Verifikation einer ECDSA-Signatur

signierte Nachricht (m, r, s)

öff. Schlüssel des Unterzeichners

E, G, p, n, Q / $m = 18522$

↑ !E!

$p = 27583$

$n = 27427$

$r = 23611$

$s = 15017$

$Q = (23577, 11783)$

$G = (1, 13017)$

Schritte 1–4:

$r, s \in [1, n-1]$

$1 \leq 23611 \leq 27426$

$1 \leq 15017 \leq 27426$ (✓)

$w \equiv \frac{1}{s} \bmod n$

$\equiv \frac{1}{15017} \bmod 27427 \equiv 11278 \bmod n$

$u_1 \equiv m \cdot w \equiv 18522 \cdot 11278 \equiv 7084 \bmod n$

↑ eigentlich SHA(m)

$u_2 \equiv r \cdot w \equiv 23611 \cdot 11278 \equiv 23542 \bmod n$

Schritt 5:

$X = u_1 \cdot G + u_2 \cdot Q = 7084 \cdot G + 23542 \cdot Q$

$(20041, 25368) + (17345, 25135)$

$X = (23611, 14327) \neq \mathcal{O}$

↳ $x_1 \rightarrow x_1 \bmod n$

$23611 \bmod 27427 = v \overset{?}{=} r$

$23611 \overset{!}{=} 23611$ ✓