Lec 11

Signature

Lec 12

Zero-knowledge Proof

Lec 13

Multi-party Computation

Lec 14

Signature

(Gen, Sign, Verify)

$Gen(1^\lambda) \to (pk, sk)$

vk = verification key

sk = signing key

$Sign(sk, m) \to \sigma$

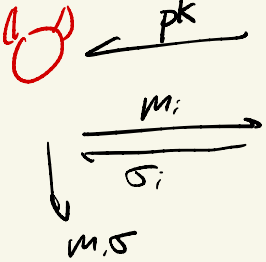
$Verify(pk, m, \sigma) \to 1/0$

Yes/No

Accept/Reject

Security

(existential unforgeable)



$\mathcal{A}$ wins iff $Verify(pk, m, \sigma) \to 1$

and $m \notin \{m_1 \cdots m_T\}$

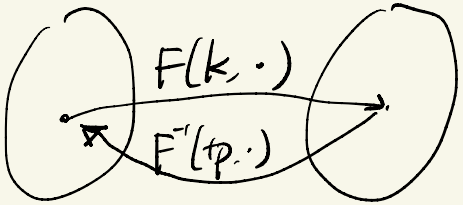
Strong Security

same

$(m, \sigma) \in \{(m, \sigma_1) \cdots (m_T, \sigma_T)\}$

Trapdoor permutation

Gen → k, tp



PKE: msg ⟶ ciphertext

Signature: signature ⟶ msg

msg $\xrightarrow{\text{Sign}}$ msg^d $\xrightarrow{\text{Verify}}$ $(msg^d)^e$

RSA-based signature

$Gen(1^\lambda)$ $pk = (N = pq, e, H)$ $sk = d$ s.t. $d \cdot e \equiv 1 \bmod \phi(N)$

