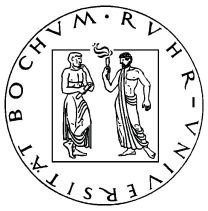
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Hausübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 6 / 01. Juli 2009 / Abgabe spätestens 15. Juli, 8:30 Uhr

Klausurtermin: 20. August 2009
zugelassene Hilfsmittel : 1 beidseitig handbeschriebenes A4 Blatt.

AUFGABE 1 (5 Punkte)**:**
Das *Textbook-Rabin Signaturschema* funktioniert wie das Textbook-RSA Signaturschema mit dem Unterschied, dass die Rabin Trapdoor Permutation verwendet wird. Zeigen Sie, das ein Angreifer mit einem Chosen Message Angriff aus Textbook Rabin Signaturen den privaten Schlüssel rekonstruieren kann.

AUFGABE 2 (5 Punkte)**:**
Sei f eine Einwegpermutation. Wir betrachten das folgende Signaturschema für Nachrichten aus der Menge $\{1, \ldots, n\}$:

- Für die Schlüsselerzeugung wird ein zufälliges $x \in \{0,1\}^n$ gewählt und $y := f^n(x)$ berechnet. Der öffentliche Schlüssel ist nun y und der private Schlüssel ist x.
- Um eine Nachricht $i \in \{1, \ldots, n\}$ zu signieren wird die Signatur $f^{n-i}(x)$ ausgegeben (wobei $f^0(x) = x$).
- Eine Signatur σ für eine Nachricht i bezüglich des öffentlichen Schlüssels y wird verifiziert indem geprüft wird, ob $y \stackrel{?}{=} f^i(\sigma)$.

1. Zeigen Sie, dass das vorgestellte Verfahren kein One-Time Signaturschema ist.

   Gegeben sei eine Signatur für Nachricht i, für welche Nachrichten j kann ein Angreifer eine Fälschung erzeugen?

2. Zeigen Sie, dass es keinen ppt. Angreifer gibt, der aus einer Signatur für Nachricht i eine Fälschung für irgendeine Nachricht $j > i$ berechnet (ausser mit vernachlässigbarer Wahrscheinlichkeit).

3. Wie kann das angegebene Verfahren modifiziert werden um ein One-Time Signaturverfahren zu erhalten?

   Hinweis: Benutzen Sie zwei Werte y, y' im öffentlichen Schlüssel.

AUFGABE 3 (5 Punkte)**:**
Das Lamport One-Time Signaturverfahren benutzt 2ℓ Werte im öffentlichen Schlüssel um Nachrichten der Länge ℓ zu signieren. Betrachten Sie die folgende Variante: der private Schlüssel besteht aus 2ℓ Werten $x_1, \ldots, x_{2\ell}$ und der öffentliche Schlüssel beinhaltet die Werte $y_1, \ldots, y_{2\ell}$ mit $y_i = f(x_i)$. Eine Nachricht $m \in \{0,1\}^{\ell'}$ wird 1-zu-1 auf eine Teilmenge $S_m \subset \{1, \ldots, 2\ell\}$ der Größe ℓ abgebildet. Um eine Nachricht zu signieren veröffentlicht der Signierer $\{x_i\}_{i \in S_m}$. Zeigen Sie, dass dieses Verfahren ein One-Time Signaturverfahren ist. Was ist die maximale Nachrichtenlänge ℓ' für dieses System?

AUFGABE 4 (5 Punkte)**:**

Definition: Eine Familie von Funktionen Π_f besteht aus den 3 ppt Algorithmen:

- $I \leftarrow \mathsf{Gen}(1^n)$ wobei I eine Urbildmenge $\mathcal{D}_I$ und einen Wertebereich $\mathcal{R}_I$ definiert.
- $x \leftarrow \mathsf{Samp}(I)$ wobei $x \in_R \mathcal{D}$.
- $y = f(I, x)$ mit $y \in \mathcal{R}_I$ und $x \in \mathcal{D}_I$.

(vgl. Permutationsfamilie)

Das Spiel $\mathsf{Invert}_{\mathcal{A},\Pi_f}(n)$ ist analog zu dem im Skript angegebenen Spiel für Permutationsfamilien und wir sagen, dass eine Familie von Funktionen eine *Einwegfunktionsfamilie* ist, falls für alle ppt. Angreifer $\mathcal{A}$ eine vernachlässigbare Funktion negl existiert, so dass

$$Pr[\mathsf{Invert}_{\mathcal{A},\Pi_f}(n) = 1] \leq \mathsf{negl}(n).$$

Sei (Gen, H) eine kollisionsresistente Hashfunktion, die Strings der Länge $2n$ auf Strings der Länge n abbildet. Zeigen Sie, dass die Familie von Funktionen $\Pi = (\mathsf{Gen}, \mathsf{Samp}, H)$ eine Einwegfunktionsfamilie ist. Samp ist dabei der triviale Algorithmus, der einen zufälligen String der Länge $2n$ ausgibt.
Hinweis: Das Urbild eines zufälligen Wertes x liefert nicht immer eine Kollision, aber meistens...