Digital signatures

What is a digital signature

- A digital signature allows the holder of the secret key (the signing key) to sign a document
- Everyone who knows the verification key can verify that the signature is valid (correctness)
- No one can forge a signature even given the verification key even though he is given a signature

Structure of digital signature

- $Gen(1^n) \rightarrow (sk, vk)$
- $Sign_{sk}(m) \rightarrow sig$
- $Ver_{vk}(m, sig) \rightarrow \{0,1\}$

Structure of digital signature scheme (DSS)

- $Gen(1^n) \rightarrow (sk, vk)$
- $Sign_{sk}(m) \rightarrow sig$
- $Ver_{vk}(m, sig) \rightarrow \{0,1\}$

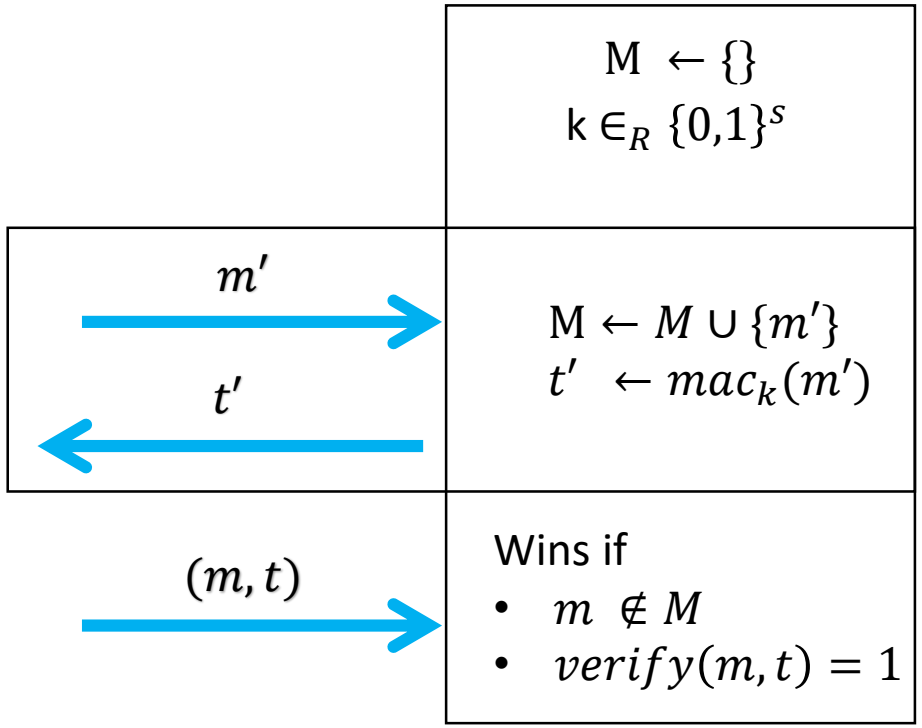
- Correctness
  - $Ver_{vk}(m, Sign_{sk}(m)) = 1$
- Unforgeability
  - To be continued

DSS VS MAC

- $Gen(1^n) \rightarrow (sk, vk)$
- $Sign_{sk}(m) \rightarrow sig$
- $Ver_{vk}(m, sig) \rightarrow \{0,1\}$

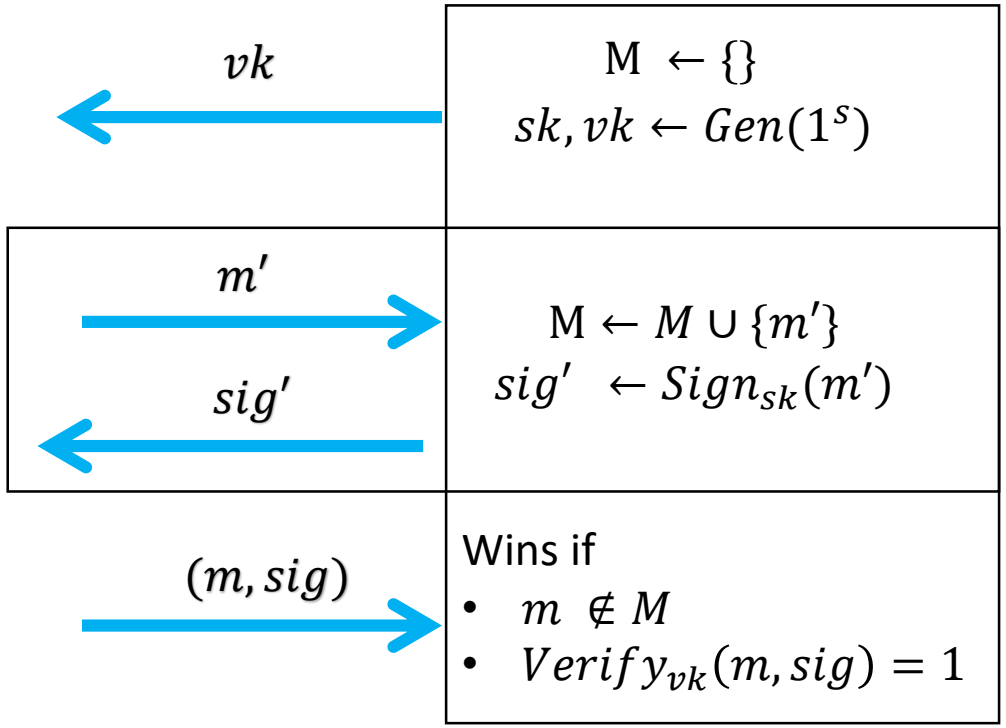
- $Gen(1^n) \rightarrow k$
- $mac_k(m) \rightarrow t$
- $\mathrm{v}er_k(m, t) \rightarrow \{0,1\}$

