André Bajorat
Rasmus Diederichsen
Lisa Goerke

Sebastian Höffner
Kristin Schmidt

Lösungen zu Übungsblatt 4
Kryptographische Verfahren

Besprechung 27. November 2015

Aufgabe 4.1. Zufallsgeneratoren

Meines Erachtens macht es keinen Sinn, nach einem generellen Beweis zu fragen, dass L und H keine PZG sind. Eher sollte es darum gehen, dass sie nicht *notwendigerweise* PZG sind, wenn G und G' PZG sind, denn dies könnte von der Wahl von G und G' abhängen. Diese Interpretation der Aufgabe wird hier angenommen (so wie z.B. Aufgabe 3.6 aus Katz & Lindell).

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

a)

Da $|G'| > 2n$, gilt

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

Also berechnet H für alle s der Länge n den selben Wert und ist damit leicht von echtem Zufall unterscheidbar. Ein Distinguisher $\mathcal{D}$ muss nur für gegebenes $|s|$ (die Länge des Seeds dürfte bekannt sein, oder er probiert alle n Längen durch, was polynomiell in n wäre) 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.

b)

Da $|G'| > 2n$, nehmen wir an

$$\begin{aligned} L(s) &= G'(s) \parallel G'(s+1) \\ &= G(s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor}) \parallel G'(s+1) \\ &= G(s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor}) \parallel G(s') \\ &= G(s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor}) \parallel G(s'_1, \ldots, s'_{\lfloor \frac{n}{2} \rfloor}) \end{aligned}$$

Sei $D(K)$ ein Distinguisher mit

$$D(K) = \begin{cases} 1, \text{falls } k_1, \ldots, k_{\frac{n}{2}} = k_{\frac{n}{2}+1}, \ldots, k_n \\ 0 \text{ sonst} \end{cases}$$

$|K|$ muss für Strings, die durch L generiert wurden, gerade sein, da es eine Konkatenation zweier gleich langer Strings ist. Strings ungerader Länge können sofort als echt zufällig identifiziert werden und sind daher uninteressant.

Addiert man 1 zu s, so ist die Wahrscheinlichkeit, dass sich ein Bit in der vorderen Hälfte ändert die Wahrscheinlichkeit, dass alle Bits der unteren Hälfte 1 sind. Damit D 0 zurück gibt auf einem von L

generierten String, muss genau der Fall eintreten, da die untere Hälfte jeweils abgeschnitten und ignoriert wurde.

$$P(\text{Bit } i \text{ geflippt mit } i > \frac{n}{2}) = \frac{1}{2^{\frac{n}{2}}},$$

denn die unteren $\frac{n}{2}$ Bits müssen 1 sein. Daher ist

$$P(D(G(s)) = 1) = 1 - P(D(G(s)) = 0) = 1 - \frac{1}{2^{\frac{n}{2}}}$$

Die Wahrscheinlichkeit, dass bei einem gleichverteilten Bitstring r die obere und untere Hälfte übereinstimmen (was zu einer Fehleinschätzung von $D(r)$ führen würde), lässt sich als Quotient der Anzahl von Strings, deren Hälften gleich sind und der Anzahl aller Strings berechnen. Für eine Hälfte gibt es $2^{\frac{n}{2}}$ Möglichkeiten und daher genauso viele Strings mit gleichen Hälften, gegenüber 2^n Strings insgesamt.

$$P(D(r) = 1) = \frac{2^{\frac{n}{2}}}{2^n} = 2^{-\frac{n}{2}} = \frac{1}{2^{\frac{n}{2}}}$$

Es gilt also

$$|P(D(G(s)) = 1) - P(D(r) = 1)| = |1 - \frac{1}{2^{\frac{n}{2}}} - \frac{1}{2^{\frac{n}{2}}}| = 1 - \frac{2}{2^{\frac{n}{2}}} = 1 - \frac{1}{2^{\frac{n}{2}-1}}$$

Dies ist nicht vernachlässigbar und wird insbesondere größer für wachsendes n. L ist also nicht notwendigerweise ein PZG.

Aufgabe 4.2. Beweis des Satzes von Goldbach-Levin (erster Teil)

Put up your damn slides, man.

Aufgabe 4.3. Einwegfunktionen?

Angenommen, g wäre keine Einwegfunktion und man könnte g^{-1} effizient berechnen. Dann gälte

$$\begin{aligned} g^{-1}(g(x)) &= x \\ g^{-1}(f(f(x))) &= x \\ g^{-1}(y) &= f^{-1}(f^{-1}(y)) \end{aligned}$$

g^{-1} revidiert also zwei Anwendungen von f. Dann ist aber auch für $y = f(x)$

$$\begin{aligned} g^{-1}(f(y)) &= f^{-1}(f^{-1}(f(y))) \\ &= f^{-1}(y) \end{aligned}$$

Und die Umkehrfunktion $f^{-1(y)}$ ist effizient als $g^{-1}(f(y))$ berechenbar, was ein Widerspruch ist, denn f ist Einwegfunktion.