Security notiions for public-key cryptography

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Security notions

Some requirements are obvious

- It should be hard to recover the private key sk from a public key pk.
- It should be hard to recover the plaintext from a ciphertext.
- It should be hard to forge a signature.

Security notions

Some requirements are obvious

- It should be hard to recover the private key sk from a public key pk.
- It should be hard to recover the plaintext from a ciphertext.
- It should be hard to forge a signature.

But what powers does the attacker get?

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.

Encryption

Attacker goals

- Recover sk from pk.
- Recover m from $\mathsf{Enc}_{\mathsf{pk}}(m)$,
  i.e. break one-wayness (OW).
- Learn any information about plaintext (semantic security).

Encryption

Attacker goals

- Recover sk from pk.
- Recover m from $\mathsf{Enc}_{\mathsf{pk}}(m)$,
  i.e. break one-wayness (OW).
- Learn any information about plaintext (semantic security).
  Equivalent to breaking indistinguishability (IND),
  i.e., learning which of two attacker-chosen messages m_0, m_1 was encrypted in $c = \mathsf{Enc}_{\mathsf{pk}}(m_i)$ (beyond 50% chance of guessing.)

Attacker abilities

- Chosen plaintext attack (CPA)
  Attacker gets encryption of plaintexts of his choice.
- Chosen ciphertext attack (CCA I / II)
  Attacker can ask for decryptions of ciphertexts of his choice.
  For II the attacker can continue asking for decryptions after receiving a challenge ciphertext.