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

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 3 / 15. November 2010 / Abgabe 29. November, 16 Uhr, Kasten NA 02

AUFGABE 1. Unter Strom. (5 Punkte)
Wir betrachten die Konstruktion „Stromchiffre“ und den zugehörigen Sicherheitsbeweis aus der Vorlesung (siehe Folie 44 ff) mit folgender spezieller Wahl für G. Sei $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator mit Expansionsfaktor $\ell(n) > 2in$ für ein festes $i \in \mathbb{N}$. Wir definieren ein symmetrisches Verschlüsselungsverfahren $\Pi_{s_i} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter 1^n für Nachrichten der Länge $\frac{\ell(n)}{i}$ wie folgt.

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

$\mathsf{Enc}_k(m)$: Zur Nachricht $m = (m_1, \ldots, m_{\frac{\ell(n)}{i}}) \in \{0,1\}^{\frac{\ell(n)}{i}}$ berechne $c = (c_1, \ldots, c_{\frac{\ell(n)}{i}}) \in \{0,1\}^{\frac{\ell(n)}{i}}$ mit

$$c_j := G(k)_{ij} \oplus m_j$$

für $j = 1, \ldots, \frac{\ell(n)}{i}$ wobei $G(k)_{ij}$ das $(i \cdot j)$-te Ausgabebit von $G(k)$ bezeichnet.

$\mathsf{Dec}_k(c)$: Aus $c = (c_1, \ldots, c_{\frac{\ell(n)}{i}}) \in \{0,1\}^{\frac{\ell(n)}{i}}$ berechne $m = (m_1, \ldots, m_{\frac{\ell(n)}{i}}) \in \{0,1\}^{\frac{\ell(n)}{i}}$ mit

$$m_j := G(k)_{ij} \oplus c_j$$

für $j = 1, \ldots, \frac{\ell(n)}{i}$.

Beweisen Sie die KPA-Sicherheit von Π_{s_i} auf zwei verschiedene Arten.

a) Betrachten Sie $G' : \{0,1\}^n \to \{0,1\}^{\frac{\ell(n)}{i}}$ mit $s \mapsto G(s)_{ij}$ für $j = 1, \ldots, , \frac{\ell(n)}{i}$ und zeigen Sie, dass G' ein Pseudozufallsgenerator ist, d.h. konstruieren Sie aus einem Unterscheider $\mathcal{D}'$ für G' einen Unterscheider $\mathcal{D}$ für G. Begründen sie damit die KPA-Sicherheit.

b) Beweisen Sie die KPA-Sicherheit *direkt*, indem Sie den Beweis zur „Stromchiffe “(Folie 45 ff) immitieren, d.h. konstruieren Sie aus einem KPA-Angreifer $\mathcal{A}$ einen Unterscheider $\mathcal{D}$ für G.

AUFGABE 2. Zu wenig Zufall. (5 Punkte)
Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein KPA-sicheres, symmetrisches Verschlüsselungsverfahren mit deterministischer Verschlüsselungsfunktion Enc. Betrachten Sie folgende randomisierte Variante Π^{rand} von Π mit

$$\mathsf{Enc}_k^{\mathsf{rand}}(m) := \mathsf{Enc}_k(r||m)$$

für $r \in \{0,1\}^{\log(n^i)}$ und $m \in \{0,1\}^{n-\log(n^i)}$ mit konstantem $i \in \mathbb{N}$ sowie

$$\mathsf{Dec}_k^{\mathsf{rand}}(c) := (\mathsf{Dec}_k(c)_{\log(n^i)+1}, \ldots, \mathsf{Dec}_k(c)_n)$$

wobei $\mathsf{Dec}(c)_j$ das j-te Bit der Ausgabe von Dec bezeichnet.

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

In der kommenden Aufgabe wollen wir zeigen, wie wir einen Pseudozufallsgenerator G mit fixer Expansion $\ell(n) = n + 1$ in einen anderen Pseudozufallsgenerator G'' mit Expansion $\ell''(n) = p(n)$ für ein beliebiges Polynom $p \geq 0$ transformieren können.

AUFGABE 3. Stretching. (10 Punkte)
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 weiteres zusätzliches Ausgabebit. Beweisen Sie, dass G' ein Pseudozufallsgenerator ist, indem Sie ein „Hybridargument “ verewenden. Gehen Sie hierbei wie folgt vor.

   i) Um G' zu konstruieren, wenden Sie G mit einem initialen Seed s_0 an und verwenden Sie einen Teil s_1 der Ausgabe $G(s_0) = \sigma_1 s_1$ erneut als Eingabe für G.

   ii) Betrachten Sie die folgenden drei hybriden Verteilungen. In H^0 wählt man $s \in_R \{0,1\}^n$ und gibt $G'(s)$ aus; in H^1 wählt man $s = (s_0, \ldots, s_n) \in_R \{0,1\}^{n+1}$ und gibt $(s_0, G(s_1, \ldots, s_n))$ aus; in H^2 gibt man ein komplett zufälliges $s \in \{0,1\}^{n+2}$ aus. Begründen Sie, wieso es reicht, für beliebige ppt-Unterscheider $\mathcal{D}'$ zu zeigen, dass

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

   gilt.

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

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