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

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 4 / 25. und 27. Mai 2011

AUFGABE 1. Random Oracle.
Sei $H : \{0,1\}^{2n} \to \{0,1\}^n$ eine Funktion. Definiere

$$F_k(x) := H(k||x)$$

wobei $|k| = |x| = n$. Zeigen Sie, dass F_k eine Pseudozufallsfunktion ist, wenn H als Random Oracle modelliert ist.

Wir wollen in der Hausübung den Beweis für die Hardcore-Eigenschaft des *Goldreich-Levin* Hardcore-Prädiakts $\mathsf{gl}(x,r) :=< x,r >:= \sum_{i=1}^{n} x_i r_i \bmod 2$ führen, siehe Theorem 1 auf Hausübungsblatt 4.
Hierzu betrachten wir folgende abstrakte Fragestellung. Sei für festes $x \in \{0,1\}^n$ ein Orakel $\mathcal{O}_x : \{0,1\}^n \to \{0,1\}$ gegeben, so dass für ein $\varepsilon > 0$ gilt

$$\mathbf{Pr}_{r \in_R \{0,1\}^n} [\mathcal{O}_x(r) = \mathsf{gl}(x,r)] \geq \frac{1}{2} + \frac{\varepsilon}{2} \ . \tag{1}$$

Wir wollen zunächst zeigen, dass $\mathcal{O}_x$ die Menge $\{0,1\}^n$ in „gute“ und „böse“ r's unterteilt.

AUFGABE 2. Gute Menge.
Für festes $x \in \{0,1\}^n$ sei $\mathsf{Good}(x) := \{r \in \{0,1\}^n : \mathcal{O}_x(r) = \mathsf{gl}(x,r)\}$. Zeigen Sie

$$|\mathsf{Good}(x)| \geq \frac{1+\varepsilon}{2} \cdot 2^n \qquad .$$

Das Herzstück der Reduktion zum obigen Theorem ist der folgende Algorithmus Predict, welcher unter Benutzung von $\mathcal{O}_x$ und zur randomisierten Eingabe $r = (r_1, \ldots, r_m) \in_R \{0,1\}^{n \times m}$ sowie $\sigma = (\sigma_1, \ldots, \sigma_m) \in \{0,1\}^m$ für jedes $z \in \{0,1\}^n$ mit „guter“ Wahrscheinlichkeit $\mathsf{gl}(x,z) =< x,z >$ berechnet.
Der Algorithmus wird aus den r_i neue zufällige Vektoren $r^I = \sum_{i \in I} r_i$ für Indexmengen $\emptyset \neq I \subset \{1, \ldots, m\}$ berechnen und anschliessend das Orakel für $z + r^I$ befragen.

Algorithmus $\textsc{Predict}^{\mathcal{O}_x}$

Input: $z \in \{0,1\}^n$, $r_i \in \{0,1\}^n$ und $\sigma_i \in \{0,1\}$ für $i = 1, \ldots, m$.
Output: $b \in \{0,1\}$
Parameter: m

01 $i \leftarrow 0$
02 **For all** $\emptyset \neq I \subset \{1, \ldots, m\}$ **do**
03 $\quad \sigma^I \leftarrow \sum_{i \in I} \sigma_i$ und $r^I = \sum_{i \in I} r_i$
04 $\quad c^I \leftarrow \mathcal{O}_x(z + r^I) + \sigma^I$
05 $\quad i \leftarrow i + c^I$
06 **End For**
07 **If** $i \geq 2^m/2$ **then** $b \leftarrow 1$ **else** $b \leftarrow 0$
08 Output b

Wir wollen nun zeigen, dass $\textsc{Predict}^{\mathcal{O}_x}$ mit „guter“ Wahrscheinlichkeit $\mathsf{gl}(x, z)$ korrekt berechnet sofern $\sigma_i = \mathsf{gl}(x, r_i)$ für alle $i = 1, \ldots, m$ gilt. In der Hausübung werden wir dann $\textsc{Predict}$ einfach für alle möglichen $\sigma \in_R \{0,1\}^m$ ausführen, bis wir x gefunden haben.

AUFGABE 3. Algorithmenanalyse.
Sei $M = 2^m$ und gelte $\sigma_i = \mathsf{gl}(x, r_i)$ für alle $i = 1, \ldots, m$. Zeigen Sie, dass die Laufzeit von $\textsc{Predict}$ durch $t_{\textsc{Predict}}(n) = \mathcal{O}(M \cdot t_{O_x}(n))$ gegeben ist wobei $t_{\mathcal{O}_x}(n)$ die Laufzeit für eine Orakelantwort bezeichnet. Zeigen Sie außerdem, dass für *jedes* $z \in \{0,1\}^n$

$$\mathbf{Pr}_{r \in_R \{0,1\}^{n \times m}} \left[\textsc{Predict}^{\mathcal{O}_x}(z, r, \sigma) \neq \mathsf{gl}(x, z) \right] \leq \frac{1}{M\varepsilon^2}$$

gilt, wobei $r = (r_1, \ldots, r_m)$ und $\sigma = (\sigma_1, \ldots, \sigma_m)$ ist. Gehen Sie hierbei wie folgt vor.

i) Definieren Sie Zufallsvariablen

$$X^I(r) = \begin{cases} 1 & \text{falls } \mathcal{O}_x(z + r^I) + \sigma^I = \mathsf{gl}(x, z) \\ 0 & \text{sonst} \end{cases}$$

und begründen Sie, wieso die X^I paarweise unabhängig sind. Hierbei ist $X^I : S \to \{0,1\}$ auf der Menge aller m-Tupel $(r_1, \ldots, r_m) \in \{0,1\}^{n \times m}$ definiert, wobei wir S mit der Gleichverteilung versehen.

ii) Berechnen Sie den Erwartungswert $\mathbb{E}\left[X^I\right]$. Hierbei hilft Aufgabe 1.

iii) Definieren Sie $X := \sum X^I$ und wenden Sie die Chebyshev-Ungleichung an, um $\mathbf{Pr}\left[X < M/2\right] \leq \frac{1}{M\varepsilon^2}$ zu zeigen. Hierbei dürfen Sie die Abschätzung $\mathrm{Var}\left[X^I\right] \leq \frac{1}{4}$ für jede $\{0,1\}$-Zufallsvariable X^I benutzen.