Problem 3. «One-time signature keys»

The client uses one-time keys for ECDSA signing distinct messages in order to ensure their unlinkability. In order not to store many keys either on the client side or on the verifier side, the signing master key pair (sk, pk) is used, and each one-time key pair is produced from the master key using the identifier id.

For example, the following one-time keys will be generated

pk_{1976}:
(61169738454268678583460034936064297717270301135969262814478294443307068229252,
128111840706843653762271008760619955400322927882498031335433298309099094927 36),

pk_{2025}:
(24453843338537316254013968815895450156309709523339826431891869789646992767085,
25869566496341048395665983125532875931564283027116920587554169802031201907034)

for the master public key pk:
(10816614485495457876478125091777347557516186713906190912971613884173360259 5564,
21094420584895241134570605732830595252834312939967791385802578924623343135307)

and the NIST P-256 elliptic curve, the generator of the group is P:
(48439561293906451759052585252797914202762949526041747995844080717082404635286,
36134250956749795798585127919587881956611106672985015071877198253568414405109).

Let's give one message m and its signature (r, s), formed using a one-time key generated from some master key (not equal to the one given in the example above) using the identifier id. The problem is 1) to find the master public key from which the one-time signature generation key was obtained; 2) to forge signature for the message $m^* \neq m$ for some new identifier (to find valid id^* and (r^*, s^*)).

ECDSA. For convenience, we describe all signature schemes for the case of calculations in a prime order subgroup of an elliptic curve. Let P be the generator of the subgroup of prime order q. The elliptic curve is defined over a field $\mathbb{Z}_p$, where p is a prime. Let H be the hash function that maps binary strings to the elements in $\mathbb{Z}_q$.

Below the ECDSA signature scheme is given.

ECDSA.Gen( )

$d \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
$Q \leftarrow d \cdot P$
return (d, Q)

ECDSA.Sign(d, m)

$e \leftarrow \mathsf{H}(m) \bmod q$
$k \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
$R \leftarrow k \cdot P$
$r \leftarrow R.x \bmod q$
if $r = 0$: **return** $\perp$
$s \leftarrow k^{-1} \cdot (e + d \cdot r)$
if $s = 0$: **return** $\perp$
return (r, s)

ECDSA.Verify$(Q, (r, s), m)$

if $(r = 0 \vee s = 0)$: **return** 0
$e \leftarrow H(m)$
$R \leftarrow s^{-1} \cdot e \cdot P + s^{-1} \cdot r \cdot Q$
if $R.x \bmod q \neq r$: **return** 0
return 1