Scheme EdDSA

The EdDSA signature scheme [Sch91] for $ed25519(\mathbb{G}, q, G, I)$ and hash function H (often $\mathsf{Sha512}$). Signer run holds private key $x \in \mathbb{Z}_2^{|q|}$ and public key $Q \in \mathbb{G}$.

Inputs: m, a message to sign

KeyGen$()\dashrightarrow(x, Q)$

1: Sample $a \xleftarrow{\$} \{0,1\}^{2|q|}$
2: $Q \leftarrow a \cdot G$
3: $x \leftarrow \{a_{(i+|q|)}\}_{i \in [|q|]}$
return (x, Q) as the key pair

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

4: $k \leftarrow \mathsf{H}(x \,||\, m)$ *(Nonce generation)*
5: $R \leftarrow k \cdot G$ *(Commitment)*
6: $e \leftarrow \mathsf{H}(R \,||\, Q \,||\, \mathsf{H}(m))$ *(Challenge)*
7: $s \leftarrow (x \cdot e) + k$ *(Signature composition)*
return $\sigma = \{R, s\}$ as the signature

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

1: $e' \leftarrow \mathsf{H}(G \,||\, R \,||\, Q \,||\, \mathsf{H}(m))$
2: $R' \leftarrow s \cdot G + (-e) \cdot Q$
3: Check if $R' \stackrel{?}{=} R$, otherwise ABORT.
return *valid*

References

[Sch91] C. P. Schnorr. Efficient signature generation by smart cards. In *Journal of Cryptology*, 1991.