Übungen zur Vorlesung Kryptographie

Blatt 10

Aufgabe 37: (Elliptische Kurven mit Primzahlordnung)
Es ist sehr praktisch, wenn die Ordnung einer elliptischen Kurve eine Primzahl p ist (warum nochmal?). Für große p ist es aber nicht einfach, so eine zu finden. Diese Aufgabe soll das ein wenig illustrieren.

(a) Finden Sie alle a und b, so dass die Anzahl der Elemente der elliptischen Kurve über $\mathbb{F}_{19}$ mit der Gleichung $y^2 = x^3+ax+b$ eine Primzahl ist. Berechnen Sie den Anteil dieser an allen Möglichkeiten, die a, b zu wählen. Berechnen Sie auch den Anteil der a, b, die keine Gruppe liefern. *(Als Abgabe reichen die Anteile, als Prozentzahl, oder als* $0 < x < 1$*.)*
(b) Machen Sie dasselbe für $\mathbb{F}_{641}$.

Aufgabe 38: (ElGamal auf elliptischen Kurven)
Bob möchte eine Nachricht an Alice schicken und dabei ElGamal-Verschlüsselung 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 $a = 3$.

(a) Was ist das g^a in Alice öffentlichem Schlüssel (E, g, g^a)?
(b) Bob wählt zufällig $r = 6$. Was ist der Einmalschlüssel $k = (g^a)^r$ für diese Verschlüsselung?
(c) Bob verschlüsselt die Nachricht $m = 10$. Dazu wählt er das Element $(10, 3) \in E$ 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 vermutlich auch hier hilfreich, den Cayleygraphen zu haben und zu nutzen. Dazu und für andere Aufgaben auf diesem Blatt ist die Software von meiner Webseite sicher wieder hilfreich.)

Aufgabe 39: (Gruppenstruktur)
Bestimmen Sie — im Sinne von Satz 6.1 — die Struktur der elliptischen Kurven, die durch die Gleichungen $y^2 = x^3 + ax$ für $a = 1, 2, 3$ über $\mathbb{F}_{17}$ gegeben sind und zeichnen Sie jeweils ihren Cayleygraphen.

(Als Lösung reicht der Graph mit Knoten und Kanten, die Knoten brauchen nicht beschriftet zu werden.)

Aufgabe 40: (Ordnung von E ist ungefähr p)
Sei E eine elliptische Kurve über $\mathbb{F}_p$ (wie in Def. 6.1).

(a) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der x-Achse ist. (Also: ist $(x, y) \in E$, dann auch $(x, -y) \in E$. Das $\mathcal{O}$ kann hier ignoriert werden.)

(b) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der Achse $\{(x, \frac{p}{2}) \mid x \in \mathbb{R}\}$ ist.
(Zwar ist $\frac{p}{2}$ *nicht in* E *oder* $\mathbb{F}_p$*, aber das Spiegeln haut dennoch hin.)*

(c) Zeigen Sie: für die Ordnung $|E|$ von E gilt: $|E| \leq 2p + 1$.

Abgabe bis Montag 27.6.2022 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-bl10.pdf`, oder `dfrettloeh+mnebel-bl10.pdf`.

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