Zp*
    - Preferrend in practice to GF(2^m)

Elliptic Curve DSA (ECDSA)

- ECDSA was standardized in US by ANSI in 1998
- Pros
  - ECC allow 160-256-bit lengths which provide a security level equivalent to 1024-3072-bit RSA/DL
    - Shorter processing time
    - Shorter signatures
- Cons
  - Finding EC with good cryptographic properties in nontrivial
  - Standardize curves by NIST or Brainpool consortium

ECDSA

THE CRYPTOSYSTEM

Key Generation

UNIVERSITÀ DI PISA

1. Select domain parameters
   - modulus p
   - Elliptic curve E (coefficients a and b)
   - a point A which generates a cyclic group of prime order q
2. Choose a random integer *d* with $0 < d < q$.
3. Compute $B = d \cdot A$.
4. The keys are:
   1. kpub = (p,a,b,q,A,B)
   2. kpr = (d)

Signature generation

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $R = k_E \cdot A = (x_R, y_R)$
3. Let $r = x_R$.
4. Compute $s \equiv (H(x) + d \cdot r) \cdot k_E^{-1} \bmod q$.

Signature verification

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot H(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $P = u_1 \cdot A + u_2 \cdot B = (x_p, y_p)$.
5. The verification follows from:
   1. If $x_P \equiv r \bmod q$ ➔ valid signature
   2. Otherwise ➔ invalid signature

Proof

- We show that a signature (r, s) satisfies the verification condition r ≡xP mod q.
  1. $s \equiv (H(x)+d \cdot r)k_E^{-1} \bmod q$
  2. $k_E \equiv s^{-1} \cdot h(x) + d \cdot s^{-1} \cdot r \bmod q$.
  3. $k_E \equiv u_1 + d \cdot u_2 \bmod q$.
  4. $k_E \cdot A = (u_1 + d \cdot u_2) \cdot A$.
  5. $k_E \cdot A = u_1 \cdot A + d \cdot u_2 \cdot A$
  6. $k_E \cdot A = u_1 \cdot A + u_2 \cdot B$.
  7. Remember that $P = u_1 \cdot A + u_2 \cdot B$ and $R = k_E \cdot A$.
     - So, P = R and thus $x_P = x_R = r$ Q.E.D.

ECDSA

DISCUSSION

Computational aspects

UNIVERSITÀ DI PISA

- Key generation
  - Point multiplication
  - Doubl-and-add algorithm
  - Finding good EC is nontrivial
- Signing
  - point multiplication (r)
    - Precomputation is possible
  - EEA (s)
  - Hashing
  - Reduction modulo q

Computational aspects

UNIVERSITÀ DI PISA

- Verification
  - Two point multiplications
  - Techniques to make simultaneous point multiplications (exponentiations) faster

Security

- If E is chosen properly the main analytical attacks are against DLP
  - Square root attacks: running time in the order of $\mathcal{O}\left(\sqrt{q}\right)$
    - At least q must be on 160 bit (security level 80)
    - Security levels of 128, 192 and 256 are also chosen
    - H's output bit size = q bit size
- Avoid reusing ephemeral keys