The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

3. Assignment

(Due: Thursday, 26 April 2012, 13^{00})

Exercise 3.1 (Simple distinguisher)**.** Suppose that n is even and X is a random variable that takes only values with exactly $n/2$ ones, and each value with the same probability: if $x \in \mathbb{B}^n$ and $\text{Prob}\{x \xleftarrow{\text{R}} X\} > 0$, then $w(x) = \frac{n}{2}$. Here $w(x)$ is the Hamming weight of x, that is, the number of ones in x. Then the following deterministic algorithm $\mathcal{A}$ distinguishes between X and the uniform variable U_n on $\mathbb{B}^n$: on input x, return 1 if $w(x) = n/2$ else return 0.

(i) (2 points) Compute $\mathcal{E}(\mathcal{A}(X))$.

(ii) (4 points) For the uniform distribution U_n on n bits, derive an explicit formula for $\mathcal{E}\{\mathcal{A}(U_n)\}$.

(iii) (2 points) Compute the distinguishing power of $\mathcal{A}$ between U_n and X for $n = 2, 10, 100$.

Exercise 3.2 (Predictors)**.** (5 points) Consider the linear congruent generator which is given by $x_i = sx_{i-1} + 1$ in $\mathbb{Z}_m$. Let $m = qs + 1$ be with s odd and q even integers. Let $z_i = x_i \bmod 2$ be the least significant bit of x_i.

(i) Prove that $B_i(z) = 1 - z_{i-1}$ is an ε-predictor for z_i with success rate

$$\frac{1}{2} + \varepsilon = \frac{q(s+1)}{2m}.$$

(ii) Approximate the prediction power ε for $q \gg s$.

Exercise 3.3 (Distinguishers and predictors)**.** We are given the following generator $g\colon \mathbb{B}^3 \to \mathbb{B}^6$:

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

(i) (3 points) 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.

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

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

(iv) (3 points) Construct from $\mathcal{P}$ a distinguisher $\mathcal{A}'$ between X and U_6. What is its distinguishing power?

(v) (3 points) We want to visualize the hybrid distributions Y_2, Y_4, Y_6 as in the proof of Yao's theorem presented in class. To do this identify the generated bit strings from $\mathbb{B}^6$ with integers in $\{0, \ldots, 63\}$ and determine the probabilities of each string. Draw histograms of the three distributions. (You may do this by hand or use some small program.)

(vi) (3 points) Construct from $\mathcal{A}$ a predictor $\mathcal{P}'$ for g with prediction power at least $7/(6 \cdot 64)$. Hint: Use the construction of Yao's theorem.

(vii) (3 points) Compute the actual prediction power of $\mathcal{P}'$.