

provable security of used signature schemes

signature algorithm

- keygen  $(1^k)$  bitstring of length  $k$ , i.e.  $1$  raised to the power  $k$   
generates  $s_k, p_k$
- sign  $(s_k, M)$  outputs signature  $\sigma$
- verify  $(p_k, M, \sigma)$  outputs 1 iff  $\sigma$  is a valid signature on  $M$  under  $p_k$

$$\Pr [ (p_k, s_k) \leftarrow \text{keygen}(1^k), \forall (M \in \mathcal{M}): \text{Verify}(p_k, M, \text{sign}(s_k, M)) = 1 ] = 1$$

- 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 some 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  $(\sigma, M)$  for some random messages  $M$  + pub key
- CMA adaptive chosen message attack: A learns pub key and can ask for  $\sigma$  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 has property  $P$ . e.g. collision resistance Use property in reduction
- idealised 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

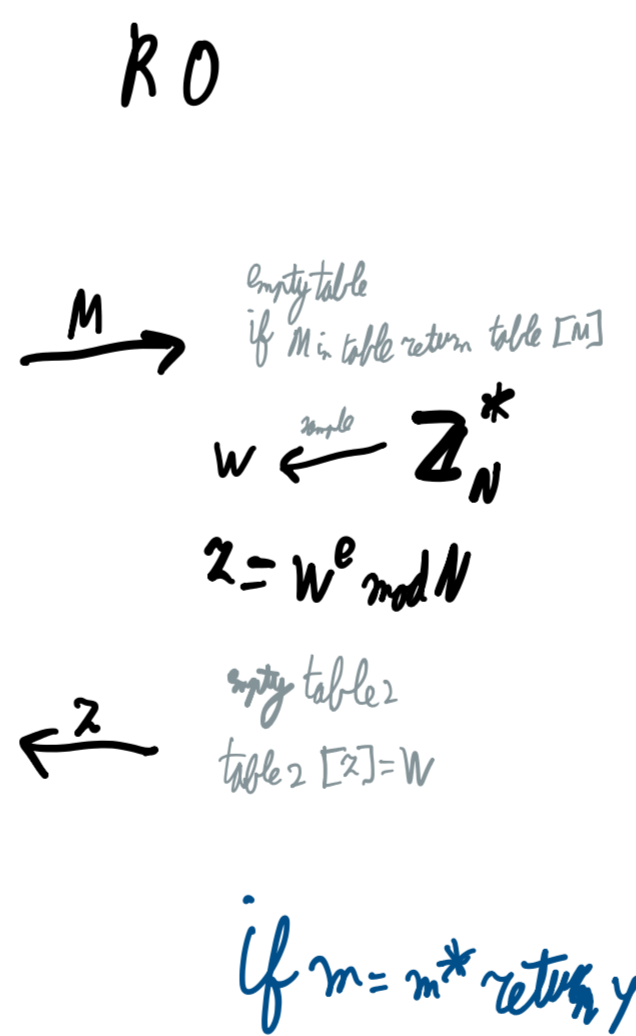
for proof, replace hash by random oracle (RO)

full domain hash signature scheme

one-way permutation

computing  $D^{-1}(y)$  without knowledge of  $s_k$  is computationally hard

sign  $(M)$   
 $r \leftarrow$  from random oracle  
 $h = H(r || M)$   
 return table  $z [r]$



Success probability  $\epsilon$  }  $\frac{\epsilon}{qr}$  probability of breaking RSA  
 or queries to oracle

RSA-PFDH: sign hash of message, prepended/added with uniform random sample

RO  
 $R = [ \leftarrow U_R, \dots, \leftarrow U_R ]$

r || M  
 if  $r \in R$  :  $w \leftarrow Z_N^*$ ,  $z := w^e$ , table  $z [r] = w$ , return  $z$   
 else:  $w \leftarrow Z_N^*$ ,  $z := y \cdot w^e$ , table  $z [r] = w$ , return  $z$

sign  $(m)$   
 $r \leftarrow$  next value of  $R$   $m^*, (y \cdot w^e)^d = y^d \cdot w$   
 $h = H(r || m)$   $y^d = \frac{\sigma [r]}{w}$   
 return table  $z [R]$