Cryptology Exercise Week 13

Zijun Yu 202203581

December 2023

Misuse of randomness in Schnorr signatures

Since the verifier can compute c himself and $c = \alpha^r$, the verifier can simply tell if r_1 and r_2 are the same by comparing c_1 and c_2. This follows from the fact that r_1 and r_2 are chosen in $\mathbb{Z}_q$ which is the order of α and thus $c_1 = c_2$ if and only if $r_1 = r_2$.

When the same r is used in two signatures, the verifier can compute $z_1 - z_2 = r + e_1 a - (r + e_2 a) = (e_1 - e_2)a \mod q$. The verifier can then simply compute the secret key a by $a = (z_1 - z_2)(e_1 - e_2)^{-1} \mod q$.

For the second senario, the verifier can still compute $z_1 - z_2 = r_1 + e_1 a - (r_2 + e_2 a) = (e_1 - e_2)a + (i - j)u \mod q$ and find the secret key by $a = (z_1 - z_2 - (i - j)u)(e_1 - e_2)^{-1} \mod q$.