

Übungen zur Vorlesung Kryptographie

Blatt 9

Aufgabe 33: (Aufwärmübung zu elliptischen Kurven)

Lösen Sie diese Aufgabe nur per Hand, also ohne jede Computerhilfe.

- (a) Zeigen Sie, dass die Gleichung $y^2 = x^3 + 3x + 2$ eine elliptische Kurve E über $\mathbb{F}_{13}$ definiert.
- (b) Welche der Punkte $p = (4, 2)$, $q = (3, 5)$ und $r = (2, -5)$ liegen auf E ?
- (c) Was sind jeweils die inversen Elemente von $p = (5, 5)$, $q = (2, 4)$ und $r = (4, 0)$ in E ?
- (d) Berechnen Sie $(2, 4) \odot (5, 5)$ und $(3, 5) \odot (5, 8)$ in E .
(*Graphisch oder mit Formel, aber beschreiben Sie, wie Sie vorgehen.*)
- (e) Berechnen Sie p^2 für $p = (5, 5)$.

Aufgabe 34: (Diffie-Hellman auf elliptischen Kurven)

Hier führen Sie den Diffie-Hellman-Schlüsseltausch auf einer konkreten (unrealistisch kleinen) elliptischen Kurve durch. Es sei E die elliptische Kurve, die durch $y^2 = x^3 + x$ über $\mathbb{F}_{11}$ gegeben ist. (*Es ist hilfreich, den Cayleygraphen der Gruppe E zu nutzen: damit kann praktisch alles hier ohne Formeln berechnet werden.*)

- (a) Ein Erzeuger von E ist $g = (7, 3)$. Die öffentliche Information ist (E, g) . Alices geheimer Schlüssel ist $a = 5$, Bobs geheimer Schlüssel ist $b = 3$. Was schickt Alice an Bob? Was schickt Bob an Alice? Was ist ihr gemeinsamer Schlüssel k ?
- (b) Ein anderer Erzeuger von E ist $g' = g^7 = (8, 6)$. Die öffentliche Information ist jetzt (E, g') . Alices geheimer Schlüssel ist wieder $a = 5$, Bobs geheimer Schlüssel ist wieder $b = 3$. Was schickt Alice diesmal an Bob? Was schickt Bob diesmal an Alice? Was ist nun ihr gemeinsamer Schlüssel k ?

Aufgabe 35: (ElGamal auf elliptischen Kurven)

Hier führen Sie die ElGamal-Verschlüsselung auf einer konkreten elliptischen Kurve durch. Angenommen, Bob möchte eine Nachricht an Alice schicken und dabei ElGamal über der elliptischen Kurve E^* mit der Gleichung $y^2 = x^3 + x$ über $\mathbb{F}_7$ nutzen. Der öffentliche Erzeuger von E^* sei $g = (3, 3)$. Alices geheimer Schlüssel ist $a = 3$.

- (a) Was ist das g^a in Alice' öffentlichem Schlüssel (E^*, g, g^a) ?
- (b) Bob wählt zufällig $r = 4$. Was ist der Einmalschlüssel $k = (g^a)^r$ für diese Verschlüsselung?
- (c) Bob verschlüsselt die Nachricht $m = 5$. Dazu wählt er das Element $(5, 2) \in E^*$ und verschlüsselt es als $c = m \odot k$. Was ist c ? Was genau schickt Bob an Alice?
- (d) Was berechnet Alice alles, um die Nachricht zu entschlüsseln?

(*Es ist auch hier hilfreich, den Cayleygraphen der Gruppe E^* zu nutzen, siehe Bsp. 6.2 im Skript.*)

Weiter auf Seite 2.

Aufgabe 36: (Gruppenstruktur)

Eine elliptische Kurve hat — als abstrakte Gruppe — immer die Struktur einer zyklischen Gruppe Z_n , oder des direkten Produkts $Z_k \times Z_\ell$ zweier zyklischer Gruppen Z_k und Z_ℓ .

Bestimmen Sie die Struktur der elliptischen Kurven (als Gruppen), die durch die Gleichungen $y^2 = x^3 + ax$ für $a = 1, 2, 3$ über $\mathbb{F}_{17}$ gegeben sind (*dazu ist die Software von meiner Webseite sehr hilfreich!*) und zeichnen Sie jeweils ihren Cayleygraphen.

Abgabe bis Mittwoch 16.6.2021 bis 14 Uhr per Email an den Tutor.

Jan	Jan-Philipp	Brünger	jbruenger@techfak.de
Leonard	Simon	Ellinghaus	lellinghaus+krypto@techfak.de
Kallias	Stoupas		kstoupas+krypto@techfak.de