Kryptologie 2 Sommersemester 2010
Johannes Köbler, Sebastian Kuhnert 9. Juni 2010

Übungsblatt 8

Aufgabe 59 ***mündlich***

Eine elliptische Kurve E über $\mathbb{F}_q$ $(q = 2^n)$ enthält neben dem Punkt $\mathcal{O}$ alle Lösungen $(x, y) \in \mathbb{F}_{2^n}$ einer Gleichung der Form

$$y^2 + cy = x^3 + ax + b \text{ oder } y^2 + xy = x^3 + ax^2 + b \ .$$

Leiten Sie für beide Gleichungen Formeln für die Koordinaten von $-P$ und $P + Q$ in Abhängigkeit der Koordinaten von $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ her.

Hinweis: Bestimmen Sie hierzu wie in der Vorlesung die Koordinaten des Schnittpunktes der durch P und $\mathcal{O}$ (bzw. durch P und Q) definierten Geraden mit der Kurve über $\mathbb{R}$ und beachten Sie die Besonderheiten der Arithmetik in $\mathbb{F}_{2^n}$.

Aufgabe 60 ***mündlich***

Sei E_q die durch $y^2 + y = x^3$ über $\mathbb{F}_q$ $(q = 2^n)$ definierte elliptische Kurve.

(a) Sei $P = (x, y) \in E_q$. Bestimmen Sie die Koordinaten von $-P$ und von $2P$.

(b) Bestimmen Sie die Ordnung aller Punkte P von E_{16}.

Hinweis: Berechnen Sie die Koordinaten von $4P$.

(c) Bestimmen Sie die Anzahl der Punkte von E_4 und von E_{16}.

Hinweis: Zeigen Sie $\#E_{16} = \#E_4$ und benutzen Sie den Satz von Hasse.

Aufgabe 61 ***mündlich***

Bestimmen Sie die Anzahl der Punkte der durch $y^2 + y = x^3$ definierten elliptischen Kurve E_q über $\mathbb{F}_q$, falls $q \equiv_3 2$ ist.

Aufgabe 62 ***mündlich***

Was wären die Folgen, wenn man beim ECDSA-Signaturverfahren $y = 0$ oder $z = 0$ zulassen würde?

Aufgabe 63 ***mündlich***

(a) Bestimmen Sie die NAF-Darstellung der Zahl 87.

(b) Bestimmen Sie mit Hilfe des Algorithmus DoubleAddSub das Vielfache $87P$ des Punktes $P = (2, 6)$ auf der elliptischen Kurve E, die über $\mathbb{Z}_{127}$ durch $y^2 = x^3 + x + 26$ definiert ist.

Aufgabe 64 ***mündlich***

Bestimmen Sie die Anzahl l_i aller natürlichen Zahlen, die eine NAF-Darstellung der Form $(c_{i-1}, \ldots, c_0)$ mit $c_{i-1} = 1$ haben. Zeigen Sie hierzu folgende Rekursion und finden Sie eine explizite Formel für l_i.

$$l_i = \begin{cases} 1, & i \leq 2, \\ 2(l_1 + \cdots + l_{i-2}) + 1, & i \geq 3. \end{cases}$$

Aufgabe 65 ***mündlich***

Angenommen, Alice signiert mit der Lamport-Signatur zwei Dokumente x und x', die an l Bitpositionen differieren. Für wie viele verschiedene neue Nachrichten kann der Gegner dann eine gültige Signatur berechnen?

Aufgabe 66 ***10 Punkte***

Zur Erinnerung: Bei der Lamport-Signatur wird ein Dokument $x = x_1 \cdots x_n \in \{0,1\}^n$ durch die Folge $u_{(i,x_i)}$ $(i = 1, \ldots, n)$ signiert, d. h. durch x wird die Indexmenge $A_x = \{(i, x_i) \mid i = 1, \ldots, n\}$ aus der Grundmenge $A = \{1, \ldots, n\} \times \{0, 1\}$ ausgewählt. Ein Mengensystem $\{A_x \subseteq A \mid i \in I\}$ heißt *Spernersystem* über A, falls für alle $x, x' \in I$ gilt:

$$x \neq x' \Rightarrow A_x \not\subseteq A_{x'}$$

(a) Zeigen Sie, dass die Spernereigenschaft notwendig für die Sicherheit der Lamport-Signatur ist.

(b) Bestimmen Sie für $B = \{1, \ldots, 2m\}$ ein Spernersystem der Größe $\|I\| = \binom{2m}{m}$.

(c) Benutzen Sie das Spernersystem aus Teilaufgabe (b) für die Konstruktion einer Signatur, deren Signaturlänge gegenüber der Lamport-Signatur um ca. 50% verkürzt ist. Beschreiben Sie hierzu den Signieralgorithmus und die Verifikationsbedingung.

Hinweis: Verwenden Sie $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$, um eine injektive Funktion $f\colon \{0,1\}^n \to I$ anzugeben.

(d) Zeigen Sie, dass kein Spernersystem der Größe $\|I\| > \binom{2m}{m}$ über der Grundmenge $B = \{1, \ldots, 2m\}$ existiert.