ECDSA

elliptic curve digital signature algorithm

Dokument:
ECDSA von Johnson / Menezes / Vanstone

Beispiel:

$p = 54037$

$E: y^2 \equiv x^3 - 32 \bmod p$ (bzw. $x^3 + 54005$)

$|E| = 53623$ → siehe CM

$G = (1, 42442)$ zufälliger Punkt

$d = 2606$ geheimer Schlüssel

$Q = d \cdot G = (10267, 9156)$

Signaturerzeugung (kap. 7 des Dok.)

$e = 43210$ Hashwert der zu signierenden Nachricht

1. $k = 2019$ Zufallswert $2 \leq k \leq |E| - 1$

2. $k \cdot G = (32724, 3370)$ → 3. r

4. $\frac{1}{k} \bmod |E|$

$\frac{1}{2019} \equiv 23558 \bmod 53623$

(5. $e = SHA(m)$)

6. $s \equiv \frac{1}{k}(e + d \cdot r) \equiv 23558 \cdot (43210 + 2606 \cdot 32724)$

$\equiv 32831 \bmod 53623$

7. Signierte Nachricht

$(e, r, s) = (43210, 32724, 32831)$

Signaturverifikation (Kap. 7)

1. $1 \leq r < |E|, \quad 1 \leq s < |E|$ ✓

2. $e = SHA(m)$

   $e = 43210$

3. $w = \frac{1}{s} \bmod |E|$

   $w \equiv \frac{1}{32831} \equiv 35134 \bmod 53623$

4. $u_1 \equiv e \cdot w \equiv 43210 \cdot 35134 \equiv 19387 \bmod |E|$

   $u_2 \equiv r \cdot w \equiv 32724 \cdot 35134 \equiv 47896 \bmod |E|$

5. $X = \underbrace{u_1 \cdot G} + \underbrace{u_2 \cdot Q}$

   $(21096,47879) + (19731,2243)$

   $= (32724,3370)$

   r = r → Signatur ok

$G = (1,42442)$

$Q = (10267,9156)$