Heads and tails, summer 2015

PROF. DR. JOACHIM VON ZUR GATHEN AND DR. DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Saturday, 02 May 2015, 23:59:59

Exercise 3.1 (Probabilities). (6 points)

Consider the following generator $g\colon \mathbb{B}^3 \to \mathbb{B}^5$ and let $(X_1, \ldots, X_5) := g(U_3)$.

x	$g(x)$
000	11100
001	00101
010	01011
011	10101

x	$g(x)$
100	00110
101	11110
110	01010
111	01101

(i) Compute the distribution of the projection on the second to fourth bit, thus of (X_2, X_3, X_4). [3]

(ii) Compute a table of the probabilities $\mathrm{prob}(b \xleftarrow{\$} X_4(y))$ for all possible initial sections $y \in \mathbb{B}^3$ and all $b \in \mathbb{B}$. [3]

Exercise 3.2 (Distinguishers and predictors). (8+1 points)

We consider $f : \mathbb{B}^3 \to \mathbb{B}^6$ from the lecture, and a circuit $\mathcal{P}$ with the following specification. It takes as input $y \in \mathbb{B}^4$ and returns a random bit if $w(y) = 2$, and otherwise $\mathrm{minority}(y)$.

(i) Determine a Boolean circuit with which $\mathcal{P}$ can be implemented. [2]

(ii) Determine the prediction power of $\mathcal{P}$ as predictor for the fifth bit of $f(U_3)$. [+1]

(iii) Describe the resulting distinguisher between $f(U_3)$ and U_6, and determine its distinguishing power. [2] [2]

(iv) Compare to the predictors and distinguishers presented in the lecture. [2]

Exercise 3.3 (Distinguishers and predictors). (10 points)

We are given the following generator $g\colon \mathbb{B}^3 \to \mathbb{B}^6$:

x	$g(x)$
000	001100
001	001110
010	010101
011	011011
100	101000
101	100101
110	110010
111	110011

The algorithm $\mathcal{A}$ answers 1 if and only if at most four bits are 1, and 0 otherwise. The algorithm $\mathcal{P}$ returns the second bit.

3 (i) Show: $\mathcal{A}$ is a $\frac{7}{64}$-distinguisher between the output distribution $X = g(U_3)$ of the generator and the uniform distribution U_6 on 6 bits.

3 (ii) Show: $\mathcal{P}$ is a $\frac{1}{4}$-predictor for the sixth bit under X.

4 (iii) Find a predictor of higher quality and compute its prediction power.