$Sign(sk, m)$ $\sigma = H(m)^d$

$Verify(pk, m, \sigma)$ check if $\sigma^e = H(m)$

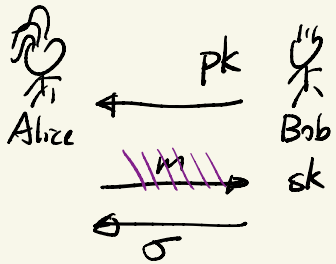
in the security proof

$H(m)$: compute $\sigma = F(m)$

output σ^e

Secure if H is modeled as a RO + RSA assumption

Blind Signature



RSA-based signature

$$H(m) \cdot r^e$$

$$(H(m) \cdot r^e)^d$$

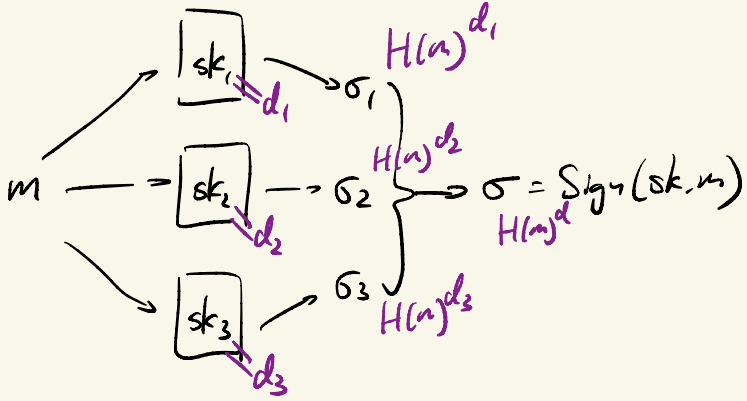
$$= (H(m))^d \cdot r$$

$$= Sign(sk, m) \cdot r$$

Threshold Signature

Gen $\rightarrow$ pk, sk

$sk \rightarrow sk_1 \quad sk_2 \quad sk_3$



RSA-based signature

$H(m)$

$d_1 + d_2 + d_3 = d \mod \phi(N)$

$\sigma = H(m)^d$

Pairing-based Signature

$q, g, G, G_T \qquad G \cong G_T \cong \mathbb{Z}_q$

$e: G \times G \to G_T$

$Gen(1^\lambda)$: $pk = g^a, H \qquad sk = a$

$Sign(sk, m) \quad \sigma = H(m)^a$

$Verify(pk, m, \sigma) \quad e(H(m), g^a) = e(\sigma, g)$

$= e(H(m), g)^a$

Breaking the scheme: $g \; g^a \; \underline{H(m)} \to H(m)^a$

$g^{t_m} \qquad g^{a \cdot t_m}$

which is CDH

only in the security proof

$H(m)$ sample random t_m

output g^{t_m}

$\sigma = H(m)^a = g^{t_m \cdot a} = (g^a)^{t_m}$

BDH assumption

$g \; g^a \; g^b \; g^c \xrightarrow{\text{hard}} e(g,g)^{abc}$

DBDH assumption $\Rightarrow$ CDH assumption

Pairing-based Signature

supports blind signature

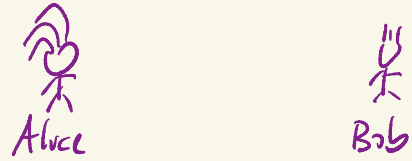
q, g, G, G_T $\quad G \cong G_T \cong \mathbb{Z}_q$

$e: G \times G \to G_T$

$Gen(1^\lambda)$: $pk = g^a, H$ $\quad sk = a$

$Sign(sk, m)$ $\quad \sigma = H(m)^a$

$Verify(pk, m, \sigma)$



Pairing-based Signature

supports threshold signature

$q, g, G, G_T \qquad G \cong G_T \cong \mathbb{Z}_q$

$e: G \times G \to G_T$

$Gen(1^\lambda)$: $pk = g^a, H \qquad sk = a$

$Share(a, n, t) \to a_1 \cdots a_n$

$Sign(sk, m) \quad \sigma = H(m)^a$

Correctness

$\forall S \subseteq \{1, \cdots, n\} \wedge |S| \geq t$

$Recover_S(Sign(a_i, m), i \in S) \to Sign(a, m)$

$Verify(pk, m, \sigma)$

$\exists (c_i, i \in S) \quad \sum c_i a_i = a$

$Recover_S(\cdots) = \prod_{i \in S} Sign(a_i, m)^{c_i} = Sign(a, m)$

sample random deg-(t-1) poly f, $f(0) = a$

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} \quad M \quad \end{bmatrix} \begin{bmatrix} a \\ r_1 \\ \vdots \\ r_{t-1} \end{bmatrix}$$

$a_i = f(i)$

Security $\forall S \subseteq \{1, \cdots, n\} \wedge |S| < t$

$\{a_i, i \in S\}$ reveals no info about a

Pairing-based Signature

supports signature aggregation

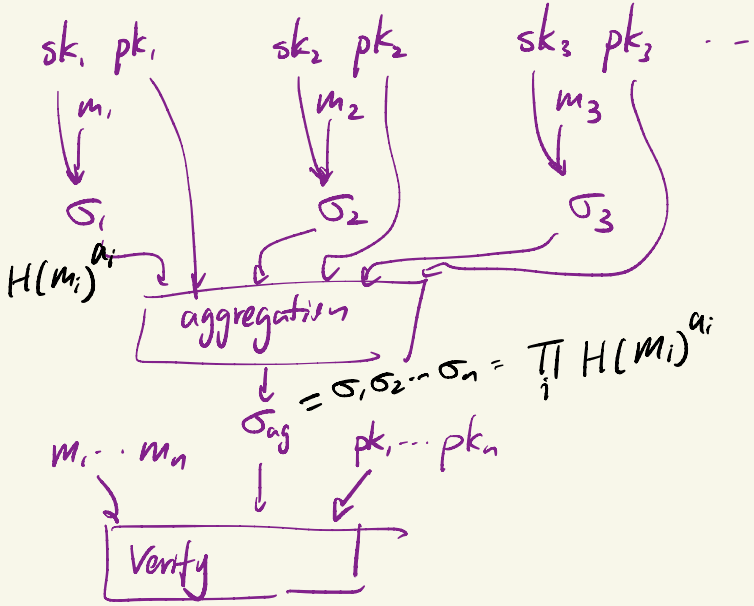
q, g, G, G_T

$e: G \times G \to G_T$

$Gen(1^\lambda)$: $pk = g^a, H$ $\quad sk = a$

$Sign(sk, m)$ $\quad \sigma = H(m)^a$

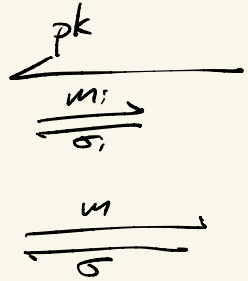
$Verify(pk, m, \sigma)$



Verify: $e(\sigma_{ag}, g) \stackrel{?}{=} \prod_i e(H(m_i), g^{a_i})$

$e(\prod_i H(m_i)^{a_i}, g) = \prod_i e(H(m_i), g)^{a_i}$

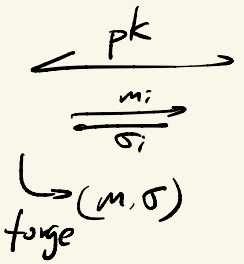
Duplicate Signature Key Selection



output (pk', sk')

