lecture 20

Digital Signature Schemes with Message Recovery

Def: A digital Sig schem with MR is a scheme for which a prior knowledge of the message in NOT required for the verification algorithm. ⟶ RSA, Rabin pk Enc schemes.

Alg. for key generation

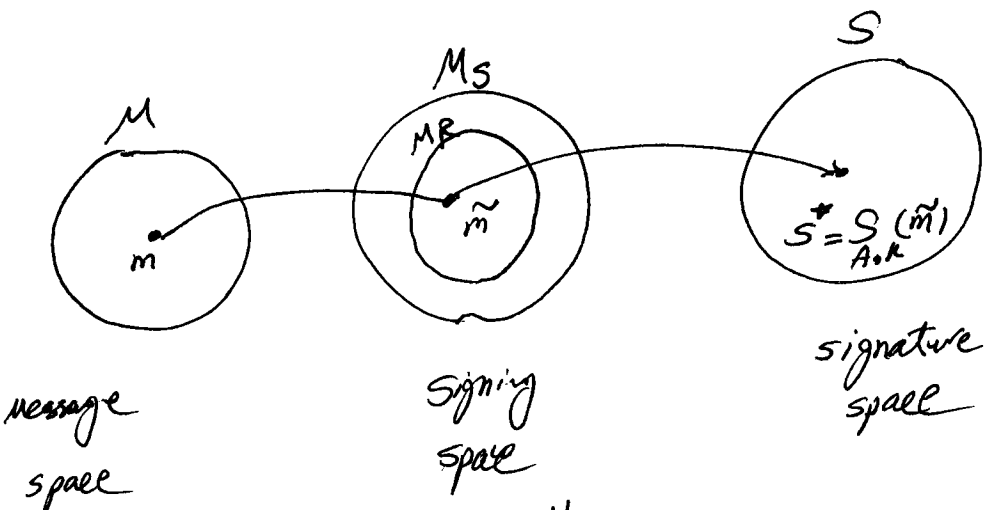
Summary: create private key to be used for signing & public key for verification.

(1.) "A" should select a set $SA = \{S_{A,K} : K \in \mathcal{K}\}$ of transformations. Each $S_{A,K}$ is a one-to-one mapping from $M_S \longrightarrow S$ (signing space ⟶ signature space)

M (message) ↑ M_S (signing space) ↑ S (signature)

(2.) S_A defines a corresponding mapping V_A with the property that $V_A \circ S_{A,K}$ is the identity map on M_S for all $K \in \mathcal{K}$. V_A: verification transformation.

(3.) public key V_A, private key S_A



Alg. signature process & verification process

summary: "A" produces a signature $s \in S$ for a message $m \in M$, "B" verifies the signature. recover "m" from "s"

(1.) signature generation: [A]

[1.1] select an elemat $k \in \mathcal{K}$ → (to select the transformation)

[1.2] Compute $\tilde{m} = R(m)$ → R is a redundancy function

$$s^* = S_{A,k}(\tilde{m})$$

[1.3] signature s^* is sent to "B" → verify & recover "m"

(2.) verification : [B]

[2.1] obtains A's authentic public key V_A

[2.2] Compute $\tilde{m} = V_A(s^*)$

[2.3] verify that $\tilde{m} \in M_R$ → if it's not true the signature will be rejected

[2.4] Recover m from $\tilde{m}$

by $R^{-1}(\tilde{m})$ → inverse of the redundancy function

$R: M \longrightarrow M_R \quad (M_R \subseteq M_S)$

$S_{A,k}: M_S \longrightarrow S$

$R^{-1}: M_R \longrightarrow M$

Req: ① For each $k \in \mathcal{K}$, $S_{A,k}$ should be efficient to compute

② V_A should be eff to compute

(efficiency)

③ It should be computationally infeasible for an entity other than "A" to find any $s^* \in S$ such that $V_A(s^*) \in M_R$ → generation a valid signature / forging a signature

(security)

RSA Singature Scheme

$\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ $\quad n = pq$ → large & almost the same size

DS scheme with message recovery → deterministic

signing space M_s & signature space S are $\mathbb{Z}_n$

$R: M \longrightarrow \mathbb{Z}_n$

Alg: key generation

1. Two large primes p & q are selected
2. $n = pq$ & $\phi = (p-1)(q-1)$
3. a random number e $1 < e < \phi$ such that $\gcd(e, \phi) = 1$ (relatively prime numbers)
4. use EEA to compute "d" $1 < d < \phi$ such that $ed \equiv 1 \pmod{\phi}$ (e & d are multiplicative inverse)
5. (n, e) are public, (d) is private

Alg.2 RSA signature generation & verification

1. signature generation

1.1 $\tilde{m} = R(m)$ an integer in range $[0, n-1]$

1.2 $s = \tilde{m}^{d} \pmod{n}$

1.3 signature for "m" is (s)

2. verfication ⟶ verify "s" is a valid signature & generat "m" from "s"

2.1 obtain Authentic public key (n, e)

2.2 Compute $\tilde{m} = s^{e} \pmod{n}$

2.3 verify $\tilde{m} \in \mu_R$: if not, reject the signature

2.4 Recover $m = R^{-1}(\tilde{m})$

Example: A RSA DS scheme with message recovery 5

$p = 7927 \quad , \quad q = 6997$

$n = pq = 55\,465219$

$\phi = (p-1)(q-1) = 7926 \times 6996 = 55450296$

select $e = 5 \longrightarrow 5d \equiv 1 \pmod{55450296}$

$d = 44360237$

$\mathcal{M} = \mathbb{Z}_n$

$R : \mathcal{M} \longrightarrow \mathbb{Z}_n$ is the identity map ($R(m) = m$) for all $m \in \mathcal{M}$

$m = 31229978 \longrightarrow \tilde{m} = 31229978$

signature $\rightarrow s = \tilde{m}^d \pmod n = 30729435$

verification $\rightarrow \tilde{m} = s^e \pmod n = 31229978 \in \mathcal{M}_R$ it's valid

$m = R^{-1}(\tilde{m}) = 31229978.$