Elliptic-curve cryptography X

Signatures – definitions and properties

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Public-key signatures

- Security goals: authenticity and integrity.
  Ensure that a message was really sent by Alice.
  Ensure that modifications to signed message get caught.
- In crypto, identity is often linked to, or equal to, a public key.
  Everybody knows that public key.
  Alice is the person who knows the private key for it.

Public-key signatures

- Security goals: authenticity and integrity.
  Ensure that a message was really sent by Alice.
  Ensure that modifications to signed message get caught.
- In crypto, identity is often linked to, or equal to, a public key.
  Everybody knows that public key.
  Alice is the person who knows the private key for it.
- Nobody can produce signatures valid under a public key
  without knowing the matching private key.
- Alice signs messages using her private key.
  Other people verify using her public key.

Public-key signatures

- Security goals: authenticity and integrity.
  Ensure that a message was really sent by Alice.
  Ensure that modifications to signed message get caught.
- In crypto, identity is often linked to, or equal to, a public key.
  Everybody knows that public key.
  Alice is the person who knows the private key for it.
- Nobody can produce signatures valid under a public key without knowing the matching private key.
- Alice signs messages using her private key.
  Other people verify using her public key.
- Note that a key pair for signing is separate from a key pair for encryption or Diffie–Hellman.

Signatures

Attacker goals

- Recover sk from pk.
- Produce forgeries on any message m.
  i.e., break universal unforgeability (UU).
- Create some forgery (no control over the message),
  i.e., break existential unforgeability (EU).

Signatures

Attacker goals

- Recover sk from pk.
- Produce forgeries on any message m.
  i.e., break universal unforgeability (UU).
- Create some forgery (no control over the message),
  i.e., break existential unforgeability (EU).
  This is bad even if the attacker does not have control over what message the forgery is on.

Attacker abilities

- Key only attack (KOA)
  Attacker only knows pk.
- Known message attack (KMA)
  Attacker knows some $(m, \mathrm{Sign}(m))$ pairs.
- Chosen message attack (CMA)
  Attacker can request signatures $(m, \mathrm{Sign}(m))$
  on messages m of his choice.