



Übung 10

Ausgabe: Freitag, 21. Dezember 2007

Besprechung: Montag, 7. Januar bis Freitag, 12. Januar

Aufgabe 1 (RSA-OAEP-Variante)

Alice E. Sicher schlägt folgende Vereinfachung von RSA-OAEP vor: Um eine Nachricht $m \in M_{pk} = \{0, 1\}^{n/2}$ zu verschlüsseln, wähle $r \in \{0, 1\}^{n/4}$ zufällig und setze

$$C = (\text{Zahl}(m || 0^{n/4} || r))^e \bmod N,$$

wobei wir zur Vereinfachung annehmen, dass n durch 4 teilbar ist und der Bitstring $m || 0^{n/4} || r$ sich durch die (übliche) Abbildung $\text{Zahl}(x) = \sum x_i \cdot 2^i$ von Strings auf Zahlen stets auf einen Wert aus \mathbb{Z}_N^* abbilden lässt (und das erste Bit des m -Teils höchstwertig ist). Beim Entschlüsseln berechnet man die d -te Potenz und wandelt die so erhaltene Zahl wieder in einen Bitstring um, und gibt m aus, falls die $n/4$ "Test-Bits" alle 0 sind, und \perp sonst.

Ist diese Variante noch CCA-IND?

Hinweis: Sie können zunächst mit einer noch einfacheren Variante starten, bei der die Nachricht $3n/4$ Bits hat und dafür die Nullbits $0^{n/4}$ entfallen. Die Analyse lässt sich dann auf den Fall mit $0^{n/4}$ übertragen.

B.W.

Aufgabe 2 (Kombination von Hash-Funktionen)

Alice E. Sicher möchte zusätzlich die Kollisionsresistenz von Hash-Funktionen verbessern, indem sie zwei vermutlich kollisionsresistente Hash-Funktionen H_0 und H_1 (z.B. SHA-386 und SHA-256) zu einer Hash-Funktion H kombiniert, so dass folgendes gilt: Sofern mindestens eine der beiden Hash-Funktionen H_0, H_1 tatsächlich kollisionsresistent ist, dann ist es auch die Kombination H . Mit anderen Worten, selbst wenn sich eine der beiden Hash-Funktionen als schwach herausstellt, soll die Kombination noch sicher sein, sofern die andere Hash-Funktion noch sicher ist.

Alice schlägt zwei Varianten vor (wobei die zweite Variante kürzere Hash-Werte erzeugt):

$$H(m) = H_0(m) || H_1(m), \quad H^*(m) = H_1(H_0(m)).$$

Dabei nehmen wir an, dass die Hash-Funktionen längeninvariant sind, also die Ausgabelänge nur vom Sicherheitsparameter abhängt, aber für alle Eingaben m sonst gleich lang ist (so dass man im ersten Fall klar den H_0 -Teil und den H_1 -Teil trennen kann).

Diskutieren Sie die Sicherheit der beiden Ansätze (können Sie die Vorschläge als sicher beweisen, oder brechen, etc.?).