Dr. Dirk Frettlöh 12.6.2019

Übungen zur Vorlesung Kryptographie

Blatt 10

Aufgabe 37: (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.
(e) Berechnen Sie p^2 für $p = (5, 5)$.

Aufgabe 38: (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 $g = (3, 3)$. Alice' geheimer Schlüssel ist $a = 3$.

(a) Was ist das g^a in Alice' öffentlichem Schlüssel (E^*, g, g^a)?

(b) Bob wählt zufällig $r = 4$. 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 hilfreich, die Informationen über die Gruppe E^* aus Bsp. 5.5 des Skripts zu nutzen: damit kann praktisch alles hier ohne Formeln berechnet werden.)

Aufgabe 39: (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.

(a) 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.

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

Abgabe: Mittwoch 19.6.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de