Übungsblatt 4

Aufgabe 26 ***mündlich***

Sei H eine 2-universale (n, m, l)-Hashfamilie und sei $\lambda = l/m^2$.

(a) Wieviele Text-Hashwert-Paare $(x_i, h_k(x_i))$ $(i = 1, \ldots, j)$ benötigt der Gegner im Fall $\lambda = 1$, um mit Erfolgswahrscheinlichkeit 1 ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, \ldots, x_j\}$ generieren zu können?

(b) Schätzen Sie die Erfolgswahrscheinlichkeit nach unten und nach oben ab, mit der ein Gegner bei Kenntnis von 2 Text-Hashwert-Paaren $(x_i, h_k(x_i))$ ein gültiges Paar $(x, h_k(x))$ mit $x \notin \{x_1, x_2\}$ für den unbekannten Schlüssel k generieren kann?

Aufgabe 27 ***mündlich***

Sei H eine (n, m, l)-Hashfamilie mit $\alpha, \beta \leq j^{-1}$. Wie groß muss dann der Schlüsselraum K von H mindestens sein, wenn der Schlüssel unter Gleichverteilung gewählt wird?

Aufgabe 28 ***mündlich***

Für eine Primzahl $p > 2$ und ein Paar $(a, b) \in K = \mathbb{Z}_p \times \mathbb{Z}_p$ sei die Funktion $h_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ definiert durch $h_{(a,b)}(x) = (x + a)^2 + b \bmod p$. Zeigen Sie, dass (X, Y, K, H) mit $X = Y = \mathbb{Z}_p$ und $H = \{h_k \mid k \in K\}$ eine 2-universale Hashfamilie ist.

Aufgabe 29 ***mündlich***

Überlegen Sie, wie der mittels einer Verschlüsselungsfunktion E_k konstruierte CBC-MAC auch durch eine einfache Modifikation einer CFB-Verschlüsselung unter E_k berechnet werden kann.

Aufgabe 30 ***mündlich***

Welche Angriffe sind möglich, wenn ein Schlüssel k sowohl für eine CBC-Verschlüsselung als auch für einen CBC-MAC einer Nachricht x verwendet wird?

Aufgabe 31 ***mündlich***

Sei $E_k \colon \{0,1\}^l \to \{0,1\}^l$, $k \in K$, eine Familie von Verschlüsselungsfunktionen. Betrachten Sie für eine Konstante $d \geq 2$ die Hashfamilie (X, Y, K, H) mit $X = \{0,1\}^{dl}$, $Y = \{0,1\}^l$ und $H = \{h_k \mid k \in K\}$, wobei $h_k \colon X \to Y$ durch

$$h_k(x_1 \cdots x_d) = E_k(x_1) \oplus \cdots \oplus E_k(x_d), |x_1| = \cdots = |x_d| = l$$

definiert ist.

(a) Geben Sie im Fall d gerade einen existentiellen $(1, 0)$-Fälscher für diese Hashfamilie an.

(b) Geben Sie einen selektiven $(1, 1)$-Fälscher für diese Hashfamilie an.

Aufgabe 32 Sei E die elliptische Kurve $y^2 = x^3 - 3x - 2$ über $\mathbb{R}$. ***mündlich***

(a) Skizieren Sie zeichnerisch den Verlauf von E.

(b) Berechnen Sie die Summe $P + Q$ für $P = (3, 4)$ und $Q = (2, 0)$.

(c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.

Aufgabe 33 ***mündlich***

Sei E eine durch die Gleichung $F(x, y) = 0$ im $\mathbb{R}^2$ definierte Kurve, wobei F die Form $F(x, y) = y^2 - x^3 - ax - b$ hat. Zeigen Sie, dass folgende Bedingungen äquivalent sind.

(a) Das Polynom $p(x) = x^3 + ax + b$ hat eine mehrfache Nullstelle.

(b) Es gilt $4a^3 = -27b^2$.

(c) Es ex. ein Punkt $(x_0, y_0) \in E$, für den die partiellen Ableitungen $\frac{\delta F}{\delta x}(x_0, y_0)$ und $\frac{\delta F}{\delta y}(x_0, y_0)$ beide 0 sind. (Ein solcher Punkt heißt *singulär*.)

Aufgabe 34 ***10 Punkte***

Sei $E_k \colon \{0,1\}^l \to \{0,1\}^l$, $k \in K$, eine Familie von Verschlüsselungsfunktionen. Betrachten Sie für eine Konstante $d \geq 2$ die Hashfamilie (X, Y, K, H) mit $X = \{0,1\}^{dl}$, $Y = \{0,1\}^l$ und $H = \{h_k \mid k \in K\}$, wobei $h_k \colon X \to Y$ durch

$$h_k(x_1 \cdots x_d) = E_k(x_1) + 3E_k(x_2) + \cdots + (2d-1)E_k(x_d) \bmod 2^l, |x_1| = \cdots = |x_d| = l$$

definiert ist.

(a) Geben Sie einen existentiellen $(1, 2)$-Fälscher für diese Hashfamilie an.

(b) Geben Sie einen selektiven $(1, 3)$-Fälscher für diese Hashfamilie an.