André Bajorat
Rasmus Diederichsen
Lisa Goerke

Sebastian Höffner
Kristin Schmidt

# Lösungen zu Übungsblatt 4
# Kryptographische Verfahren

Besprechung 27. November 2015

## Aufgabe 4.1. Zufallsgeneratoren

### a)

Sei G ein PZFG mit $|G(s)| > 4|s| = 4n$. Definiere $G' \coloneqq G(s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor})$. Nach Voraussetzungen ist $G'$ PZFG. Da $|G'| > 2|s|$, gilt

$$H(s) = G'(0^{|s|}\|s) = G(0^{|s|})$$

Also berechnet $H$ für alle $s$ den selben Wert und ist damit leicht von echtem Zufall unterscheidbar. Ein Distinguisher $\mathcal{D}$ muss nur für gegebenes $s$ den Wert $G(0^{|s|})$ berechnen und prüfen, ob $H(s) = G(0^{|s|})$. Daher ist $P(\mathcal{D}(G(s)) = 1) = 1$, während die Situation, dass ein zufälliger Bistring $r$ gerade $r = G(0^{|s|})$ ist, nur eine von $2^{|s|}$ Möglichkeiten ist, $r$ zu wählen, mithin $P(\mathcal{D}(r) = 1) = \frac{1}{2^{|s|}}$. Die Wahrscheinlichkeiten unterscheiden sich also nicht-vernachlässigbar.