Eigenes „Gesamtbild" CRYPTO1 – Ell. Kurven (II) (EC) (VL vom 25.5.) 26./31.5.22

↳ Signieren, and. Darstellungen, Sicherheit

Schnorr-Signatur(verfahren):

wg. SPH (ohnehin)

Sei E EC über Körper $\mathbb{F}_p$ (p prim), $G \in E$, $ord(G)=n$ prim; öffentlich.

Alice: Privater Schlüssel: $d_A \in \mathbb{N}$
Öffentlicher Schlüssel: $P_A = d_A \cdot G \in E$
Nachricht: $m \in [1, n-1]$
Signatur berechnen:
[1] Wähle zufällig $k \in_R [1, n-1]$
$Q = k \cdot G = (x_Q, y_Q)$ temporärer/Ephemeral-Schlüssel
[2] $r = Hash(m \,||\, x_Q) \mod n$
[3] $s = k - r \cdot d_A \mod n$

Signatur: (r, s) ist Alice' Signatur von m.

Bob: Signatur prüfen: $(x_Q', y_Q') = s \cdot G + r \cdot P_A = (s + r \cdot d_A) \cdot G = k \cdot G$ (*)
Prüfe, ob $r = Hash(m \,||\, x_Q')$.

⇒ Kein Invertieren nötig (gut für Chipkarten z.B.), dafür Hashfunktion.

Idee: (*) rechne $k \cdot G$ aus, ohne k zu kennen! ⇒ k muss auch geheim bleiben, damit d_A geheim bleibt!

Verschiedene Darstellungen von EC:

(any EC can be written in Weierstrass form)

- **Weierstraß-Darstellung (bisher):** $E_{a,b} = \{(x,y) \in F^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$
- **Projektive Weierstrass-Koordinaten:** $E_{a,b} = \{(X,Y,Z) \in F^3 \mid (\frac{Y}{Z})^2 = (\frac{X}{Z})^3 + a(\frac{X}{Z}) + b\} = \{(X,Y,Z) \in F^3 \mid ZY^2 = X^3 + aXZ^2 + bZ^3\} \cup \{(0,0,0)\}$
  ↳ wobei $(k \cdot X, k \cdot Y, k \cdot Z) \triangleq (X, Y, Z)$ ∇
  ↳ in Sage bis auf $\mathcal{O} = (0,1,0)$ auf $Z=1$ normiert
  mit $\mathcal{O} := (0, 1, 0)$; ansonsten normiere $Z = 1$ (Sage) (siehe links)
- **Montgomery-Darstellung/-Form-Kurve:** $E_{a,b} = \{(x,y) \in F^2 \mid y^2 = (x+\alpha)^3 + a(x+\alpha) + b\} \cup \{\mathcal{O}\}$
  $= \{(x,y) \in F^2 \mid y^2 = x^3 + 3\alpha x^2 + 3\alpha^2 x + ax + \alpha a + b\}$
  $= \{(x,y) \in F^2 \mid y^2 = x^3 + 3\alpha x^2 + 3\alpha^2 x + ax\} \cup \{\mathcal{O}\}$
  $= \{(x,y) \in F^2 \mid \beta^3 y^2 = (\beta x)^3 + 3\alpha\beta(\beta x)^2 + \beta^3(3\alpha^2 + a)x\}$
  $= \{(x,y) \in F^2 \mid \beta(\beta y)^2 = (\beta x)^3 + 3\alpha\beta(\beta x)^2 + \beta^2(3\alpha^2 + a)(\beta x)\}$
  $E_{M,A,B} = \{(u,v) \in F^2 \mid Bv^2 = u^3 + Au^2 + u\} \cup \{\mathcal{O}\}$
  mit $\beta^2 = (3\alpha^2 + a)^{-1} \neq 0$; $A = 3\alpha B \notin \{2, -2\}$; $(x,y) \mapsto (u = \beta(x - \alpha), v = \beta y)$
  (αϵF ist eine Nullstelle von $x^3 + ax + b$)
  ↳ (geht nur für jede EC in Weierstraß-Form!)
  ↳ ($\exists x: x^2 = 3\alpha^2 + a$, d.h. ist quadrat. Rest)

en.wiki/Montgomery_curve

Wichtiger ist aber die ...:

