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

Präsenzübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 3 / 12./14. November 2012

AUFGABE 1:

Sei $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$. Wir definieren die Stromchriffre $\Pi_s = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ wie in der Vorlesung. Zeigen Sie, dass G ein Pseudozufallsgenerator ist, wenn Π_s KPA-sicher ist.

AUFGABE 2:

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein KPA-sicheres, symmetrisches Verschlüsselungsverfahren mit deterministischer Verschlüsselungsfunktion Enc und $\mathcal{M} = \mathcal{C} = \{0,1\}^{\ell(n)}$. Aus der Vorlesung wissen wir, dass Π dann nicht mult-KPA sicher sein kann. Betrachten Sie die folgende randomisierte Variante $\Pi^{\text{rand}} = (\mathsf{Gen}^{\text{rand}}, \mathsf{Enc}^{\text{rand}}, \mathsf{Dec}^{\text{rand}})$ von Π mit

$\mathsf{Gen}^{\text{rand}}(1^n)$: Gibt $k \leftarrow \mathsf{Gen}(1^n)$ zurück.

$\mathsf{Enc}_k^{\text{rand}}(m)$: Wählt bei Eingabe $m \in \{0,1\}^{\ell(n)-2}$ ein $r \in_R \{00, 01, 10, 11\}$ und gibt $c := \mathsf{Enc}_k(m, r)$ (die Nachricht wird mit der Zufallszahl aufgefüllt) zurück.

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

(b) Ist Π^{rand} nun mult-KPA-sicher? Beweisen Sie die Sicherheit oder geben Sie einen Angreifer $\mathcal{A}$ an.

AUFGABE 3:

In dieser Aufgabe wollen wir zeigen, dass die Definitionen von mult-KPA-Sicherheit und CPA-Sicherheit *nicht* äquivalent sind. Zwar folgt aus der CPA-Sicherheit die mult-CPA-Sicherheit und damit die mult-KPA-Sicherheit (siehe Vorlesung), die Rückrichtung gilt allerdings nicht. Um dies zu zeigen, geben wir ein Kryptosystem an, das zwar mult-KPA-sicher ist, aber nicht CPA-sicher.

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein CPA-sicheres Kryptosystem mit Nachrichtenraum $\mathcal{M} = \{0,1\}^n$ (wir werden in den nächsten Wochen sehen, dass solche Kryptosysteme unter bestimmten Annahmen existieren). Wir konstruieren aus Π ein Kryptosystem $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ wie folgt.

$\mathsf{Gen}'(1^n)$: Setze $k \leftarrow \mathsf{Gen}(1^n)$, wähle (eine „trapdoor") $\mathsf{td} \in_R \mathcal{M}$, gebe $k' := (k, \mathsf{td})$ zurück.

$\mathsf{Enc}'_{k'}(m)$: Gebe $c \leftarrow \begin{cases} (\mathsf{Enc}_k(m), \mathsf{td}) & , \text{falls } m \neq \mathsf{td} \\ (\mathsf{Enc}_k(m), k) & , \text{falls } m = \mathsf{td} \end{cases}$ zurück.

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

(b) Zeigen Sie, dass Π' mult-KPA-sicher ist, indem Sie aus einem ppt-Angreifer $\mathcal{A}'$ auf Π' einen ppt-Angreifer $\mathcal{A}$ auf Π konstruieren.

(c) Zeigen Sie, dass Π' *nicht* CPA-sicher ist.