provable security of used signature schemes

signature algorithm

keygen (1^k) (unary of length k, i.e. 1 raised to the power k) — generates sk, pk

sign (sk, M) — outputs signature σ

verify (pk, M, σ) — outputs 1 iff σ is a valid signature on M under pk

$$P_r\left[(pk,sk) \leftarrow keygen(1^k), \forall (M \in \mathcal{M}): Verify(pk, M, Sign(sk, M)) = 1\right] = 1$$

FB full break: A can compute secret key

UU universal forgery: A can forge a signature for any given message

SU selective forgery: A can forge a signature for one message of its choice

EU existential forgery: A can forge a signature for one, arbitrary message

KOA key only attack: A only gets public key

RMA random message attack: A gets (σ, M) for some random messages M + public key

CMA adaptive chosen message attack: A knows public key and can ask for σ on M of its choice

for us: EU-CMA

B-smooth: all prime factors smaller than B

random oracle model

standard model: assume building block property P. (e.g. collision resistance) Use property in reduction.

idealized model: assume a building block behaves perfectly (e.g. hash function behaves like truly random function) replace building block by an oracle in reduction

random oracle model: perfectly random function

↓

lazy sampling → new value: sample from uniform random, store, return result
old value: return stored result

for proofs, replace hash by random oracle (RO)

full domain hash signature scheme

one-way permutation

computing $\pi^{-1}(y)$ without knowledge of sk is computationally hard

sign (M)

$h = H(m)$ (from random oracle)

return table2 $[h]$

RO

M → (empty table if h was not seen before)

$w \leftarrow \mathbb{Z}_N^*$

$z = w^e \bmod N$

z ← (empty table) table2 $[h] = w$

if $m = m^*$ return y

success probability ϵ for q_H queries to oracle $\geq \frac{\epsilon}{q_H}$ probability of breaking RSA

RSA-PFDH: sign hash of message, expanded/padded with uniform random sample

RO

$R = [\leftarrow U_k, \ldots, \leftarrow U_k]$ (q_s)

H/M

if $r \in R$: $w \leftarrow \mathbb{Z}_N^*$, $z := w^e$, table2 $[x] = w$, return z

else: $w \leftarrow \mathbb{Z}_N^*$, $z := y \cdot w^e$, table2 $[x] = w$, return z

sign (m)

$r \leftarrow$ next value of R

$h = H(r \| m)$

return table2 $[h]$

M^*, $(y \cdot w^e)^d = y^d \cdot w$

$y^d = \frac{\sigma[i]}{w}$