SCHNORR SIGNATURE

We have a $Str(1^\lambda)$ which produces a world. ~~We have~~ (λ: security parameters)

DLP: Schnorr runs as follows:

KeyGen (G)

$x \leftarrow_R \mathbb{Z}_q$

$X \leftarrow g^x$

ret (x, X)

Having keys generated, we can sign a message

Sign (m, x)

$a \leftarrow_R \mathbb{Z}_q$

$r \leftarrow g^a$

$h \leftarrow \mathcal{H}(m, r)$

$s \leftarrow a + xh$

ret $\sigma = (r, s)$

verify (m, σ, X)

$h = \mathcal{H}(m, r)$

$g^s = rX^h$

true

else false

The signature is correct if $Pr\left[G \leftarrow Str(1^\lambda), (x, X) \leftarrow KeyGen, m \in M, \sigma \leftarrow Sign(m, x) : Verify(\sigma, m, X) \rightarrow 1\right] = 1$

The signature is unforgeable if ~~$Pr[G \leftarrow Str(1^\lambda), (x,X) \leftarrow KeyGen, (m,\sigma) \leftarrow \mathcal{A}^{Sign}(X) : \mathcal{A} \text{ hasn't queried } Sign(m,G) \text{ and } Verify(\sigma, m, X) = 1] \leq$ negligible~~

In the given world after some number of queries to signing oracle and hash, adversary is able to create a signature of a new message

Proof of correctness:

$$L = g^s = g^{a+xh} = g^a g^{xh} = rX^h = \rho$$

Proof of unforgeability:

1° Simulation in ROM without knowing a secret key (2°)

$Sim(X, m)$

$s, h \leftarrow_R \mathbb{Z}_q$

$r \leftarrow \frac{g^s}{X^h}$

$h \rightarrow \mathcal{H}(m, r)$

O_{Sign}

$O_{\mathcal{H}}()$

m, r	h
m, r_1	h

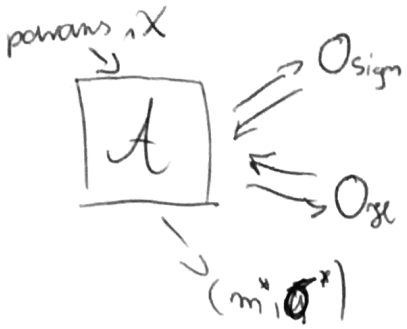
2° r, h, s $\quad s = a + xh$

r, h', s' $\quad s' = a + xh'$

$s - s' = x(h - h')$

$x = \frac{s - s'}{h - h'}$

with non-negligible probability the adv. will reuse the same ephemeral value a (rewinding lemma)



If those 2 requirements (sim, and (Rth, S)) are fulfilled then $\mathcal{A}$ will return two different signatures with the same source of randomness (we rewind to a, so it is the same)

(1) Signature is unforgeable if

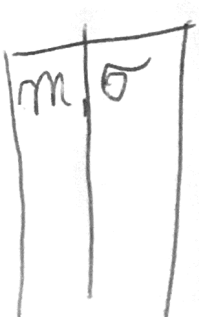
$$\forall_{\mathcal{A}} \; Pr\left[\begin{array}{l} g \leftarrow Str(\xi),\ (x, X) \leftarrow Keygen \\ \{(m_i, \sigma_i)\} \leftarrow \mathcal{A}^{O_{sign}(\cdot),\, O_H()}(X) \\ \hline \text{forgery step} \qquad \text{symulacja} \\ (m^*, \sigma^*) \leftarrow \mathcal{A}(pk, \{(m_i, \sigma_i)\} = V), \\ (m^*, \sigma^*) \notin V \ \wedge \\ Verify(m^*, \sigma^*, pk) \to 1 \end{array}\right] \leq$$

Probability that in world generated by Str having key generated by Keygen, adversary given having access

(2) Proof of unforgeability

We simulate 2 functionalities

$O_{sign}(m, X)$: $O_H(m)$



$h, s \xleftarrow{\$} \mathbb{Z}_q$

$g^s / X^h \Rightarrow r$

return (r, s)

m	r	h