Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 12
16. Januar 2019

Übungen zur Kryptographie
Lösung

Aufgabe 45

b) Wir erhalten $\omega = 79572\,40097$.[1]

Aufgabe 46

Für $x = 1$ ist $\mathrm{ch}(x, y, z) = y$ und $x \wedge y = y, \overline{x} \wedge z = 0$ sowie $(x \wedge y) \oplus (\overline{x} \wedge z) = y$. Analog ist für $x = 0$: $\mathrm{ch}(x, y, z) = z = 0 \oplus z = (x \wedge y) \oplus (\overline{x} \wedge z)$.
O.B.d.A sei $x = 0, y = 0$ und damit $\mathrm{maj}(x, y, z) = 0$. Dann ist aber auch $x \wedge y, x \wedge z, y \wedge z = 0$. Ist $x = y = 1$, dann ist $\mathrm{maj}(x, y, z) = 1$ und $x \wedge y = 1$ sowie $x \wedge z = z, y \wedge z = z \Rightarrow (x \wedge z) \oplus (y \wedge z) = 0$.

Aufgabe 47

a) $K[i] = \lfloor 2^{32}(\sqrt[3]{p_i} - \lfloor \sqrt[3]{p_i} \rfloor) \rfloor$ ist gerade die Definition von $K[i]$. Sei $\sqrt[3]{p_i} = \sum_{i=-2}^{\infty} b_i 2^{-i}$. Dann ist $\sqrt[3]{p_i} - \lfloor \sqrt[3]{p_i} \rfloor = \sum_{i=1}^{\infty} b_i 2^{-i}$ und $2^{32}(\sqrt[3]{p_i} - \lfloor \sqrt[3]{p_i} \rfloor) = \sum_{i=1}^{\infty} b_i 2^{32-i}$. Es folgt $\lfloor 2^{32}(\sqrt[3]{p_i} - \lfloor \sqrt[3]{p_i} \rfloor) \rfloor = \sum_{i=1}^{32} b_i 2^{32-i} = (b_1, \ldots, b_{32})$.

b) Die Zahl $K[30] =$ `06CA6351` hat 5 führende Nullen.

c) Für 8 ist $p_{565} = 4099$ und $K[565] = (11111111\,11101111\,11000000)_2 = 16773056$. Weiter ist $p_{22051} = 250049$ und $K[22051] = (1011\,00000000\,11000000)_2 = 721088$ sowie $p_{660808} = 9938377$ und $K[660808] = (11110001\,11110110)_2 = 60788$.

Aufgabe 48

a) Für $i = 10$ und $j = 19$ sowie für $i = 25$ und $j = 41$ stimmen jeweils die ersten 10 Stellen überein.

b) Für $p_5 = 11$ und $p_{2515} = 22483$ ist $K[4] - K[2514] = 47526 = (10111001\,10100110)_2$. Oder $p_{207} = 1279, p_{865} = 6703$ und $K[864] - K[206] = 31850 = (1111100\,01101010)_2$. Weiter ist für $p_{977} = 7699$ und $p_{8169} = 83717$ ist $K[8168] - K[976] = 96 = (1100000)_2$. Schließlich ist für $p_{18383} = 205031$ und $p_{20150} = 226609$ ist $K[18382] - K[20149] = 0$.

[1] Mittels $P = \omega P_0$ kann man die Richtigkeit von ω überprüfen.