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

Präsenzübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 4 / 07. Juni 2013

In dieser Präsenzübung und der zugehörigen Hausübung soll die Hardcoreeigenschaft des Goldreich-Levin Hardcoreprädikats, konkret das folgende Theorem, gezeigt werden.

Theorem 1. *Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Einwegpermutation. Dann ist auch $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ definiert durch $g(x,r) := (f(x),r)$ eine Einwegpermutation. Ferner ist die Funktion $\mathsf{gl}(x,r) := \langle x,r\rangle := \sum_{i=1}^{n} x_i \cdot r_i$ mod 2 ein Hardcoreprädikat für g, d.h. für alle ppt-Angreifer $\mathcal{A}$ gilt*

$$\mathsf{Ws}_{x,r\in_R\{0,1\}^n}[\mathcal{A}(g(x,r)) = \mathsf{gl}(x,r)] \leq \frac{1}{2} + \mathsf{negl}(n).$$

Die Einwegeigenschaft von g wird in der Hausübung gezeigt.

Um die Hardcoreeigenschaft zu zeigen, definieren wir zunächst einen beliebigen ppt-Angreifer $\mathcal{A}$ mit polynomieller Laufzeit $t_{\mathcal{A}}(n)$ und

$$\mathsf{Ws}_{x,r\in_R\{0,1\}^n}[\mathcal{A}(g(x,r)) = \mathsf{gl}(x,r)] = \frac{1}{2} + \varepsilon(n).$$

In der Präsenzübung zeigen wir nun, dass es eine Menge von „guten" $x \in \{0,1\}^n$ gibt, für die der Angreifer $\mathcal{A}$ mit konstantem x mehrfach angefragt werden kann. Anschließend geben wir einen Algorithmus $\mathcal{B}$ an, mit dem wir mit guter Wahrscheinlichkeit das Hardcoreprädikat für *frei wählbare* $r = z \in \{0,1\}^n$ bestimmen können. In der Hausübung können wir dann schließlich einen Algorithmus $\mathcal{C}$ angeben, der mit Hilfe von $\mathcal{B}$ die Einwegeigenschaft von g verletzt, d.h. zu gegebenem $f(x)$ das x bestimmt.

AUFGABE 1:

Sei

$$\mathsf{Good}_n := \left\{ x \in \{0,1\}^n \;\middle|\; \mathsf{Ws}_{r\in_R\{0,1\}^n}[\mathcal{A}(g(x,r)) = \mathsf{gl}(x,r)] \geq \frac{1}{2} + \frac{1}{2}\cdot\varepsilon(n) \right\} \subseteq \{0,1\}^n.$$

Zeigen Sie: $\mathsf{Ws}_{x\in_R\{0,1\}^n}[x \in \mathsf{Good}_n] \geq \frac{1}{2}\cdot\varepsilon(n)$.

Bitte wenden!

Das Herzstück der Reduktion zum obigen Theorem ist der folgende Algorithmus $\mathcal{B}$, welcher unter Benutzung von $\mathcal{A}$ zur randomisierten Eingabe $s = (s_1, \ldots, s_m) \in_R \{0,1\}^{n \times m}$, für „korrektes" $h = (h_1, \ldots, h_m) \in \{0,1\}^m$ und beliebiges $z \in \{0,1\}^n$ mit „guter" Wahrscheinlichkeit das Hardcorebit $\mathsf{gl}(x, z)$ berechnet. Die Idee ist es, diesen Algorithmus für jedes $h \in \{0,1\}^m$ laufen zu lassen, bis man das „richtige" (s.u.) gefunden hat. Damit der Algorithmus polynomiell in n bleibt, wählen wir später m in der Größenordnung $\log(n)$.

1: **procedure** $\mathcal{B}(f(x), z, s, h, m)$
2: $\quad \mathsf{count} \leftarrow 0$ ▷ Zählt die Anzahl der $\mathsf{tmpbit}s$, die 1 sind
3: $\quad$ **for all** $\{\} \neq I \subset \{1, \ldots, m\}$ **do** ▷ Alle Teilmengen, bis auf die leere Menge
4: $\quad\quad S_I \leftarrow \sum_{i \in I} s_i$ ▷ $S_I \in \{0,1\}^n$ ist ein Zufallswert, Addition im $\mathbb{F}_2^n$ (xor)
5: $\quad\quad H_I \leftarrow \sum_{i \in I} h_i$ ▷ $H_I \in \{0,1\}$ ist das zugehörige (geratene) Hardcorebit
6: $\quad\quad \mathsf{tmpbit} \leftarrow H_I + \mathcal{A}(f(x), S_I + z)$
7: $\quad\quad \mathsf{count} \leftarrow \mathsf{count} + \mathsf{tmpbit}$
8: $\quad$ **end for**
9: $\quad$ **if** $\mathsf{count} \geq 2^m/2$ **then**
10: $\quad\quad \mathsf{bit} \leftarrow 1$
11: $\quad$ **else**
12: $\quad\quad \mathsf{bit} \leftarrow 0$
13: $\quad$ **end if**
14: $\quad$ **return** bit ▷ Das Rückgabebit wird per Mehrheitsvotum bestimmt
15: **end procedure**

AUFGABE 2:

Sei $m \in \mathbb{N}$, $x \in_R \{0,1\}^n$, $s = (s_1, \ldots, s_m) \in_R \{0,1\}^{n \times m}$, $h_i = \mathsf{gl}(x, s_i)$ die zugehörigen (geratenen) Hardcorebits, $z \in \{0,1\}^n$ beliebig und $\mathcal{A}$ wie oben definiert. Zeigen Sie:

(a) Die Laufzeit von $\mathcal{B}$ ist $t_{\mathcal{B}}(n) := \mathcal{O}(2^m \cdot (t_{\mathcal{A}}(n) + n))$.

(b) Die Fehlerwahrscheinlichkeit unter der Bedingung, dass x „gut" ist, ist

$$\mathsf{Ws}_{x \in_R \{0,1\}^n, s \in_R \{0,1\}^{n \times m}}[\mathcal{B}(f(x), z, s, h, m) \neq \mathsf{gl}(x, z) \mid x \in \mathsf{Good}_n] \leq \frac{1}{2^m \cdot \varepsilon(n)^2}.$$

AUFGABE 3:

Sei $N = p \cdot q$ für prime, ungerade $p \neq q$. Zur Erinnerung:

$$\mathcal{J}_N^{+1} := \{x \in \mathbb{Z}_N^* \mid \left(\frac{x}{N}\right) = +1\}$$

ist die Menge aller x mit Jacobi-Symbol $+1$,

$$\mathcal{QR}_N := \{x \in \mathbb{Z}_N^* \mid \exists\, y \in \mathbb{Z}_N^* \text{ mit } x = y^2 \bmod N\}$$

die Menge aller quadratischen Reste, $\mathcal{QNR}_N := \mathbb{Z}_N^* \setminus \mathcal{QR}_N$ die Menge aller quadratischen Nichtreste und $\mathcal{QNR}_N^{+1} := \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$ die Menge aller quadratischen Nichtreste mit Jacobi-Symbol $+1$. Zeigen Sie:

(a) $|\mathcal{J}_N^{+1}| = \frac{1}{2} \cdot |\mathbb{Z}_N^*|$

(b) $\mathcal{QR}_N \subset \mathcal{J}_N^{+1}$

(c) $|\mathcal{QR}_N| = \frac{1}{2} \cdot |\mathcal{J}_N^{+1}|$