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

Hausübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 3 / 05. November 2012

Abgabe: Am 19. November 2012 entweder bis 12 Uhr in den Kasten NA/02 (Kasten wird um 12 Uhr geleert!) oder bis 16.15 Uhr in der Übung, NA 5/99

AUFGABE 1 (5 Punkte)**:**

Wir betrachten die Konstruktion „Stromchiffre" und den zugehörigen Sicherheitsbeweis aus der Vorlesung (siehe Folie 44 ff.), wobei $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator ist. Wir definieren ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter n für Nachrichten der Länge $\ell(n)$ wie folgt.

$\mathsf{Gen}(1^n)$: Wähle $k \in_R \{0,1\}^n$.

$\mathsf{Enc}_k(m)$: Zur Nachricht $m \in \{0,1\}^{\ell(n)}$ berechne $c := m \oplus \overleftarrow{G}(k)$, mit der Konstruktion $\overleftarrow{G}(k) := (G(k)_{\ell(n)}, G(k)_{\ell(n)-1}, \ldots, G(k)_1)$, wobei $G(k)_i$ das i-te Ausgabebit von G bezeichnet. D.h. $\overleftarrow{G}(k)$ ist definiert als die Rückwärtsdarstellung der Ausgabe von $G(k)$.

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

(b) Zeigen Sie die KPA-Sicherheit von Π, indem Sie zeigen dass $G' : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ mit $s \mapsto \overleftarrow{G}(s)$ ebenfalls ein Pseudozufallsgenerator ist. Benutzen Sie dann den Satz „Stromchiffre" (Folie 45) aus der Vorlesung.

(c) Zeigen Sie die KPA-Sicherheit *direkt*, indem Sie den Beweis zur „Stromchiffre" (Folie 45 ff.) immitieren, d.h. aus einem KPA-Angreifer $\mathcal{A}$ auf Π einen Unterscheider $\mathcal{D}$ für G konstruieren.

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein KPA-sicheres, symmetrisches Verschlüsselungsverfahren mit deterministischer Verschlüsselungsfunktion Enc und $\mathcal{M} = \mathcal{C} = \{0,1\}^{\ell(n)}$. Betrachten Sie für ein festes $i \in \mathbb{N}$ folgende randomisierte Variante $\Pi^{\text{rand},i} = (\mathsf{Gen}^{\text{rand}}, \mathsf{Enc}^{\text{rand},i}, \mathsf{Dec}^{\text{rand},i})$ von Π mit

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

$\mathsf{Enc}_k^{\text{rand},i}(m)$: Wählt bei Eingabe $m \in \{0,1\}^{\ell(n)-\log(n^i)}$ ein $r \in_R \{0,1\}^{\log(n^i)}$ 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) Gibt es ein festes (von n unabhängiges) $i \in \mathbb{N}$, so dass $\Pi^{\text{rand},i}$ nun mult-KPA-sicher ist? Beweisen Sie die Sicherheit oder geben Sie (für alle $i \in \mathbb{N}$) einen Angreifer $\mathcal{A}$ an.

AUFGABE 3 (10 Punkte)**:**

In dieser Aufgabe sollen Sie zeigen, dass man aus einem Pseudozufallsgenerator G mit fixer Expansion $\ell(n) = n+1$ einen anderen Pseudozufallsgenerator G'' konstruieren kann, der Expansion $\ell''(n) = n + p(n)$ für ein beliebiges Polynom $p > 0$ besitzt.

Sei $G : \{0,1\}^n \to \{0,1\}^{n+1}$ ein Pseudozufallsgenerator.

(a) Konstruieren Sie zunächst einen Pseudozufallsgenerator $G' : \{0,1\}^n \to \{0,1\}^{n+2}$, d.h. realisieren Sie ein zusätzliches Ausgabebit. Um G' zu konstruieren, wenden Sie G mit einem initialen Seed s an und verwenden Sie den hinteren Teil $t \in \{0,1\}^n$ der Ausgabe $G(s) = \sigma t$ erneut als Eingabe für G.

Beweisen Sie, dass G' ein Pseudozufallsgenerator ist, indem Sie ein „Hybridargument" verwenden. Gehen Sie hierbei wie folgt vor.

(i) Betrachten Sie die folgenden drei hybriden Verteilungen.
- In H^0 wählt man $s \in_R \{0,1\}^n$, gibt $G'(s) := (\sigma, G(t))$ mit $\sigma t := G(s)$ aus.
- In H^1 wählt man $s = (\sigma', s') \in_R \{0,1\}^{n+1}$, gibt $(\sigma', G(s'))$ aus.
- In H^2 wählt man ein komplett zufälliges $s \in_R \{0,1\}^{n+2}$.

Begründen Sie, wieso es reicht für beliebige ppt-Unterscheider $\mathcal{D}'$ zu zeigen, dass

$$\left| \underset{s \leftarrow H^0}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] - \underset{s \leftarrow H^2}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] \right| \leq \mathsf{negl}(n) \tag{1}$$

(ii) Zeigen Sie mit Hilfe der Dreiecksungleichung $\left| \underset{s \leftarrow H^0}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] - \underset{s \leftarrow H^2}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] \right|$
$\leq \left| \underset{s \leftarrow H^0}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] - \underset{s \leftarrow H^1}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] \right| + \left| \underset{s \leftarrow H^1}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] - \underset{s \leftarrow H^2}{\mathsf{Ws}}[\mathcal{D}'(s) = 1] \right|$

(iii) Beweisen Sie Gleichung (1), indem Sie zeigen, dass die benachbarten Hybride H^0, H^1 bzw. H^1, H^2 jeweils ununterscheidbare Verteilungen sind. In beiden Fällen müssen Sie hierzu aus einem Unterscheider $\mathcal{D}'$, der die beiden Hybride unterscheidet, einen Unterscheider $\mathcal{D}$ für G konstruieren.

(b) Skizzieren Sie, wie die Konstruktion verallgemeinert werden kann, d.h. konstruieren Sie $G'' : \{0,1\}^n \to \{0,1\}^{n+p(n)}$ für ein beliebiges Polynom $p > 0$. Wie sehen die allgemeinen Hybride aus, die man in der Reduktion betrachtet?