Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 4

Aufgabe 26 ***mündlich***

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

Aufgabe 27 ***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 $H = \{h_k \mid k \in K\}$ ein $(p, p, p^2, 1)$-MAC ist.

Aufgabe 28 ***mündlich***

Sei (X, Y, K, H) ein (n, m, l, λ)-MAC.

(a) Für wieviele Texte $x_1, \ldots, x_j$ muss der Gegner im Fall $\lambda = 1$ die zugehörigen MAC-Werte $h_k(x_1), \ldots, h_k(x_j)$ kennen, um mit Erfolgswahrscheinlichkeit 1 den MAC-Wert $h_k(x)$ für einen Text $x \notin \{x_1, \ldots, x_j\}$ bestimmen zu können?

(b) Schätzen Sie die Erfolgswahrscheinlichkeit nach unten und nach oben ab, mit der ein Gegner bei Kenntnis der MAC-Werte $h_k(x_1), h_k(x_2)$ von 2 Texten x_1, x_2 den MAC-Wert $h_k(x)$ für einen weiteren Text $x \notin \{x_1, x_2\}$ bestimmen kann.

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 $d \geq 2$ den MAC (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 diesen MAC an.

(b) Geben Sie einen selektiven $(1, 1)$-Fälscher für diesen MAC an.

Aufgabe 32 ***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 $d \geq 2$ den MAC (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 diesen MAC an.

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