Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 5

Besprechung der mündlichen Aufgaben am 11. 12. 2020
Abgabe der schriftlichen Lösungen bis 15. 12. 2020, 23:59 Uhr

Aufgabe 30 ***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 31 ***mündlich***

Sei $E_k \colon \{0,1\}^t \to \{0,1\}^t$, $k \in K$, eine Familie von Verschlüsselungsfunktionen und $y : \{0,1\}^* \to \bigcup_{n \geq 1} \{0,1\}^n t$ mit $x \mapsto y(x) = y_0 \ldots y_n$ eine Preprocessing-Funktion, wobei $y_0 = \mathrm{bin}_t(|x|)$ und $y_1 \ldots y_n = x0^{nt-|x|}$ mit $n = \lceil |x|/t \rceil$ gilt. Sei h'_k der CBC-MAC basierend auf E_k ohne Preprocessing und h_k der CBC-MAC mit Preprocessing.

(a) Zeigen Sie, dass sich der Geburtstagsangriff auf h'_k aus der Vorlesung so modifizieren lässt, dass statt x_1 ein beliebiger Block x_l $(2 \leq l < n)$ eingeschränkt wird und alle andere Blöcke frei wählbar sind.

(b) Modifizieren Sie den Geburtstagsangriff aus der Vorlesung so, dass er auch gegen h_k funktioniert.

Aufgabe 32 ***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 33 ***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 34 ***mündlich***

Sei E die elliptische Kurve $y^2 = x^3 - 12x - 16$ über $\mathbb{R}$.

(a) Skizzieren Sie zeichnerisch den Verlauf von E.

(b) Berechnen Sie die Summe $P + Q$ für $P = (4, 0)$ und $Q = (5, 7)$

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

Aufgabe 35 ***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 36 ***10 Punkte***

Sei E die elliptische Kurve $y^2 = x^3 - 7x - 6$ über $\mathbb{R}$.

(a) Skizzieren Sie zeichnerisch den Verlauf von E.

(b) Berechnen Sie die Summe $P + Q$ für $P = (3, 0)$ und $Q = (4, \sqrt{30})$.

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