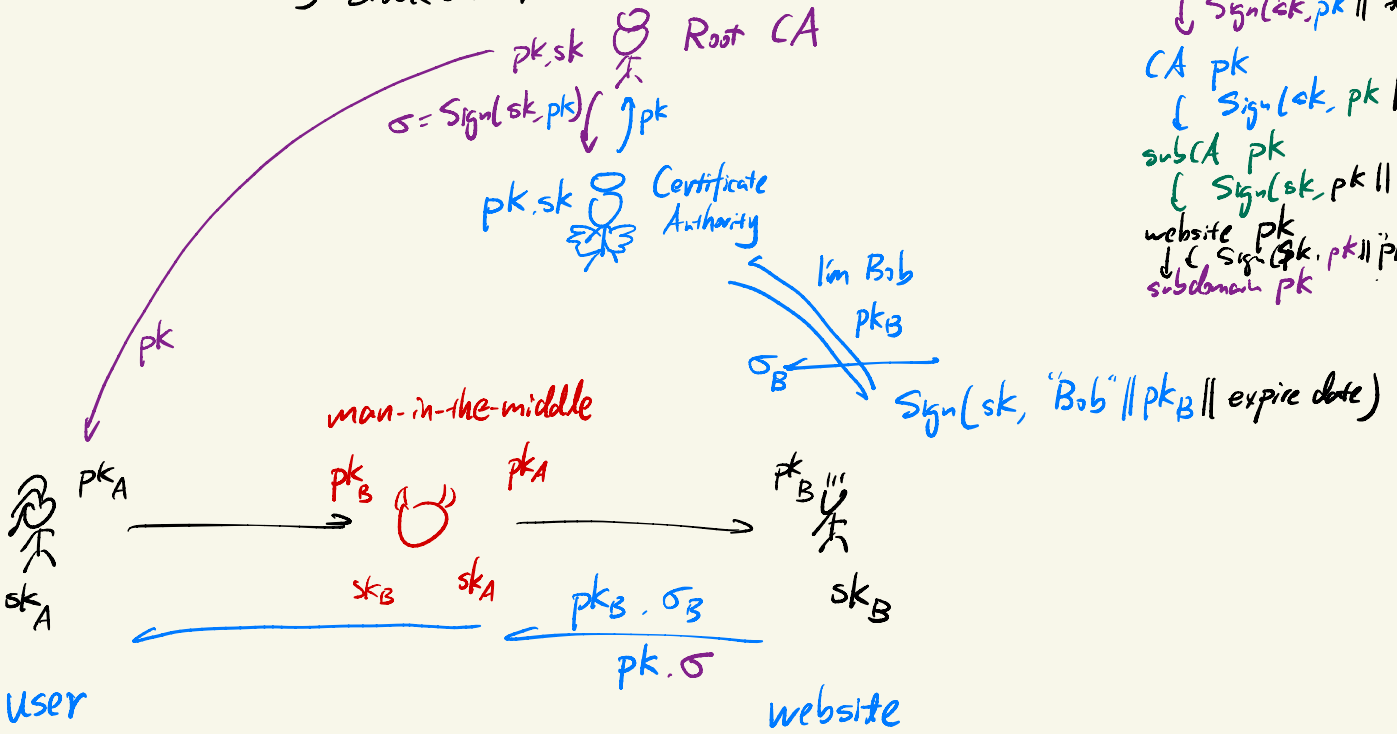
1) $\text{Verify}(pk', m, \sigma) = 1$
2) (pk', sk') is "valid"

"Standard" Security



Last Hour:

1) Public-Key Infrastructure (PKI)
2) Block chain



RootCA pk
↓ Sign(sk, pk || "*")
CA pk
↓ Sign(sk, pk || "*.com")
subCA pk
↓ Sign(sk, pk || "*.google.com")
website pk
↓ Sign(sk, pk || "play.google.com")
subdomain pk

$\xrightarrow{(c, \sigma)}$

$c = Enc(pk_B, m)$

$\sigma = Sign(sk_A, c)$

Block chain ≈ Bitcoin

SS

Public Log