Scheme Schnorr

The Schnorr signature scheme [Sch91], parametrized by an elliptic curve $\mathrm{E}(\mathbb{G}, q, G, I)$ with identity I, and a hash function H. Following a prior KeyGen, the signer holds a private key $x \in \mathbb{Z}_q^\star$ and a public key $Q = x \cdot G$

Inputs: m, a message to sign

```
Sign($m,\ x \in \mathbb{Z}_q^\star,\ Q \in \mathbb{G}$) $\dashrightarrow \sigma$
    Sample $k \xleftarrow{\$} \mathbb{Z}_{q^*}$                    (Nonce generation)
    $R \leftarrow k \cdot G$                                (Commitment)
    $e \leftarrow \mathsf{H}(R \,||\, Q \,||\, m)$                       (Challenge)
    $s \leftarrow (x \cdot e) + k$                   (Signature composition)
    return $\sigma = \{e, s\}$ as the signature

Verify($m, Q \in \mathbb{G},\ \sigma = \{e \in \mathbb{Z}_{q^*}, s \in \mathbb{Z}_{q^*}\}$) $\dashrightarrow$ valid
    $R \leftarrow s \cdot G + (-e) \cdot Q$
    $e' \leftarrow \mathsf{H}(R \,||\, Q \,||\, m)$
    Check if $e' \overset{?}{=} e$, otherwise ABORT.
    return valid
```

References

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