PD Dr. Martin Kreuzer
Fakultät für Mathematik
Universität Regensburg

Regensburg, den 3.7.2000

Übungen zur Vorlesung "Kryptographie"

Blatt 6

(Abgabetermin: 13.7.2000)

Aufgabe 26. Gegeben sei ein Körper K und eine kubische Kurve über K mit der Gleichung $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Zeigen Sie, daß diese Gleichung durch eine lineare Koordinatentransformation auf die folgende Gestalt gebracht werden kann:

a) $y^2 = x^3 + ax + b$ (mit $a, b \in K$), falls $\mathrm{char}(K) \notin \{2, 3\}$ gilt,

b) $y^2 = x^3 + ax^2 + bx + c$ (mit $a, b, c \in K$ und $ab = 0$), falls $\mathrm{char}(K) = 3$ gilt, und

c) $y^2 + ay = x^3 + bx + c$ oder $y^2 + xy = x^3 + dx^2 + e$ (mit $a, b, c, d, e \in K$), falls $\mathrm{char}(K) = 2$ gilt.

Aufgabe 27. Gegeben sei der folgende Satz:

Drei Geraden G_1, G_2, G_3 mögen eine kubische Kurve C in neun Punkten $P_1, \ldots, P_9$ schneiden. Schneiden drei weitere Geraden H_1, H_2, H_3 die Kurve C dann ebenfalls in neun Punkten $Q_1, \ldots, Q_9$ und gilt $P_i = Q_i$ für $i = 1, \ldots, 8$, so folgt $P_9 = Q_9$.

Verwenden Sie diesen Satz, um das Assoziativgesetz für die Addition von Punkten auf einer elliptische Kurve zu beweisen.
(*Hinweis:* Behandeln Sie zuerst den Fall, daß einer der drei Punkte der unendlich ferne Punkt ist.)

Aufgabe 28. Sei $K = \mathbb{Q}$ oder $K = \mathbb{Z}/p\mathbb{Z}$ mit $p \notin \{2, 3\}$.

a) Schreiben Sie eine *CoCoA* Funktion `EllipticPoint(...)`, die ausgehend von den Parametern $a, b \in K$ einer elliptischen Kurve $E(K)$ über K einen Punkt $(x, y) \in E(K)$ berechnet.

b) Entwerfen Sie einen Zero-Knowledge Beweis, bei dem Sie mit Hilfe des Feige-Fiat-Shamir Protokolls dem Übungsleiter beweisen können, daß Sie Teilaufgabe a) richtig gelöst haben, ohne daß Sie ihm das Programm verraten. Implementieren Sie die notwendigen *CoCoA* Funktionen für die Schlüsselerzeugung und die Anwendungsphase aus Ihrer Sicht und der des Übungsleiters.

Aufgabe 29. Gegeben sei eine Zahl $e > 0$ und der Körper $K = \mathbb{F}_q$ mit $q = 2^e$.

a) Zeigen Sie, daß die Abbildung $\mathrm{Tr} : \mathbb{F}_q \longrightarrow \mathbb{F}_2$ die gegeben ist durch $\mathrm{Tr}(x) = \sum_{i=0}^{e-1} x^{2^i}$ surjektiv und $\mathbb{F}_2$-linear ist.

b) Beweisen Sie, daß die Gleichung $y^2 + y = x$ für ein gegebenes $x \in \mathbb{F}_q$ genau dann in $\mathbb{F}_q$ lösbar ist, wenn $\mathrm{Tr}(x) = 0$ gilt.
Tip: Genau die Hälfte der Elemente $x \in \mathbb{F}_q$ erfüllt $\mathrm{Tr}(x) = 0$.

c) Finden Sie einen Algorithmus, wie man für $x \in \mathbb{F}_q$ mit $\mathrm{Tr}(x) = 0$ ein $y \in \mathbb{F}_q$ mit $y^2 + y = x$ finden kann.
Tip: Wählen Sie eine $\mathbb{F}_2$-Basis von $\mathbb{F}_q$ und identifizieren Sie die Elemente x, y mit ihren Koordinatenvektoren.

d) Sei $E(K)$ eine elliptische Kurve über K. Finden Sie einen probabilistischen Algorithmus, wie man einen Punkt von $E(K)$ berechnen kann.
Tip: Unterscheiden Sie die beiden Fälle von Aufgabe 26.c.

Aufgabe 30. Gegeben seien der Körper $K = \mathbb{Q}$ oder $K = \mathbb{Z}/p\mathbb{Z}$ mit $p \notin \{2, 3\}$ sowie eine elliptische Kurve $E(K)$ über K mit Gleichung $y^2 = x^3 + ax + b$.

a) Schreiben Sie eine *CoCoA* Funktion `EllipticAdd`(...), die die Summe zweier Punkte von $\overline{E}(K)$ berechnet. Der unendlich ferne Punkt $\mathcal{O}$ werde dabei durch den String `"InfPoint"` repräsentiert.

b) Verwenden Sie die Funktion aus a), um eine *CoCoA* Funktion `EllipticMult`(...) zu schreiben, die zu gegebenen $n \in \mathbb{Z}$ und $P \in \overline{E}(K)$ den Punkt $nP \in \overline{E}(K)$ berechnet.
Tip: Berechnen Sie die Punkte $2^i P$ und gehen Sie wie bei "square-and-multiply" vor.

c) Implementieren Sie die verschiedenen Teile des ECDSA Signaturverfahrens. Arbeiten Sie dabei nur über einem Körper $K = \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl p. Schreiben Sie dazu *CoCoA* Funktionen `ECKeyGen`(...), `ECSign`(...) und `ECVerifiy`(...).