

5. Übungsblatt
Kryptographie I (SS 2006)

Stefan Lucks, Emin Islam Tatlı

Besprechung: Mittwoch, 31. Mai 2006

Aufgabe 1 In der Vorlesung wurden Pseudozufallsfunktionen (PZF) und die entsprechenden Generatoren eingeführt. Ein Pseudozufallspermutationsgenerator (PZPG) ist eine Familie von Paaren (p, p^{-1}) effizient berechenbarer Funktionen

$$p, p^{-1} : \{0, 1\}^k \times \{0, 1\}^{m(k)} \rightarrow \{0, 1\}^{m(k)}$$

mit polynomiell beschränkten $m(k)$, wobei für jedes $K \in \{0, 1\}^k$ und jedes $x \in \{0, 1\}^{m(k)}$ gilt:

$$p^{-1}(K, p(K, x)) = x.$$

Eine Pseudozufallspermutation (PZP) ist ein Mitglied dieser Familie mit einem fest gewählten Parameter K , d.h.

$$p(K, \cdot), p^{-1}(K, \cdot) : \{0, 1\}^{m(k)} \rightarrow \{0, 1\}^{m(k)}.$$

Die Definition eines Chosen Plaintext (C.P.) Angreifers ist analog.

Beantworte nun die folgenden Fragen dazu:

- a) Wie viele Funktionen $f : \{0, 1\}^m \rightarrow \{0, 1\}^m$ gibt es, wenn
 - f eine beliebige Funktion sein darf?
 - f eine beliebige Permutation sein darf?
- b) Wie viele Funktionen kann ein Generator $f_k : \{0, 1\}^k \times \{0, 1\}^m \rightarrow \{0, 1\}^m$ höchstens enthalten, wenn
 - f_k ein Pseudozufallsfunktionsgenerator (PZFG) sein soll?
 - f_k ein Pseudozufallspermutationsgenerator (PZPG) sein soll?

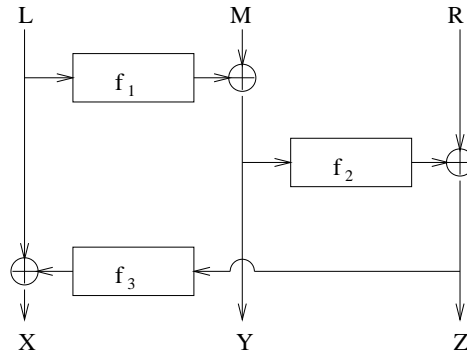
Wie groß ist also die Wahrscheinlichkeit, dass eine zufällig gewählte Funktion bzw. Permutation f in einem gegebenen PZFG bzw. PZPG f_k enthalten ist?

- c) Gegeben sei eine Funktion $f : \{0, 1\}^m \rightarrow \{0, 1\}^m$. Gib einen C.P.-Angreifer an, der zwischen einer Zufallsfunktion (ZF) und einer Zufallspermutation (ZP) mit signifikanter Wahrscheinlichkeit (d.h., $> 1/2$) unterscheiden kann. Kannst du den Vorteil

$$|\Pr(A(f) = 0 | f \text{ ist ZF}) - \Pr(A(f) = 0 | f \text{ ist ZP})|$$

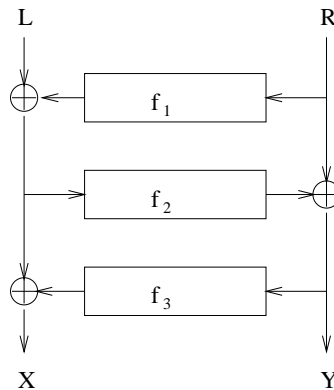
abschätzen, wenn der Angreifer q Anfragen an die Funktion stellen darf?

Aufgabe 2 Betrachte den Generator $G : \{0, 1\}^{3m} \rightarrow \{0, 1\}^{3m}$, dessen Funktionsweise in der nachfolgenden Abbildung dargestellt wird:



- Zeige, dass es sich bei G um eine Permutation handelt.
- Finde einen effizienten Angreifer gegen diesen Generator. Gib auch die Zahl der benötigten Chosen Plaintexte und den erzielten Vorteil an.

Aufgabe 3 In der Vorlesung wird der Generator $P_3 : \{0, 1\}^{2m} \rightarrow \{0, 1\}^{2m}$ eingeführt werden, welcher in der folgenden Abbildung dargestellt ist:



Dabei sind $f_i := \{0, 1\}^m \rightarrow \{0, 1\}^m$ Boolesche Funktionen.

Finde einen effizienten C.P.-Angreifer gegen diesen Generator, falls

- a) zwei Blöcke $R, R' \in \{0, 1\}^m$ bekannt sind mit $f_1(R) = f_1(R')$.
- b) die Funktion f_2 die Komplement-Eigenschaft $f_2(x) = \overline{f_2(\bar{x})}$ hat. Dabei bezeichnet \bar{a} das bitweise Inverse von a , also z.B. $\overline{01101} = 10010$.

Gib auch die Zahl der Chosen Plaintexte an, die dein Angreifer benötigt, sowie den Vorteil, den er erzielt.

Aufgabe 4 Auf der Internetseite

<http://th.informatik.uni-mannheim.de/teach/Krypto-06/uebungen/Interaktiv1/>

findet ihr die interaktive Aufgabe.