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

Hausübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 5 /
Abgabe: 05. Juli 2013, 10 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Betrachten Sie folgende Variante der Goldwasser-Micali Verschlüsselung: $\mathsf{GenModulus}(1^n)$ liefert (N, p, q), der öffentliche Schlüssel ist N und der geheime Schlüssel (p, q). Um eine 0 zu verschlüsseln wählt der Sender n zufällige Elemente $c_1, \ldots, c_n \in_R \mathcal{QR}_N$. Um eine 1 zu verschlüsseln wählt der Sender n zufällige Elemente $c_1, \ldots, c_n \in_R \mathcal{J}_N^{+1}$. In beiden Fällen ist der Chiffretext $c := (c_1, \ldots, c_n)$.

(a) Zeigen Sie, dass der Sender ein zufälliges Element aus $\mathcal{J}_N^{+1}$ in (erwarteter) Polynomialzeit erzeugen kann.

(b) Wie kann der Empfänger effizient den Chiffretext entschlüsseln? Mit welcher Wahrscheinlichkeit tritt dabei ein Entschlüsselungsfehler auf?

(c) Zeigen Sie, dass wenn die Quadratische Residuositätsannahme bzgl. $\mathsf{GenModulus}$ gilt, so ist das Verfahren CPA-sicher.

Hinweis: Wählen Sie in der Reduktion $b \in_R \{0, 1\}$ und dann die c_i abhängig von der Eingabe z des Unterscheiders als $c_i := z^{b \cdot d_i} \cdot x_i$ für $x_i \in_R \mathcal{QR}_N$ und $d_i \in_R \{0, 1\}$. Sie können im Fall $z \in \mathcal{QNR}_N^{+1}$ und $b = 1$ ohne Beweis verwenden, dass die c_i so in $\mathcal{J}_N^{+1}$ *gleichverteilt* sind.

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

Beweisen Sie: Wenn das DCR-Problem hart ist bzgl. $\mathsf{GenModulus}$ (siehe Folie 111), so ist auch Faktorisieren hart bzgl. $\mathsf{GenModulus}$ (siehe Folie 57). Gehen Sie wie folgt vor:

(a) Zeigen Sie, dass man bei bekannter Faktorisierung effizient $f^{-1} : \mathbb{Z}_{N^2}^* \to \mathbb{Z}_N \times \mathbb{Z}_N^*$ berechnen kann.

(b) Zeigen Sie durch Angabe eines Unterscheiders, dass man das DCR-Problem effizient lösen kann, wenn f^{-1} effizient berechenbar ist.

AUFGABE 3 (5 Punkte)**:**

Sei $\Pi_f = (\mathsf{Gen}, \mathsf{Samp}, f_I, \mathsf{Inv})$ eine Familie von Td-Einwegpermutationen und $\mathsf{dh} : \{0,1\}^n \to \{0,1\}^2$ ein Doppelhardcoreprädikat für Π_f (siehe Präsenzübung 5, Aufgabe 4). Konstruieren Sie aus Π_f und dh analog zur Vorlesung (Folie 67) ein asymmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}^2$, d.h. wählen Sie $c = (f_I(x), m \oplus \mathsf{dh}(x))$.

Zeigen Sie die Korrektheit und die CPA-Sicherheit Ihres Verfahrens.

Hinweis: Raten Sie wie im Beweis auf Folie 70 das Doppelhardcoreprädikat mit $z \in_R \{0,1\}^2$. Betrachten Sie dann in der Reduktion die Ereignisse $\mathsf{GOOD} := (z = \mathsf{dh}(x) \wedge b = b')$ und $\mathsf{OKAY} := (z = \mathsf{dh}(x) \oplus m_0 \oplus m_1 \wedge b \neq b')$. Das Ereignis GOOD beschreibt also die Tatsache, dass dh richtig geraten wurde und der Angreifer korrekt antwortet, während OKAY das Ereignis beschreibt, dass z einen speziellen Wert annimmt und der Angreifer zudem mit seiner Antwort falsch liegt. Betrachten Sie oBdA nur Angreifer, die $m_0 \neq m_1$ wählen. Schätzen Sie schließlich $\mathsf{Ws}[d' = \mathsf{dh}(x)] \geq \mathsf{Ws}[d' = \mathsf{dh}(x) \wedge \mathsf{GOOD}] + \mathsf{Ws}[d' = \mathsf{dh}(x) \wedge \mathsf{OKAY}]$ ab.

AUFGABE 4 (5 Punkte)**:**

Sei $\mathsf{GenModulus}$ wie aus der Vorlesung bekannt ein Algorithmus der eine *Blumzahl* $N = p \cdot q$ und die zugehörige Faktorisierung p, q liefert. Wir betrachten nun eine Rabin-Variante (Folie 103) des ROM-RSA Verfahren aus der Vorlesung (Folie 74). Sei $H : \mathcal{QR}_N \to \{0,1\}^{\ell(n)}$ ein Random Oracle. Wir konstruieren daraus wie folgt ein asymmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}^{\ell(n)}$.

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

$\mathsf{Enc}_{\mathsf{pk}}(m)$: Wähle $r \in_R \mathcal{QR}_N$ und setze $c := (r^2 \bmod N, H(r) \oplus m)$.

(a) Geben Sie eine Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.

(b) Zeigen Sie, dass im ROM Π CPA-sicher unter der Faktorisierungsannahme ist.