- **Edwards-Darstellung/-Kurve:** $E_{a,d} = \{(x,y) \in F^2 \mid ax^2 + y^2 = 1 + dx^2y^2\}$
  mit • $a = \frac{A+2}{B}$; $d = \frac{A-2}{B}$ bzw. $A = \frac{2(a+d)}{a-d}$; $B = \frac{4}{a-d}$
  en.wiki: • $x = \frac{u}{v}$; $y = \frac{u-1}{u+1}$ bzw. $u = \frac{1+y}{1-y}$; $v = \frac{1+y}{(1-y)x}$
  und $(x_1,y_1) + (x_2,y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)$
  mit $\mathcal{O} := (0,1)$ neutr. El. & $-(x_1,y_1) = (-x_1, y_1)$

(Twisted) esp. when $a \neq 1$ (Bernstein ∇ et al. 2008) ○

Sicherheit von EC/DLP:

→ Weierstraß-Param. b fehlt in Formeln!

- SPH, Pollard-ρ, BSGS gibt es ohnehin (generisch); Indexkalkül dagegen n. für EC
  ↳ (spezielle Kurven meiden)
- **Invalid Curve Attack:** (Biehl et al. 2000) (Jager et al.) Annahmen: – EC für Public Key Crypto eingesetzt, priv. Key = const.
  – kann $k \cdot P$ für bel. P berechnen → Server using Static ECDH
  ↳ TLS-ECDH: – Das Opfer (Server/Smartcard) überprüft nicht, ob $P \in E_{a,b}$.

en.wiki/ECDH: (TLS-)ECDH: Alice: $(d_A, Q_A = d_A \cdot G$ ephemeral); Bob: $(d_B, Q_B = d_B \cdot G$ static/trusted)
Shared Secret: $d_A \cdot Q_B = d_B \cdot Q_A = (x_K, y_K)$ (private, public; G = agreed upon)

Regulär Szenario:
Alice → $Q_A = d_A \cdot G$ → Server
Alice ← $Q_B = d_B \cdot G$ ← Server
Alice → Client Finished → Server
Alice ← Server Finished ← Server
(mit $d_A \cdot Q_B = d_B \cdot Q_A$ als Schlüssel)

Angriffs-Szenario: (Jager et al.)
Eve → $P_i \notin E_{a,b}$ → Server
Eve ← $Q_B = d_B \cdot G$ ← Server
Eve → Client Finished → Server
(mit $d_B \cdot P_i$ als Schlüssel, geraten!)
Falls Eve ← Server Finished ← Server
dann kenne $d_B \bmod ord(\langle P_i \rangle)$!
⇒ wiederhole & finde iwann d_B mit CRT
(P_i = Generator einer kl. Untergruppe v. Pr.ordnung p_i)

(Menezes, Okamoto, Vanstone)

crypto.stackex

- **MOV-Angriff:** Sei Abb. $w: E_{a,b}(\mathbb{F}_p) \times E_{a,b}(\mathbb{F}_p) \to \mathbb{F}_{p^k}$ bilinear, k Einbettungsgrad.
  Gegeben: $x \cdot P$; Gesucht: x Verschiebe nun das DLP-Problem nach $\mathbb{F}_{p^k}$:
  Es gilt: $w(x \cdot P, Q) = w(P, Q)^x \Rightarrow x = dLog_{w(P,Q)}(w(x \cdot P, Q))$ (w heißt „Weil-Paarung")
  ⇒ Lehre: verwende nur Kurven mit hohem Einbettungsgrad, am besten standardisierte EC