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 a und b, so dass die Anzahl der Elemente der elliptischen Kurve über $\mathbb{F}_{17}$ mit der Gleichung $y^2 = x^3 + ax + b$ eine Primzahl ist.
(b) Finden Sie a und b, so dass die Anzahl der Elemente der elliptischen Kurve über $\mathbb{F}_{641}$ mit der Gleichung $y^2 = x^3 + ax + b$ eine Primzahl ist.

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: (Buchstaben zu Punkten zu Buchstaben)
Wir benutzen die Koblitz-Kodierung aus der Vorlesung für die elliptische Kurve E mit der Gleichung $y^2 = x^3 + 5x + 3$ über $\mathbb{F}_{17}$. Dabei ist wie üblich a=0, b=1, ... z=25. Also können wir jeden Buchstaben mit 6 Bit darstellen. Wir wählen hier also $d = 4$ und zerschneiden eine zu verschlüsselnde Botschaft (in Binärcodierung) in 2-Bit-Worte.

(a) Was ist die Koblitz-Kodierung des Buchstaben "y"?
(b) Welches Wort ergibt das Ent-Kodieren der nach obigem Schema Koblitz-kodierten Nachricht

$$(1, 3), (13, 2), (4, 6),\ (1, 3), (10, 13), (1, 14),\ (5, 0), (2, 2), (10, 13),\ (4, -6), (2, -2), (15, -6)?$$

(c) Finden Sie ein b, so dass die Koblitz-Kodierung mit $d = 4$ für die elliptische Kurve E mit der Gleichung $y^2 = x^3+5x+b$ über $\mathbb{F}_{17}$ versagt. (D.h., es gibt ein $m \in \{0, 1, 2, 3\}$, so dass für kein $x = dm+j$ ($j \in \{0, 1, 2, 3\}$) ein y existiert mit $(x, y) \in E$.)

Abgabe bis Mittwoch 17.6.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de