Mac forgery game



Repeat as many times
as the adversary wants

Signature forgery game



Repeat as many times as the adversary wants

Definition of signature scheme

- Correctness:
  - $\Pr\left[Ver_{vk}\left(m, Sign_{sk}(m)\right) = 1 \mid \ \ (sk, vk) \leftarrow Gen(1^s) \right] = 1$

- Unforgeability
  - For all PPT adversary A, there exists negligible function μ,
    - $\Pr[\ A\ \ wins\ the\ signature\ forgery\ game] \leq \mu(n)$

Relation between macs and signatures

- Every signature scheme is a message authentication code.

- A mac scheme is not necessarily a signature.
  - Without the key, it may be impossible to verify a mac.

Signatures are expensive

- They require public-key operations for each signature you wish to do.
- Hash functions are relatively cheap

Hash and sign

- Let $(Gen', Sign', Verify')$ be a signature scheme and let H be a collision resistant hash function, then the following

- $Gen(1^s) := Gen'(1^s)$
- $Sign_{sk}(m) := Sign'_{sk}(H(m))$
- $Verify_{vk}(m, sig) := Verify'_{vk}(H(m), sig) = 1$

Security of hash and sign

- Let $(Gen', Sign', Verify')$ be a signature scheme and let H be a collision resistant hash function, then the following

- $Gen(1^s) \coloneqq Gen'(1^s)$
- $Sign_{sk}(m) \coloneqq Sign'_{sk}(H(m))$
- $Verify_{sk}(m, sig) \coloneqq Verify'(H(m), sig) = 1$

- Essentially the same proof as hash and mac
  - Breaking security of this scheme means
    - Finding a collision
    - Finding a signature on an unsigned message

Interesting property of plaintext RSA

- $(sk, pk) \leftarrow KeyGen(1^s) \Rightarrow \ Enc_{pk}\big(Dec_{sk}(m)\big) = m$

- Due to the fact that $(m^e)^d = \left(m^d\right)^e = m^{ed}$

RSA signature scheme

- Let $(Keygen, Enc, Dec)$ denote the RSA encryption scheme
- $Gen(1^s) \coloneqq \{sk \leftarrow sk',\ vk \leftarrow pk \mid \ (sk', pk') \leftarrow Keygen(1^s)\}$
- $Sign_{sk}(m) \coloneqq Dec_{sk}(m)$
- $Verify_{vk}(m, sig) \coloneqq \ Enc_{vk}(sig) \ = m$

Insecure RSA signature scheme

- $Gen(1^s) := \{ vk \leftarrow pk,\ sk \leftarrow sk' \mid (sk', pk') \leftarrow Keygen(1^s)\}$
- $Sign_{sk}(m) := Dec_{sk}(m)$
- $Verify_{vk}\big(m, Sign_{sk}(m)\big) = Enc_{vk}\big(Dec_{sk}(m)\big)$
  - $Enc_{vk}\big(Dec_{sk}(m)\big) = \big(m^d\big)^e = m^{e \cdot d} = m$

Secure RSA signature scheme

- Assumptions
  - Random oracle H (Hash function modeled as a random oracle
  - $n = pq$ where p, q are prime

- $Gen(1^s) := \{ vk \leftarrow pk,\ sk \leftarrow sk' \mid (sk', pk') \leftarrow Keygen(1^s)\}$

- $Sign_{sk}(m) := Dec_{sk}(H(m))$

- $Verify_{vk}\big(m, Sign_{sk}(m)\big) := H(m) = Enc_{vk}\big(Dec_{sk}(H(m))\big)$

  - $Enc_{vk}\big(Dec_{sk}(H(m))\big) = \big((H(m))^d\big)^e \ (mod\ n)$

  - $\big((H(m))^d\big)^e \ (mod\ n) = H(m)^{e \cdot d \ mod\ \phi(n)} \ (mod\ n) = H(m)$

Schnorr signature scheme

- Based on
  - Group G
  - Generator g for G
  - Random oracle H
  - Discrete logarithm

Schnorr signature scheme

- Requirement: Group G, $|G| = q$, generator g, random oracle H

- $Gen(1^s)$
  - $sk \in_R G$
  - $vk \leftarrow g^{sk}$

- $Verify_{vk}(m, sig)$
  - $(a, s) \leftarrow sig$
  - u $\leftarrow g^s \cdot vk^{-a}$
  - Output $H(u, m) = a$

- $Sign_{sk}(m)$
  - $b \in_R Z_{|G|}$
  - $u \leftarrow g^b$
  - $a \leftarrow H(u, m)$
  - $s \leftarrow a \cdot sk + b \ (mod \ q)$
  - Output (a, s)