Privatdozent Dr. C. Diem
diem@math.uni-leipzig.de
http://www.math.uni-leipzig.de/∼diem/krypto

KRYPTOGRAPHIE
ÜBUNGSBLATT NR. 6

Wir betrachten im Folgenden – wie in der Vorlesung – Scharen von Funktionen $(f_{k^{(0)}})_{k^{(0)} \in \{0,1\}^*}$, mit dieser Eigenschaft: Für $n = |k^{(0)}|$ ist $f_{k^{(0)}} : \{0,1\}^n \longrightarrow \{0,1\}^n$.
Für festes n und k uniform in $\{0,1\}^n$ haben wir dann die zufällige Funktion f_k.
Daneben betrachten wir auch (wie in der Vorlesung) längenerhaltende uniform zufällige ("echt zufällige") Zufallsfunktionen, d.h. uniform zufällige Funktionen $\{0,1\}^n \longrightarrow \{0,1\}^n$. Ferner betrachten wir uniform zufällige ("echt zufällige") Zufallspermutationen $\{0,1\}^n \longrightarrow \{0,1\}^n$. Für asymptotische Analysen können wir hier wieder n variieren.
In der Vorlesung haben wir für Scharen wie oben definiert, was eine Pseudozufallsfunktion und eine Pseudozufallspermuation sei.

Aufgabe 1 In dieser Aufgabe vergleichen wir uniform zufällige längenerhaltende Funktionen und Zufallspermutationen – wie immer vom asymptotischen Gesichtspunkt aus.

a) Überlegen Sie sich, was in diesem Kontext ein Unterscheider sein soll.

b) Zeigen Sie: Man kann längenerhaltende uniforme Zufallsfunktionen nicht effizient von uniformen Zufallspermutationen unterscheiden.

c) Zeigen Sie: Eine Pseudozufallspermutation ist auch eine Pseudozufallsfunktion.

Bemerkung zu a. Der gesuchte Unterscheider ist vollkommen analog zum Unterscheider in der Vorlesung.
Bemerkung zu b. Das "nicht effizent" ist eine Kurzform für "Es gibt keinen PPT-Unterscheider mit nicht-vernachlässigbarem Erfolg".

Definition. Eine starke Pseudozufallspermutation ist eine Pseudozufallspermutation $(f_{k^{(0)}})_{k^{(0)}}$, für die auch die Schar $(f^{-1}_{k^{(0)}})_{k^{(0)}}$ eine Pseudozufallspermutation ist. (Dies fungiert als theoretisches Modell für Blockchiffren.)

Aufgabe 2 Wir betrachten das folgende Verschlüsselungsverfahren aus der Vorlesung für eine starke Pseudozufallspermutation $(f_{k^{(0)}})_{k^{(0)}}$:

- $\mathcal{G}en$. Unter Eingabe 1^n, gib $k \in \{0,1\}^n$ uniform aus.
- $\mathcal{E}nc$. Unter Eingabe eines Schlüssels k und der Nachricht m (mit $|k| = |m|$), gib
$$c := f_k(m)$$
aus.
- $\mathcal{D}ec$. Unter Eingabe eines Schlüssels k und eines Chiffriertexts c (mit $|k| = |c|$), gib
$$m := f_k^{-1}(c)$$
aus.

Ist dieses Verfahren stets IND-EAV-sicher?

Aufgabe 3 Wir betrachten das folgende Verschlüsselungsverfahren für eine starke Pseudozufallspermutation:

- $\mathcal{G}en$. Unter Eingabe 1^n, gib $k \in \{0,1\}^n$ uniform aus.
- $\mathcal{E}nc$. Unter Eingabe eines Schlüssels k und der Nachricht m (mit $|k| = |m|$), wähle $r \in \{0,1\}^n$ uniform und gib

  $$c := (r, f_k(r \oplus m))$$

  aus.
- $\mathcal{D}ec$. Unter Eingabe eines Schlüssels k und eines Chiffriertexts $c := (r, a)$ (mit $|k| = |r| = |a|$), gib

  $$m := f_k^{-1}(a) \oplus m$$

  aus.

Zeigen Sie, dass das Verfahren IND-CPA-sicher ist.
Hinweis. Schauen Sie sich den Beweis aus der Vorlesung für das Verfahren dort an. Gegen Sie entsprechend vor. Zeigen sie die Aussage also auch zuerst im Zufallsorakelmodell und verglichen Sie dann den Erfolg dort und den Erfolg im "echten Spiel".

Bemerkung. Das Verfahren entspricht der Verschlüsselung des ersten Blocks im Cipher-Block-Chaining-(CBC)-Modus.