ECDSA - Signaturen

ElGamal → DSA → ECDSA

g, y, p	E, G, Q, p
a geheim	d geheim
$g^a \equiv y \bmod p$	$Q = d \cdot G$
$(\mathbb{Z}_{/p\mathbb{Z}}/\{0\}, \cdot)$	$(E, +)$
benutzt $g^{p-1} \equiv 1 \bmod p$	$\lvert E \rvert \cdot G = \mathcal{O}$
Signieren	
$r \equiv g^k \bmod p$	$R = kG \rightarrow r = R_x$
$s \equiv \frac{1}{k} \cdot (m^{\circledast} - a \cdot r) \bmod p-1$	$\frac{1}{k} (m^{\circledast} + d \cdot r) \bmod \lvert E \rvert$
Sig ist (r, s)	

$\circledast$ bzw $h(m)$
für Hashfunktion $h()$
z. B. SHA-256, SHA-3

Beispiel für ECDSA

benutze CM-Implementierung für eine Kurve E mit $|E| \approx 2^{16}$

$\Rightarrow$ brauche Primzahl $p \approx 2^{16}$ Satz von Hasse

$p = 27583$ Parametererzeugung

$E: \; y^2 \equiv x^3 + 27502 \bmod p$ mit $|E| = n = 27427$

Punkt G finden: $x = 0, 1, 2, \ldots$ bis rechte Seite ein $\square$

$x = 0$: $y^2 \equiv 27502 \bmod p$

lösbar, wenn $27502^{\frac{p-1}{2}} \equiv 1 \bmod p$

$x = 1$: $y^2 \equiv 1^3 + 27502 \equiv 27503 \bmod p$ ist $\square$

Quadratwurzel berechnen

hängt ab von $p \bmod 8$, hier ist $p \equiv 7 \bmod 8$

also $p \equiv 3 \bmod 4 \rightarrow$ Formel $z^{\frac{p+1}{4}}$ funktioniert

$$y \equiv 27503^{\frac{p+1}{4}} \equiv 13017 \bmod p$$

$\Rightarrow \; G = (1, 13017)$

$d = 18704 \Rightarrow Q = d \cdot G = (23577, 11283)$

Signatur für eine Nachricht m erzeugen

$m = 18522$ Message

$k = 23594$ Zufallszahl

$k \cdot G = (\underbrace{23611}_{r}, 14327)$

$s \equiv \frac{1}{k} \cdot (m + d \cdot r) \bmod |E|$

$\equiv 15017$

$\Rightarrow$ Signatur für $m = 18522$ ist

$(23611, 15017)$