Scheme ECDSA

The standardized Elliptic Curve Digital Signature Algorithm [Por13], for an elliptic curve $\mathrm{E}(\mathbb{G}, q, G, I)$ with identity I. Following a prior KeyGen, the signer holds a private key $sk \equiv x \in \mathbb{Z}_q$ and a public key $pk \equiv Q = x \cdot G$

Inputs: m, the message to sign.

Sign$(x \in \mathbb{Z}_q,\ m) \dashrightarrow \sigma$

1: $d \leftarrow \mathsf{sha256}(m)$ and $m' \leftarrow (d \mod 2^{|q|})$, the $|q|$ leftmost bits of d
2: Sample $k \xleftarrow{\$} \mathbb{Z}_{q^*}$
3: $R \leftarrow k \cdot G$ and $r \leftarrow R_x \mod q$
4: Check $r \stackrel{?}{=} 0$; if so, go back to step 2
5: $s \leftarrow k^{-1}(m' + rx) \mod q$
6: $v \leftarrow (R_y \mod 2) + 2(R_x \stackrel{?}{\geq} q)$ as the recovery identifier $\in \mathbb{Z}_4$
7: **if** $(-s \mod q) \stackrel{?}{<} s$ **then** *(Normalize to "low s form")*
8: $\quad s \leftarrow (-s) \mod q$
9: $\quad v \leftarrow (v + 2) \mod 4$

return $\sigma = (r, s, v)$ as the signature

Verify$(Q \in \mathbb{G},\ m,\ \sigma = \{r \in \mathbb{Z}_{q^*}, s \in \mathbb{Z}_{q^*}, v \in \mathbb{Z}_4\}) \dashrightarrow valid$

10: $d \leftarrow \mathsf{sha256}(m)$ and $m' \leftarrow (d \mod 2^{|q|})$, the $|q|$ leftmost bits of d
11: $R \leftarrow (m's^{-1}) \cdot G + (rs^{-1}) \cdot Q$
12: Check if $(Q \stackrel{?}{=} I)$ or $(R \stackrel{?}{=} I)$ or $(r \stackrel{?}{=} R_x \mod q)$. If so, ABORT

return *valid*

References

[Por13] Thomas Pornin. Rfc 6979: Deterministic usage of the digital signature algorithm (dsa) and elliptic curve digital signature algorithm (ecdsa), 2013.