Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie II

SS 2012

Blatt 5 / 29. Juni 2012 / Abgabe **bis spätestens Mittwoch, 11.07.2012 10:00 Uhr**

AUFGABE 1:

Anstelle von hashed RSA kann man versuchen, die bestehenden Angriffe gegen Textbook RSA Signaturen zu unterbinden, indem man Encoded RSA benutzt (siehe Präsenzblatt 5). Für einen $n+1$-Bit RSA Modulus N betrachten wir dazu die Kodierung
$\text{encode}_N(m) = m \mid\mid m \in \{0,1\}^n \subset \mathbb{Z}_N$ für $0 \neq m \in \{0,1\}^{\frac{1}{2}n}$.

Wir betrachten also $\Pi_{\text{encRSA}} = (\mathbf{Gen}, \mathbf{Sign}, \mathbf{Vrfy})$ mit
Gen: Ruft $N \leftarrow$ GenModulus auf, wobei N genau $n+1$ Bit hat und wählt $e \in_R \mathbb{Z}^*_{\phi(N)}, d = e^{-1} \bmod \phi(N)$. Gibt (N,e) als public key aus und (N,d) als secret key.
$\mathbf{Sign}_{N,d}(m)$: Gibt $(m \mid\mid m)^d \bmod N$ aus für $0^{\frac{n}{2}} \neq m \in \{0,1\}^{\frac{n}{2}}$.
$\mathbf{Vrfy}_{N,e}(m,\sigma)$: Akzeptiere, gdw. $0 \neq m \in \{0,1\}^{\frac{n}{2}}$ ist und $\sigma^e \bmod N = m \mid\mid m$.

Zeigen Sie, dass dieses Π_{encRSA} nicht CMA-sicher ist. [4 Punkte]

AUFGABE 2:

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Einwegpermutation. Wir konstruieren daraus folgendes Signaturverfahren $\Pi_f = (\mathbf{Gen}, \mathbf{Sign}, \mathbf{Vrfy})$ für den (sehr kleinen) Nachrichtenraum $\{1, \dots M\}$ mit $M = \text{poly}(n)$.

$\mathbf{Gen}(1^n)$: Wählt $x, x' \in_R \{0,1\}^n$ unabhängig, uniform und setze $y = f^M(x), y' = f^M(y')$. Der public key ist (y,y'). Der secret key ist (x,x').
$\mathbf{Sign}_{x,x'}(m)$: Berechne $\sigma = f^{m-1}(x)$ und $\sigma' = f^{M-m}(x')$. Ausgabe (σ,σ')
$\mathbf{Vrfy}_{y,y'}(m,\sigma,\sigma')$: Teste ob sowohl $f^{M+1-m}(\sigma) = y$ und $f^m(\sigma') = y'$ ist. Falls beides der Fall ist, akzeptiere, andernfalls nicht.

Dabei bedeutet $f^i(x)$ die i-fache Hintereinanderausführung von f, d.h. $f^0(x) = x$, $f^1(x) = f(x)$, $f^2(x) = f(f(x))$, usw.

Zeigen Sie:

(a) Π_f ist ein korrektes Signaturverfahren. [1 Punkt]

(b) Π_f ist kein CMA-sicheres Signaturverfahren. [2 Punkte]

(c) Π_f ist CMA-sichere *Einweg*signatur. [5 Punkte]

Hinweise zu (c):
Da der Nachrichtenraum nur polynomiell gross ist, kann und sollte Ihre Reduktion die Nachricht m, die der CMA-Angreifer A anfragen wird und die Nachricht $m_{\text{forge}} \neq m$, für die A die Fälschung $(m_{\text{forge}}, \sigma_{\text{forge}})$ ausgeben wird, raten, bevor A gestartet wird.
Wählen Sie eines der Paare (x, y) oder (x', y') selbst wie in **Gen** und betten Sie Ihre Challenge $z = f(a)$ für die Einwegpermuation geschickt in das andere Paar ein, so dass Sie sowohl die Signatur von m kennen als auch aus σ_{forge} das gesuchte Urbild a berechnen können.

AUFGABE 3:

Wie bei MACs kann man bei Signaturen und Einwegsignaturen auch einen stärkeren Sicherheitsbegriff betrachten. Wir nennen ein (Einweg)signaturverfahren $\Pi = (\mathbf{Gen}, \mathbf{Sign}, \mathbf{Vrfy})$ stark sicher, wenn es durch ppt. Algorithmen A nicht mit nicht-vernachlässibarer Wahrscheinlichkeit möglich ist, eine gültige Forgery (m, σ) auszugeben. Dabei darf A Signieranfragen für Nachrichten m_i (bei Einwegsignaturverfahren höchstens einmal, sonst polynomiell oft) stellen mit Antworten σ_i. (m, σ) ist gültige Fälschung, falls $\mathbf{Vrfy}_{\text{pk}}(m, \sigma) = 1$ und $(m, \sigma) \neq (m_i, \sigma_i)$ für alle zuvor gestellten Anfragen.
Im Gegensatz zur normalen CMA-Sicherheit ist hierbei $m = m_i$ erlaubt, wenn $\sigma \neq \sigma_i$ ist.

(a) Geben Sie eine formale Definition von starker CMA-sicherheit für Einwegsignaturen an. Definieren Sie sich hierfür ein geeignetes Spiel. [2 Punkte]

(b) Zeigen Sie, dass Lamports Einwegsignaturverfahren Π_f ein stark CMA-sicheres Einwegsignaturverfahren ist, wenn die verwendete Einwegfunktion f eine Einwegpermuatation ist. [2 Punkte]

(c) Sei f eine Einwegfunktion. Konstruieren Sie damit eine neue Einwegfunktion f', so dass Lamports Einwegsignaturverfahren $\Pi_{f'}$ damit *kein* stark sicheres Einwegsignaturverfahren ist. [2 Punkte]