Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 14 / 3./4. Februar 2014

AUFGABE 1:

Wir betrachten das Lamport Einwegsignaturverfahren (Folie 141). Beschreiben Sie einen Angreifer, der Signaturen von zwei Nachrichten seiner Wahl erhält und anschließend Signaturen für andere Nachrichten fälschen kann.

AUFGABE 2:

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Funktion. Betrachten Sie eine Variante $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ des Lamport Verfahrens, parametrisiert durch $\ell \in \mathbb{N}$ mit $\ell = \ell(n)$ polynomiell in n, für Nachrichten $m \subset \{1, \ldots, 2\ell\}$ mit $|m| = \ell$, d.h. für insgesamt $\binom{2\ell}{\ell}$ Nachrichten:

$\mathsf{Gen}(1^n)$: Wähle $x_1, \ldots, x_{2\ell} \in_R \{0,1\}^n$ und setze $y_i = f(x_i)$ für $1 \leq i \leq 2\ell$.
Setze $\mathsf{sk} := (x_1, \ldots, x_{2\ell})$ und $\mathsf{pk} := (y_1, \ldots, y_{2\ell})$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Falls $m \not\subset \{1, \ldots, 2\ell\}$ oder $|m| \neq \ell$ gib $\perp$ zurück, sonst gib $\sigma := \{x_i\}_{i \in m}$ zurück.

In jeder Nachrichten werden also genau ℓ der 2ℓ Elemente ausgewählt. Mögliche Nachrichten für $2l = 8$ wären also $\{1,3,5,6\}$ und $\{2,3,4,8\}$, aber nicht $\{2,4,5,6,7\}$ (zu viele Elemente), nicht $\{1,4,6\}$ (zu wenige Elemente) und auch nicht $\{1,3,6,9\}$ (darf nur Zahlen von 1 bis 8 enthalten). Die zugehörigen Signaturen für die gültigen Nachrichten wären $\{x_1, x_3, x_5, x_6\}$ bzw. $\{x_2, x_3, x_4, x_8\}$.

(a) Geben Sie eine Vrfy-Funktion an und zeigen Sie die Korrektheit von Π.

(b) Zeigen Sie, dass Π ein CMA-sicheres Einwegsignaturverfahren ist, falls f eine Einwegfunktion ist.

Bitte wenden!

AUFGABE 3:

Zeigen Sie, dass das Paillier-Verschlüsselungsverfahren nicht CCA-sicher ist. Konstruieren Sie dazu einen Angreifer auf die CCA-Sicherheit.

AUFGABE 4:

Wir betrachten das Rabin-Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}$ aus der Vorlesung, wobei $\mathsf{lsb}(x)$ das unterste Bit von x liefert:

$\mathsf{Gen}(1^n)$: $(N,p,q) \leftarrow \mathsf{GenModulus}(1^n)$ mit N Blumzahl, $\mathsf{pk} := N$ und $\mathsf{sk} := (p,q)$.

$\mathsf{Enc}_{\mathsf{pk}}(m)$: Wähle $x \in_R \mathcal{QR}_N$, gib $c := (c_1, c_2) := (x^2 \bmod N, \mathsf{lsb}(x) \oplus m)$ zurück.

$\mathsf{Dec}_{\mathsf{sk}}(c)$: Berechne die Hauptwurzel x von c_1 und gib $m := \mathsf{lsb}(x) \oplus c_2$ zurück.

(a) Geben Sie die Definition von CPA-Sicherheit und das Spiel $\mathsf{PubK}^{\mathsf{cpa}}$ an.

(b) Zeigen Sie, dass $\mathsf{lsb}(x)$ ein *Hardcoreprädikat* ist, falls Π *CPA-sicher* ist. Zeigen Sie dazu, dass für alle ppt-Angreifer $\mathcal{A}$ gilt:

$$\underset{x \in_R \mathcal{QR}_N}{\mathsf{Ws}}[\mathcal{A}(1^n, N, x^2 \bmod N) = \mathsf{lsb}(x)] \leq \frac{1}{2} + \mathsf{negl}(n).$$