Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 5

Besprechung der mündlichen Aufgaben am 24. 11. 2022
Abgabe der schriftlichen Lösungen bis 29. 11. 2022, 23:59 Uhr

Aufgabe 26 ***mündlich***

(a) Konstruieren Sie für jede Primzahl p und jede natürliche Zahl $d \geq 2$ einen 2-universalen (n, m, l)-MAC mit $n = (p^d - 1)/(p - 1)$, $m = p$ und $l = p^d$.

(b) Sei H ein 2-universaler (n, m, l)-MAC. Konstruieren Sie auf der Basis von H einen 2-universalen (n, m^d, l^d)-MAC H'.

Aufgabe 27 ***mündlich***

Ein (n, m, l)-MAC heißt **(stark) j-universal**, falls für alle $x_1, \ldots, x_j \in X$ mit $x_i \neq x_{i'}$ für $i \neq i'$ und alle $y_1, \ldots, y_j \in Y$ gilt:

$$\big\|\{k \in K \mid h_k(x_i) = y_i \text{ für } i = 1, \ldots, j\}\big\| = \frac{\|K\|}{m^j} \ .$$

(a) Zeigen Sie, dass jeder j-universale MAC auch j'-universal ist, falls $1 \leq j' \leq j$ gilt.

(b) Konstruieren Sie für jede Primzahl p und jedes $j \geq 1$ einen j-universalen (p, p, p^j)-MAC.

Hinweis: Betrachten Sie die Menge aller Polynome vom Grad höchstens $j - 1$ über dem Körper $\mathbb{F}_p$.

Aufgabe 28 ***mündlich***

Konstruieren Sie einen 2-universalen $(6, 5, l)$-MAC und einen 2-universalen $(13, 3, l')$-MAC für geeignete l, l'.

Aufgabe 29 ***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 30 ***mündlich***

Betrachten Sie den Substitutionsangriff aus Aufgabe 19 auf einen MAC der durch eine kollisionsresistente Kompressionsfunktion definiert ist. Für eine sponge-konforme Paddingfunktion y und eine Permutation $f\colon \{0,1\}^b \to \{0,1\}^b$ betrachten wir nun die Funktion $h(k,x) = \textsc{Sponge}_{f,y,r}(l, kx\textsc{renc}(l))$ (vereinfachte Form des KECCAK Message Authentication Code - KMAC). Dabei ist $\textsc{renc}\colon \mathbb{N} \to \{0,1\}^*$ eine suffixfreie Funktion.

(a) Lässt sich der Angriff aus Aufgabe 19 auch auf h anwenden?

(b) Definieren Sie $\textsc{renc}(l)$, sodass $|\textsc{renc}(l)| \bmod 8 = 0$ und $|\textsc{renc}(l)| = \log_2(l) + \mathcal{O}(\log\log(l))$.

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. Hierbei identifizieren wir einen Binärstring $x_{l-1} \ldots x_0 \in \{0,1\}^l$ mit der Zahl $\sum_{i=0}^{l-1} x_i 2^i \in \mathbb{Z}_{2^l}$.

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

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