1. Digital Signatures

Digital signatures

Same as MACs are used in symmetric key to prove authentication, in public key cryptography we can **sing** messages to prove authenticity

Idea

- A trusted party can generate a signature on a document D
- Anyone in the world can verify that signature
- We use two keys: a signing key and a verifyig key

Algorithm

A signature scheme is a triplet of efficient algorithms (G, S, V) where

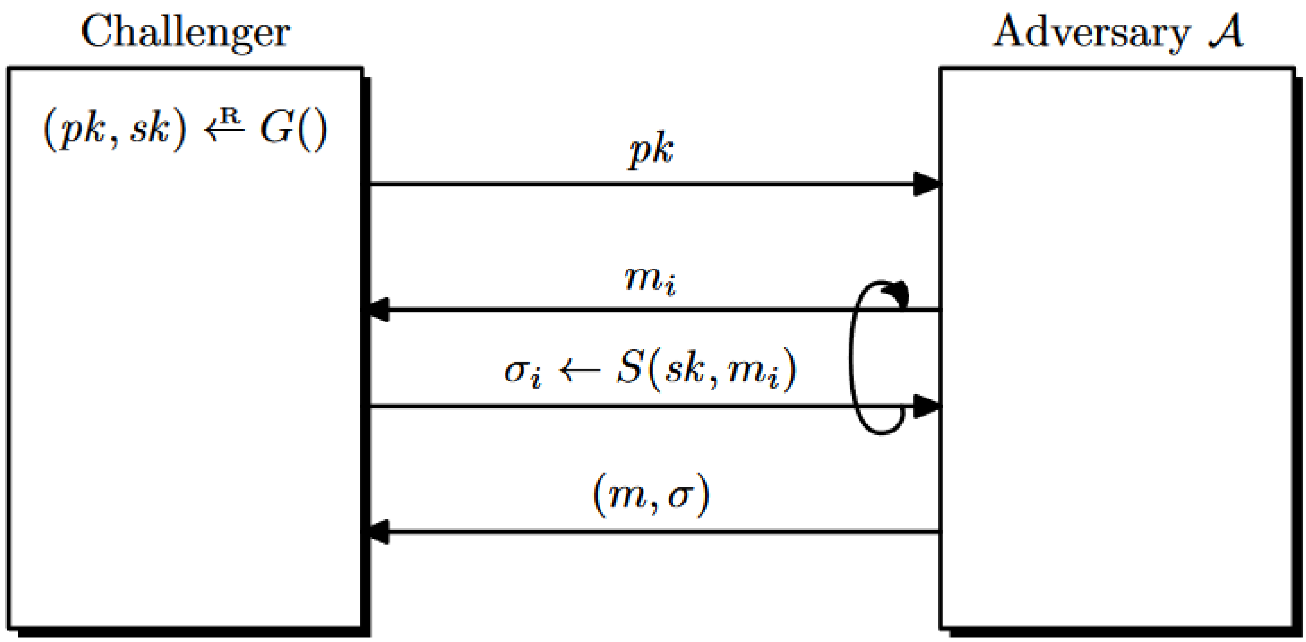
- G - key generation algoritm - *probabilistic* - $(k_{pub}, k_{priv}) \stackrel{R}{=} G()$
  - k_{pub} = **verification key**
  - k_{priv} = **Signing key**
- S - Signing algoritm - *probabilistic* $\rightarrow$ **signature** $\sigma \stackrel{R}{=} S(k_{priv}, m)$
- V - Verificaition algoritm - *deterministic* - $y{=}V(k_{pub}, m, \sigma)$
  - $y = accept/reject$

Corectness property
$Pr[\ V(k_{pub}, m,\ S(k_{priv},\ m))) = accept] = 1$

Security

For (G, E, D)

- The challenger computes $(k_{pub}, k_{priv}) \stackrel{R}{=} G()$, and sends k_{pub} to the adversary.
- The adversaries queries the challenger with multiple message queries:
  - for $m_i \in \mathcal{M}$ the challenger computes $\sigma_i \stackrel{R}{=} S(k_{priv}, m_i)$
  - Sends back σ_i
- The adversary wins if he
  - Computes a pair (m, σ) with $m \notin \{m_1, m_2, ...\}$
  - $V(k_{pub}, m, \sigma) = accept$



> A signature scheme is secure if for all efficient adversaries their advantage is negligible

Note

- The definition does not cover the case where a message can have multiple signatures
    - Therefore an adversary can create a new valid pair (m, σ') (Remember this wasn't allowed in the security definition of a MAC)
    - We can strenghten the definition if we make the pair $(m, \sigma) \notin \{(m_1, \sigma_)), (m_2, \sigma_2), ...\}$
- The definition does not bind a signature to a person.
    - a message $m' \neq m$ might have the same valid signature σ

Duplicate Signature Key selection (DSKS)

> An attacker that sees a pair (m, σ) valid to some k_{pub} can generate a new pair (k'_{priv}, k'_{pub}) that can validate the pair (m, σ)

- https://www.agwa.name/blog/post/duplicate_signature_key_selection_attack_in_lets_encrypt
- It's easy to escape this unfortunate mistake, just attach the public to the message!

Digital signatures and collision resistant hashing

If we have acces to only a small message space (for example 256b) we can use a collision resistant function like a hash to map arbitrary length messages to our desired message space

Let H be a hash function. Then we have the **hash and sign** paradigm:

- $S'(k_{priv}, m) = S(k_{priv}, H(m))$
- $V'(k_{pub}, m, \sigma) = V'(k_{pub}, H(m), \sigma)$

Resources

- https://en.wikipedia.org/wiki/Non-repudiation
- https://www.youtube.com/watch?v=s22eJ1eVLTU
- https://www.youtube.com/watch?v=JR4_RBb8A9Q