Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 3

Besprechung der mündlichen Aufgaben am 10. 11. 2022
Abgabe der schriftlichen Lösungen bis 15. 11. 2022, 23:59 Uhr

Aufgabe 14 ***mündlich***

Sei $y\colon \{0,1\}^* \to \bigcup_{k\geq 1}\{0,1\}^{kr}$ eine sponge-konforme Paddingfunktion, seien $f_o : \{0,1\}^b \to \{0,1\}^r$ und $f_i : \{0,1\}^b \to \{0,1\}^c \setminus \{0^c\}$ kollisionsresistente Kompressionsfunktionen sowie $f : \{0,1\}^b \to \{0,1\}^b$ mit $f(x) = f_o(x)f_i(x)$ (Konkatenation). Zeigen Sie, dass für alle m und $l = rm$ die Funktion $h : \{0,1\}^* \to \{0,1\}^l$ eine kollisionsresistente Hashfunktion ist, falls

$$h(x) = \textsc{Sponge}_{f,y,r}(l,x) \quad .$$

Hinweis: Zwar wird in der Aufgabe Kollisionsresistenz bewiesen, das Anwendungsszenario entspricht aber nicht dem typischen Einsatz der Sponge-Konstruktion, wo r in der Regel deutlich kleiner als c ist und sich die Sicherheit vor allem auf die inneren c Bits stützt. Kollisionsresistenz für f_o führt die Sqeezingidee ein Stück weit ad absurdum.

Aufgabe 15 ***mündlich***

Für eine sponge-konforme Paddingfunktion y für Bitrate $r \geq 1$ verlangen wir unter anderem, dass $\forall k \geq 0\, \forall x \neq x' : y(x) \neq y(x')0^{kr}$. Sei y eine Paddingfunktion, die dies für das Paar x, x' verletzt.

(a) Zeigen Sie, dass es jede Funktion h mit $h_l(x) = \textsc{Sponge}_{f,y,r}(l,x)$ und $f : \{0,1\}^b \to \{0,1\}^b$ zwei Längen l, l' gibt, sodass $h_l(x)$ Suffix von $h_{l'}(x')$ ist.

(b) Zeigen Sie, dass es ein Paar $x \neq x'$ und eine Permutation $f : \{0,1\}^b \to \{0,1\}^b$ gibt, sodass für alle $l \geq 0$ und für die Funktion h_l aus a) gilt: $h_l(x) = h_l(x')$.

Aufgabe 16 ***mündlich***

Sei $f : \{0,1\}^b \to \{0,1\}^b$ eine Permutation und $r \leq b$ beliebig sowie $c = b - r$ und $h_l(x) = \textsc{Sponge}_{f,y,r}(l,x)$ mit $y = \mathrm{id}_{\{0,1\}^*}$ (wir ignorieren also das Padding).
Ermitteln Sie eine obere Schranke für die minimale Zahl l mit $\forall k \forall x, x' \in (\{0,1\}^r)^* : h_{l+k}(x) \neq h_{l+k}(x') \Rightarrow h_l(x) \neq h_l(x')$, d.h. ab wann lohnt es sich garantiert nicht mehr, weitere Bits aus dem Sponge auszugeben, um Kollisionen zu verhindern?

Aufgabe 17 ***10 Punkte***

Seien $b = 8$ und $r = c = 4$. Geben Sie eine Funktion $f\colon \{0,1\}^8 \to \{0,1\}^8$ und zwei Werte $x, x' \in (\{0,1\}^4)^*$ an, sodass für die Funktion h_l aus Aufgabe 16 gilt: $h_{1024}(x) \neq h_{1024}(x')$, aber $h_{896}(x) = h_{896}(x')$.

Aufgabe 18 ***mündlich***

Sei A eine $(m \times l)$-Matrix über dem endlichen Körper K und sei $y \in K^m$.

(a) Zeigen Sie: Das Gleichungssystem ist genau dann lösbar, falls A und die um den Vektor y erweiterte Matrix $A|y$ denselben Rang haben.

(b) Zeigen Sie: Das Gleichungssystem $Ax = y$ besitzt im Falle der Lösbarkeit genau $\|K\|^{l-r}$ Lösungen, falls r der Rang von A ist.

(c) Geben Sie eine notwendige und hinreichende Bedingung dafür an, dass das Gleichungssystem für alle $y \in K^m$ lösbar ist.