Schnorrer signature CTF

Tuong Nguyen

September 2019

In this challenge, we have to create a valid signature for the message "fnord!" with elliptic curve signature scheme.

Let take a look on the scheme:

1. Key generation algorithm G:
   (a) (private key) $\alpha \xleftarrow{R} \mathbb{Z}_q$
   (b) (public key) $u \leftarrow g^{\alpha}$
2. Signature generation algorithm S:
   (a) (message space) $m \in \mathcal{M}$
   (b) (inputs) (α, m)
   (c) (nonce) $\alpha_n \xleftarrow{R} \mathbb{Z}_q$
   (d) (nonce commitment) $u_n \leftarrow g^{\alpha_n}$
   (e) (Fiat-Shamir heuristic challenge) $c \leftarrow H(m, u)$
   (f) (proof) $\alpha_z \leftarrow \alpha_n + \alpha c$
   (g) (output) $\sigma := (u_n, \alpha_z)$

As you can see, the challenge $c = H(m, u)$ is deterministic. That is a flaw! We can choose a arbitrary α_n, let take

$$\alpha_n = x - \alpha c$$

So that, we will have

$$\alpha_z = \alpha_n + \alpha c = x$$

And, we also have

$$u_n = g^{\alpha_n} = g^{x+\alpha c} = g^x (g^{\alpha})^{-c} = g^x u^{-c}$$

Now, we have a valid signature

$$\sigma = (u_n, \alpha_z) = (g^x u^{-c}, x)$$

Below is my sample code.