Authentication and Signature

2021年4月14日 19:20

$\text{Sign}_k(m)$ $\qquad$ $\text{Ver}_{sk/pk}(\sigma_m, m)$

$\downarrow$

σ_m

Forger $\rightarrow$ σ' on m'

Message Authentication Code (MAC) ("private-key Signature")

(Gen, Sign, Verify)

$\text{Gen}(1^n) \rightarrow sk$ (secret key)

$\text{Sign}_{sk}(m) \rightarrow \sigma_m$

$\text{Verifier}_{sk}(\sigma_m, m) = 0/1.$

Adv. have access to Sign as an oracle.

$Q = \{(m_1, \sigma_1), \cdots, (m_t, \sigma_t)\}$

Adversary: Give a pair (m^*, σ^*), $m^* \notin L$ and (m^*, σ^*) accepted by verifier.

$$\Pr_{\substack{\text{Adv.} \\ \text{Gen}}}\left[\text{Adv} \xrightarrow{\text{Sign}_{sk}(\cdot)} m^*, \sigma^* \text{ s.t. } \text{Ver}(m^*, \sigma^*) = 1,\ m^* \notin Q\right] < \varepsilon(n).$$

A trivial MAC.

Given a PRF $\{0,1\}^* \rightarrow \{0,1\}^n$.

Gen $\rightarrow k$

$\text{Sign}_k(m) = F_k(m) = \sigma$

$\text{Ver}_k(m, \sigma)$: Run $F_k(m)$

Signature (Public-key)

- Hash and Sign Signature

Hash: $H(\cdot)$ model as a random oracle.

Trapdoor P_i, f_i, t_i

$\text{Sign}_{t_i}(m)$: $H(m) = r$. $f_i^{-1}(r) = \sigma$

$\text{Verify}_{(m, \sigma)}$: $H(m) = r$, $f_i(\sigma') == r$

$m_i, f_i^{-1}(H(m_i)) \approx m_i, f_i^{-1}(u) \approx m_i, u$