Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 3 / 12. Mai 2010

AUFGABE 1. Gegenangriff.
Betrachten Sie den in der Vorlesung vorgestellten Chosen-Ciphertext Angriff auf das ElGamal-Verfahren. Ein Angreifer beobachtet dabei einen Chiffretext $c = \langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$ und sendet anschließend den Chiffretext $c' = \langle c_1, c_2 \cdot m' \rangle$, der eine gültige Verschlüsselung der Nachricht $m \cdot m'$ ist.
Angenommen der Empfänger findet es verdächtig, wenn zwei Verschlüsselungen mit der gleichen ersten Komponente an ihn gesendet werden und verwirft den zweiten Chiffretext. Zeigen Sie, wie ein Angreifer dieses Problem beseitigen kann!

AUFGABE 2. Umordnung.
Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein CCA-sicheres PK-Verschlüsselungsverfahren, welches einzelne Bits $m \in \{0,1\}$ verschlüsselt. Läßt sich die Konstruktion zur Verschlüsselung von Nachrichten $m \in \{0,1\}^*$ beliebiger Länge (siehe Folie 31 für den CPA-Fall) auf den CCA-Fall übertragen?

AUFGABE 3. Einbahnstraße I.
Wir beschäftigen uns mit einigen Details zum Thema Einwefunktionen und -permutationen:

a) Diskutieren Sie, warum es notwendig ist, dem Invertierer $\mathcal{A}$ aus dem Spiel $\mathsf{Invert}_{\mathcal{A},f}(n)$ (siehe Folie 53) zusätzlich zur Eingabe y auch die Eingabe 1^n zu übergeben!

b) Sei $\{0,1\}^* \to \{0,1\}^*$ eine Funktion und sei $y = f(0^n)$. Sei $|f^{-1}(y)| > \mathsf{negl}(n)$, d.h. das Urbild von $f(0^n)$ enthalte mehr als vernachlässigbare viele Elemente. Zeigen Sie, dass f dann keine Einwegfunktion sein kann, indem Sie einen effizienten Invertierer $\mathcal{A}$ für f angeben!

AUFGABE 4. Einbahnstraße II.
Sei $f(x)$ eine Einwegfunktion. Ist dann auch $g(x_1, x_2) := (x_1, f(x_2))$ mit $|x_1| = |x_2|$ eine Einwegfunktion?

AUFGABE 5. Harte Kerne.
Sei $\mathsf{hc} : \{0,1\}^* \to \{0,1\}$ ein Hardcore-Prädikat für eine beliebige Funktion $f : \{0,1\}^* \to \{0,1\}^*$. Zeigen Sie, dass hc *erwartungstreu (auch unbiased)* ist, d.h.

$$\left| \mathbf{Pr}_{x \in_R \{0,1\}^n} [\mathsf{hc}(x) = 0] - \mathbf{Pr}_{x \in_R \{0,1\}^n} [\mathsf{hc}(x) = 1] \right| \leq \mathsf{negl}(n)$$