Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
16. Jan. 2019

Übungen zur Vorlesung Kryptographie

Blatt 12

Aufgabe 45

Für ihr ECDL-Signier-System verwendet Alice eine Elliptische Kurve E über dem Körper $\mathbb{F}_p = \mathbb{Z}/p$, ein Element $P_0 \in E_{\text{aff}}(\mathbb{F}_p)$ mit Primzahlordnung q, sowie einen weiteren Punkt $P \in E_{\text{aff}}(\mathbb{F}_p)$ mit $P = \omega \cdot P_0$, wobei $\omega \in \mathbb{Z}/q$ von Alice geheimgehalten wird. Der öffentliche Schlüssel ist nun (E, p, q, P_0, P). Außerdem gehört zu dem Signier-System eine öffentlich bekannte Hash-Funktion mit der Bitlänge r, wobei $2^r < q$, so dass die Hash-Werte $H(x)$ in natürlicher Weise als Elemente von $\mathbb{Z}/q$ aufgefasst werden können (MSB first). Die Funktion $\psi : E_{\text{aff}}(\mathbb{F}_p) \to \mathbb{Z}/q$ ist wie folgt definiert: Für einen Punkt $Q = (\xi, \eta) \in E_{\text{aff}}(\mathbb{F}_p)$ sei $\psi(Q) := \xi$.

Zum Signieren einer Nachricht $x \in \mathbb{Z}_2^n$ wählt Alice eine geheim zu haltende Zufallszahl $\lambda \in (\mathbb{Z}/q)^*$. Die Signatur von x ist dann $\text{sig}(x) = (s_1, s_2) \in (\mathbb{Z}/q) \times (\mathbb{Z}/q)$, wobei

$$s_1 := \psi(\lambda \cdot P_0), \qquad s_2 := (H(x) + \omega \cdot s_1)\lambda^{-1}.$$

a) Man zeige: Verwendet Alice zum Signieren zweier verschiedener Nachrichten $x \in \mathbb{Z}_2^n$, $y \in \mathbb{Z}_2^m$ dieselbe geheime Zufallszahl λ, so kann Eve aus der Kenntnis von $H(x)$, $H(y)$, $\text{sig}(x)$, $\text{sig}(y)$ Alice's Geheimzahl ω berechnen (und damit künftig Alice's Unterschrift fälschen).

b) Man berechne ω im speziellen Fall

$$\begin{aligned} E &: Y^2 = X^3 + X + 60, \quad p = 85470\,62921, \quad q = 85469\,44457, \\ P_0 &= (10000\,00001, 48575\,61959), \quad P = (68316\,95389, 28678\,59999), \\ \text{sig}(x) &= (28595\,38369, 83908\,10232), \quad \text{sig}(y) = (28595\,38369, 71341\,01019) \end{aligned}$$

für Nachrichten x, y mit $H(x) =$ `3412 FABD`, $H(y) =$ `AFFE 8765` (hexadezimal)

Aufgabe 46

Im SHA-256-Algorithmus treten u.a. folgende Funktionen auf:

$$\text{ch}, \text{maj} : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 = \{0, 1\},$$

die wie folgt definiert sind:

$$\text{ch}(x, y, z) := \begin{cases} y, & \text{falls } x = 1, \\ z, & \text{falls } x = 0; \end{cases}$$

$$\text{maj}(x, y, z) := \begin{cases} 0, & \text{falls mindestens zwei Argumente} = 0, \\ 1, & \text{falls mindestens zwei Argumente} = 1. \end{cases}$$

b.w.

Man zeige:

$$\begin{aligned} \mathrm{ch}(x,y,z) &= (x \wedge y) \oplus (\overline{x} \wedge z), \\ \mathrm{maj}(x,y,z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z). \end{aligned}$$

Aufgabe 47

Im SHA-256-Algorithmus treten folgende 64 Runden-Konstanten auf (hexadezimale Schreibweise):

```
K[0..63] =
  (0x428A2F98, 0x71374491, 0xB5C0FBCF, 0xE9B5DBA5, 0x3956C25B, 0x59F111F1,
   0x923F82A4, 0xAB1C5ED5, 0xD807AA98, 0x12835B01, 0x243185BE, 0x550C7DC3,
   0x72BE5D74, 0x80DEB1FE, 0x9BDC06A7, 0xC19BF174, 0xE49B69C1, 0xEFBE4786,
   0x0FC19DC6, 0x240CA1CC, 0x2DE92C6F, 0x4A7484AA, 0x5CB0A9DC, 0x76F988DA,
   0x983E5152, 0xA831C66D, 0xB00327C8, 0xBF597FC7, 0xC6E00BF3, 0xD5A79147,
   0x06CA6351, 0x14292967, 0x27B70A85, 0x2E1B2138, 0x4D2C6DFC, 0x53380D13,
   0x650A7354, 0x766A0ABB, 0x81C2C92E, 0x92722C85, 0xA2BFE8A1, 0xA81A664B,
   0xC24B8B70, 0xC76C51A3, 0xD192E819, 0xD6990624, 0xF40E3585, 0x106AA070,
   0x19A4C116, 0x1E376C08, 0x2748774C, 0x34B0BCB5, 0x391C0CB3, 0x4ED8AA4A,
   0x5B9CCA4F, 0x682E6FF3, 0x748F82EE, 0x78A5636F, 0x84C87814, 0x8CC70208,
   0x90BEFFFA, 0xA4506CEB, 0xBEF9A3F7, 0xC67178F2);
```

Sie sind wie folgt definiert: $K[i]$ ist die 32-Bit-Zahl, die aus den ersten 32 Nachkomma-Stellen der Binär-Entwicklung der Kubikwurzel aus der i-ten Primzahl p_i besteht ($p_0 = 2$, $p_1 = 3$, …, $p_{63} = 311$).

a) Man zeige:

$$K[i] = \left\lfloor 2^{32} \left(\sqrt[3]{p_i} - \lfloor \sqrt[3]{p_i} \rfloor \right) \right\rfloor.$$

b) Da $64 = 2^6$, könnte man erwarten, dass eine der Konstanten 6 führende Nullen in der Binär-Entwicklung aufweist. Welche der Konstanten hat die meisten führenden Nullen?

c) (Analogon des Blockchain Hash-Puzzles) Bis zu welcher Primzahl muss man gehen, um 8, 12, oder 16 führende Nullen zu haben?

Aufgabe 48 (Fortsetzung von Aufgabe 47)

a) Nach dem Geburtstags-Paradoxon könnte man erwarten, dass es unter den Konstanten $K[i]$ zwei verschiedene gibt, die in den ersten 12 Binärstellen übereinstimmen. Für welche Indizes $0 \leqslant i < j < 64$ haben die 32-Bit-Konstanten $K[i]$ und $K[j]$ die längste Übereinstimmung (Kollision) führender Stellen in der Binär-Darstellung?

b) Durch weitere Berechnungen mit größeren Primzahlen versuche man, Kollisionen der Länge 16, 24 und 32 zu erzeugen.