Aufgabe 1.1

Sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Verschlüsselungsschema mit einer Plaintext-Menge $\mathcal{M} = \{0,1\}^\ell$, $\ell \geq 1$.

Nehmen wir an, dieses Verschlüsselungsschema sei „völlig unsicher" in folgendem Sinn: Es gibt einen Algorithmus $\boldsymbol{A}_0$, der zu gegebenem $\mathcal{E}_K(m)$ stets zuverlässig und schnell m ermittelt – und das für beliebige (unbekannte) mit $\mathcal{K}$ erzeugte Schlüssel K und beliebige Plaintexte $m \in \mathcal{M}$.

Beschreiben Sie (auf $\boldsymbol{A}_0$ zurückgreifend) möglichst erfolgreiche Angreifer

a. im LoR-OTCPA-Angriffsspiel,

b. im RoR-OTCPA-Angriffsspiel,

c. im RoR-CPA-Angriffsspiel, wobei der Angreifer das Verschlüsselungsorakel q mal verwendet für irgendeine ganze Zahl $q \geq 1$.

Welcher Vorteil lässt sich jeweils erreichen?

Aufgabe 1.2

Sei g ein Pseudo-Random Generator mit Schlüsselmenge $\mathcal{K}$ und sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ das folgende Verschlüsselungsschema mit Plaintextmenge $\mathcal{M} = \{0,1\}^*$:

- Der Schlüsselgenerierungsalgorithmus $\mathcal{K}$ erzeugt eine Gleichverteilung auf der Menge $\mathcal{K}$.
- Der Verschlüsselungsalgorithmus berechnet $\mathcal{E}_K(m) = g_K(|m|) \oplus m$ (ist also deterministisch).
- Der Entschlüsselungsalgorithmus berechnet $\mathcal{D}_K(c) = g_K(|c|) \oplus c$.

Wir behaupten: Ist der Pseudo-Random Generator sicher, so ist das Verschlüsselungsverfahren sicher im Sinne von RoR-OTCPA.

Zeigen Sie dafür: Ist ein Angreifer $\boldsymbol{A}$ im RoR-OTCPA-Angriffsspiel gegeben, so lässt sich ein Angreifer $\boldsymbol{B}$ im PRG-Angriffsspiel konstruieren, der mit im wesentlichen der gleichen Laufzeit genau den gleichen Vorteil erreicht.

Aufgabe 1.3

Sei $\mathcal{K} = \{0,1\}^k$ (mit einer ganzen Zahl $k \geq 1$) und sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ das folgende Verschlüsselungsschema mit Plaintextmenge $\mathcal{M} = \{0,1\}^k$:

- Der Schlüsselgenerierungsalgorithmus $\mathcal{K}$ erzeugt eine Gleichverteilung auf der Menge $\mathcal{K}$.
- Der Verschlüsselungsalgorithmus berechnet $\mathcal{E}_K(m) = K \oplus m$.
- Der Entschlüsselungsalgorithmus berechnet $\mathcal{D}_K(c) = K \oplus c$.

Zeigen Sie: Dieses Verschlüsselungsschema ist sicher im Sinne von RoR-OTCPA.

Aufgabe 1.4

Zeigen Sie in der Situation von Aufgabe 1.3, dass das dortige Verschlüsselungsschema nicht sicher ist im Sinne von RoR-CPA. (RoR-OTCPA-Sicherheit impliziert also keine RoR-CPA-Sicherheit.)

Beschreiben Sie dafür einen Angreifer, der mindestens den Vorteil 1/2 erreicht.

Aufgabe 1.5

Geben Sie analog zu Folien 2.12 ff. (RoR-OTCPA und LoR-OTCPA) Formeln an, die die folgenden Aussagen ausdrücken:

a. LoR-CPA-Sicherheit impliziert RoR-CPA-Sicherheit.

b. RoR-CPA-Sicherheit impliziert LoR-CPA-Sicherheit.

Was ist die quantitativ stärkere Anforderung: LoR-CPA-Sicherheit oder RoR-CPA-Sicherheit?

(Ansatz: „Sicherheit“ in einem bestimmten Sinn heißt, der Vorteil jedes denkbaren Angreifers liegt unter einer Grenze ϵ. Ist ein Schema denkbar, das nur für einen der Sicherheitsbegriffe an der Grenze scheitert?)

Geänderter Vorlesungstermin: mittwochs **16:00 s. (!) t.** in IC 5/161