Scheme BIP340

The BIP340 signature scheme [WNR18] for *secp256k1* $(\mathbb{G}, q, G, I)$ and hash function sha256 [Dan15]. Signer holds private key $x \in \mathbb{Z}_q$ and public key $Q = x \cdot G$

Inputs: m, a message to sign.

```
$\textsf{Sign}(m,\ x \in \mathbb{Z}_q,\ Q \in \mathbb{G}) \dashrightarrow \sigma$
    Sample $a \xleftarrow{\$} \{0,1\}^{256}$                                   (Nonce generation)
    $d \leftarrow -x$ if $(Q_y \mod 2 \neq 0)$ else $d \leftarrow x$
    $t \leftarrow d \oplus \textsf{Sha256}(\text{“}\texttt{BIP0340/aux}\text{”} \,||\, \text{“}\texttt{BIP0340/aux}\text{”} \,||\, a)$
    $k' \leftarrow \textsf{Sha256}(\text{“}\texttt{BIP0340/nonce}\text{”} \,||\, \text{“}\texttt{BIP0340/nonce}\text{”} \,||\, t \,||\, Q_x \,||\, m)$
    $R \leftarrow k' \cdot G$                                                  (Commitment)
    $e \leftarrow \textsf{Sha256}(\text{“}\texttt{BIP0340/challenge}\text{”} \,||\, \text{“}\texttt{BIP0340/challenge}\text{”} \,||\, R_x \,||\, Q_x \,||\, m)$   (Challenge)
    $k' \leftarrow -k'$ if $(Q_y \mod 2 \neq 0)$
    $s \leftarrow k' + e \cdot d$                                              (Signature composition)
    return $\sigma = (R, s)$ as the signature

$\textsf{Verify}(m,\ \sigma = (R \in \mathbb{G}, s \in \mathbb{Z}_{q^*},\ Q \in \mathbb{G})) \dashrightarrow valid$
    $Q' \leftarrow -Q$ if $(Q_{y_{(i)}} \mod 2 \neq 0)$, otherwise $Q' \leftarrow Q$
    $e \leftarrow \textsf{Sha256}(\text{“}\texttt{BIP0340/challenge}\text{”} \,||\, \text{“}\texttt{BIP0340/challenge}\text{”} \,||\, R_x \,||\, Q_x \,||\, m)$
    $R' \leftarrow s \cdot G - e \cdot Q'$
    Check if $R_x \overset{?}{=} R'_x$. Otherwise ABORT
    return $valid$

$\textsf{VerifyBatch}_{\forall \boldsymbol{i} \in [\boldsymbol{n}]}(\boldsymbol{m} = \{m_{(i)}\}, \boldsymbol{Q} = \{Q_{(i)} \in \mathbb{G}\}, \boldsymbol{\sigma} = \{R_{(i)} \in \mathbb{G}, s_{(i)} \in \mathbb{Z}^n_{q^*}\}) \dashrightarrow valid$
    Set $a_{(1)} \leftarrow 1$ and $C \leftarrow I$
    Sample $\{a_{(2)}, ..., a_{(n)}\} \xleftarrow{\$} \mathbb{Z}^{n-1}_{q^*}$ and compute $l \leftarrow \sum_{i=1}^{n} a_{(i)} \cdot s_{(i)}$
    for $i \in [n]$ do
        $Q' \leftarrow -Q_{(i)}$ if $(Q_{y_{(i)}} \mod 2 \neq 0)$, otherwise $Q' \leftarrow Q_{(i)}$
        $e \leftarrow \textsf{Sha256}(\text{“}\texttt{BIP0340/challenge}\text{”} \,||\, \text{“}\texttt{BIP0340/challenge}\text{”} \,||\, R_{x_{(i)}} \,||\, Q_{x_{(i)}} \,||\, m_{(i)})$
        $C \leftarrow C + a_i \cdot (R_i + e) \cdot Q'$
    Check if $C \overset{?}{=} l \cdot G$. Otherwise ABORT.
    return $valid$
```

References

[Dan15] Quynh Dang. Secure hash standard, 2015-08-04 2015.

[WNR18] Pieter Wuille, Jonas Nick, and Tim Ruffing. Schnorr signatures for secp256k1, 2018.