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 $y^2 = x^3 + 3x + 1$ eine elliptische Kurve E über $\mathbb{F}_{11}$ definiert.
(b) Welche der Punkte $p = (2, 3)$, $q = (3, -2)$ und $r = (4, 0)$ sind Elemente von E?
(c) Was sind jeweils die inversen Elemente von $p = (5, 3)$, $q = (2, 9)$ und $r = (4, 0)$ in E?
(d) Berechnen Sie $(4, 0) \odot (1, 4)$, $(5, 3) \odot (0, 1)$ und $(0, 1) \odot (5, 3)$ in E.
(e) Berechnen Sie p^2 für $p = (1, 4)$.

Aufgabe 34: (Wann ist's keine Gruppe?)
(a) Es wäre nahliegend, die Gruppenoperation auf einer elliptischen Kurve E über $\mathbb{R}$ einfach zu definieren als $p \odot q = r$, wobei r der dritte Schnittpunkt der Gerade durch p und q mit E ist (bzw der zweite Schnittpunkt von E mit der Tangente in p an E, falls $p = q$). Erklären Sie, warum das im Allgemeinen keine Gruppe liefert. Welche Gruppenaxiome werden verletzt? Gerne kann Ihre Lösung durch ein aussagekräftiges Bild illustriert werden.

(b) Für welche Werte von b liefert $y^2 = x^3 - x + b$ keine elliptische Kurve über $\mathbb{R}$? Für welche Werte von b liefert $y^2 = x^3 + b$ keine elliptische Kurve über $\mathbb{R}$? Zeichnen Sie all diese Kurven (gerne mit einer geeigneten Software). Erläutern Sie, warum die jeweils keine Gruppe liefern.

Aufgabe 35: (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 $\mathbb{F}_7$ gegeben ist.
(Es ist hilfreich, den Cayleygraphen die Gruppe E^* aus Bsp. 6.2 des Skripts zu nutzen: damit kann praktisch alles hier ohne Formeln berechnet werden.)

(a) Ein Erzeuger von E^* ist $g = (3, 3)$. Die öffentliche Information ist (E^*, g). Alice 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 $g' = g^3 = (5, 5)$. Die öffentliche Information ist jetzt (E^*, g'). Alice 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 ihr gemeinsamer Schlüssel k?

Aufgabe 36: (Three-Pass-Protokoll auf elliptischen Kurven)
Bob möchte die Nachricht 6 an Alice schicken und dabei Shamirs Three-Pass-Protokoll über der elliptischen Kurve E mit der Gleichung $y^2 = x^3 + 3x + 2$ über $\mathbb{F}_{11}$ nutzen. Der öffentliche Erzeuger von E sei $g = (3, 7)$. Alice' geheimer Schlüssel ist $a = 3$, Bobs geheimer Schlüssel ist $b = 4$. Bob kodiert die 6 als $m = (6, 7)$ in E.

Was sind die Werte von a' und b'? Und was genau schicken Bob und Alice sich gegenseitig?
(Es ist sicher auch hier gewinnbringend, den Cayleygraphen von E zu erstellen und zu nutzen.)

Abgabe bis Montag 20.6.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen: *techfakaccount*-bl$n$.pdf, also z.B. `dfrettloeh-bl9.pdf`, oder `dfrettloeh+mnebel-bl9.pdf`.

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de