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

Hausübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 4 /
Abgabe: 14. Juni 2013, 10 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

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.

AUFGABE 2 (10 Punkte)**:**

Wir untersuchen nun den folgenden Algorithmus $\mathcal{C}$, welcher mit Hilfe von $\mathcal{B}$ aus der Präsenzübung zu gegebenem $f(x)$ das x berechnet.

```
1:  procedure C(f(x), m)
2:      Wähle s_1, ..., s_m ∈_R {0,1}^n und setze s = (s_1, ..., s_m).   ▷ Eingabe für B
3:      for all h ∈ {0,1}^m do          ▷ Teste alle Hardcorebits, bis richtige gefunden
4:          for k = 1 to n do
5:              x̃_k ← B(f(x), e_k, s, h, m)          ▷ e_k ist der k-te Einheitsvektor
6:          end for
7:          x̃ ← (x̃_1, ..., x̃_n)
8:          if f(x̃) = f(x) then
9:              return x̃                              ▷ Falls x gefunden, gib es zurück
10:         end if
11:     end for
12:     return ⊥        ▷ Sonst gib nach Durchtesten aller h's ein Fehlersymbol zurück
13: end procedure
```

Bitte wenden!

(a) Zeigen Sie, dass $t_{\mathcal{C}}(n) := \mathcal{O}(2^{2m} \cdot n \cdot (t_{\mathcal{A}}(n) + n))$ die Laufzeit von $\mathcal{C}$ ist.

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

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

Hinweis: Verwenden Sie die „Union Bound" und die aus der Präsenzübung bekannte Fehlerwahrscheinlichkeit von $\mathcal{B}$.

(c) Geben Sie ein $m \in \mathbb{N}$ an, so dass $\mathsf{Ws}_{x \in_R \{0,1\}^n}[\mathcal{C}(f(x), m) = x \mid x \in \mathsf{Good}_n] \geq \frac{1}{2}$ ist. Zeigen Sie, dass für Ihre Wahl von m die Laufzeit $t_{\mathcal{C}}(n)$ von $\mathcal{C}$ polynomiell in n, der Laufzeit $t_{\mathcal{A}}(n)$ von $\mathcal{A}$ und $\varepsilon(n)^{-1}$ ist.

(d) Bestimmen Sie $\mathsf{Ws}_{x \in_R \{0,1\}^n}[\mathcal{C}(f(x), m) = x]$ mit Hilfe der Präsenzaufgabe 4.1. Zeigen Sie nun Theorem 1, indem Sie aus jedem ppt-Angreifer $\mathcal{A}$ mit Laufzeit $t_{\mathcal{A}}(n) := q(n)$ und $\varepsilon(n) := 1/p(n)$ für Polynome $p(n)$ und $q(n)$ einen ppt-Angreifer $\mathcal{C}$ konstruieren, der mit nicht-vernachlässigbarer Wahrscheinlichkeit $1/p'(n)$ für ein Polynom $p'(n)$ zu gegebenem $f(x)$ das x bestimmt und damit die Einwegeigenschaft von f verletzt.

Geben Sie dazu die konkrete Erfolgswahrscheinlichkeit von $\mathcal{C}$ an und zeigen Sie, dass die Laufzeit $t_{\mathcal{C}}(n)$ von $\mathcal{C}$ polynomiell in n ist.

AUFGABE 3 (5 Punkte)**:**

Betrachten Sie folgende modifizierte Version der *quadratischen Residuositätsannahme* (vgl. Folie 88), in welcher der Unterscheider $y \in_R \mathcal{QNR}_N$ anstelle von $y \in_R \mathcal{QNR}_N^{+1}$ erhält.

Das Unterscheiden quadratischer Reste ist hart bzgl. $\mathsf{GenModulus}(1^n)$*, falls für alle ppt-Unterscheider* $\mathcal{D}$ *gilt*

$$|\mathsf{Ws}_{x \in_R \mathcal{QR}_N}[\mathcal{D}(1^n, N, x) = 1] - \mathsf{Ws}_{y \in_R \mathcal{QNR}_N}[\mathcal{D}(1^n, N, y) = 1]| \leq \mathsf{negl}(n).$$

Zeigen Sie, dass die modifizierte Annahme nie gelten kann, indem Sie einen Unterscheider $\mathcal{D}$ konstruieren, der die beiden Verteilungen mit Wahrscheinlichkeit $\geq 2/3$ unterscheidet.