



Übung 12

Ausgabe: Freitag, 18. Januar 2008

Besprechung: Montag, 21. Januar bis Freitag, 25. Januar

Dies ist das letzte Übungsblatt der Veranstaltung. In der letzten Vorlesungswoche haben Sie die Gelegenheit, in den Übungen nochmal vorangegegangene Aufgaben zu diskutieren.

Aufgabe 1 (Unsichere DSA-Variante)

Zur Erinnerung: Eine DSA-Signatur $s = (r, t)$ für eine Nachricht m wird berechnet, indem man ein $k \in \mathbb{Z}_q^*$ zufällig wählt, und dann

$$r = (g^k \bmod p) \bmod q, \quad t = k^{-1} \cdot (H(m) + xr) \bmod q$$

für den geheimen Schlüssel (p, g, q, x) zu $y = g^x \bmod p$ und die Hash-Funktion $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q$ berechnet.

Zeigen Sie, dass das Verfahren nicht CMA-UNF ist, wenn der Signierer für alle Unterschriften das gleiche k verwendet (z.B. wegen eines äußerst schwachen Pseudozufallsgenerator zur Generierung von k).

Anmerkung: Es kann übrigens der äußerst seltene Fall eintreten, dass $r = 0 \bmod q$ in einer korrekt erzeugten Signatur ist. Die Verifikation lehnt solche Unterschriften ab, da unter anderem $r \in \mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\}$ geprüft wird. In diesem Sinne ist das DSA-Verfahren nicht vollständig. Da dieser Fall aber nur mit sehr kleiner Wahrscheinlichkeit eintritt, beachten wir ihn in der Regel nicht weiter.

Lösungshinweis: Sie können annehmen, dass die Hash-Funktion kollisionsresistent ist und somit keine Nachrichten $m \neq m^*$ mit $H(m) = H(m^*)$ während eines effizienten Angriffs auftreten. Sie können sogar zeigen, dass ein Angreifer mit sehr hoher Wahrscheinlichkeit nicht nur Signaturen fälschen kann, sondern sogar den geheimen Schlüssel erhalten kann (außer, wenn $r = 0 \bmod q$).

Aufgabe 2 (Signaturverfahren und Strong Unforgeability)

Analog zu den MACs kann man einen stärkeren Sicherheitsbegriff für Signaturen definieren, bei dem es für Angreifer nicht nur schwierig sein soll, eine gültige Signatur für eine neue Nachricht zu erzeugen, sondern es soll auch keine weitere Signatur s^* zu einer bereits unterschriebenen Nachricht m_i (mit Signatur $s_i \neq s^*$) leicht gefunden werden können. Formal betrachtet man das CMA-UNF-Experiment für Signaturverfahren (Folie 4, Kapitel 8), fordert aber nun, dass für alle effizienten Angreifer \mathcal{A} die Wahrscheinlichkeit, dass $\text{Vf}(pk, m^*, s^*) = 1$ und $(m^*, s^*) \neq (m_1, s_1), (m_2, s_2), \dots$ vernachlässigbar sein soll (CMA-sUNF).

Zeigen Sie, dass es ein Signaturverfahren gibt, das CMA-UNF ist, aber nicht CMA-sUNF (vorausgesetzt, es gibt überhaupt CMA-UNF-sichere Verfahren).