The art of cryptography: Heads and tails – Cryptographic random generation summer 2015

Predictors

Prof. Dr. Joachim von zur Gathen
Dr. Daniel Loebenberger

Definition 1. *Let $1 \leq i \leq n$ be integers.*

i. *A predictor for the ith bit is a probabilistic algorithm with inputs from $\mathbb{B}^{i-1}$ and output in $\mathbb{B}$.*

ii. *Let X be a random variable on $\mathbb{B}^n$, $(X_1, \ldots, X_{i-1})$ the corresponding truncated variable on $\mathbb{B}^{i-1}$, and $\mathcal{P}$ a predictor for the ith bit. Then the success rate $\rho_{\mathcal{P}}(X)$ of $\mathcal{P}$ on X is*

$$\rho_{\mathcal{P}}(X) = \sum_{y \in \mathbb{B}^{i-1}} p(y, *) \cdot \mathrm{prob}\{\mathcal{P}(y) \xleftarrow{\text{🎲}} X_i(y)\}.$$

Its advantage (or prediction power) is $\mathrm{Adv}_{\mathcal{P}}(X) = \rho_{\mathcal{P}}(X) - 1/2$. If $\mathrm{Adv}_{\mathcal{P}}(X) \geq \varepsilon$, then $\mathcal{P}$ is an ε-predictor for X.

iii. *A family $(X_k)_{k \in \mathbb{N}}$ of random variables X_k on $\mathbb{B}^{n(k)}$ is (computationally) unpredictable if for any function i_k with $i_k \leq n(k)$, any probabilistic polynomial-time predictor for the i_kth bit of X_k has negligible advantage. Here, the predictor is an algorithm which takes as input k (encoded in unary) and $y \in \mathbb{B}^{i_k - 1}$.*

Recall the generator

$$f : \mathbb{B}^3 \longrightarrow \mathbb{B}^6$$

given by the following table

x	$f(x)$
000	001101
001	001011
010	011010
011	010110
100	101100
101	100101
110	110100
111	110010

We take $X = f(U_3)$ on $\mathbb{B}^6$. Since 0 and 1 occur equally often in each $f(x)$, we consider the "minority bit predictor" $\mathcal{M}_i$ for the ith bit. We now compute its quality as a predictor for the fourth bit:

$$\rho_{\mathcal{M}_4}(X) = \sum_{y \in \mathbb{B}^3} p(y, *) \cdot \mathrm{prob}\{\mathcal{M}_4(y) \xleftarrow{\text{🎲}} X_4(y)\}.$$

We only have six $y \in \mathbb{B}^3$ with $p(y, *) > 0$.

y	$p(y,*)$	$X_4(y)$	$\mathcal{M}_4(y)$	$\mathrm{prob}\{\mathcal{M}_4(y) \xleftarrow{\text{🎲}} X_4(y)\}$
001	$1/4$	$0, 1$	1	$1/2$
011	$1/8$	0	0	1
010	$1/8$	1	1	1
101	$1/8$	1	0	0
100	$1/8$	1	1	1
110	$1/4$	$0, 1$	0	$1/2$

Therefore the success rate is

$$\frac{1}{4} \cdot \frac{1}{2} + \frac{1}{8} \cdot 1 + \frac{1}{8} \cdot 1 + \frac{1}{8} \cdot 0 + \frac{1}{8} \cdot 1 + \frac{1}{4} \cdot \frac{1}{2} = \frac{5}{8} > \frac{1}{2}.$$

ALGORITHM. Distinguisher $\mathcal{A}$ from predictor $\mathcal{P}$.

Input: $y \in \mathbb{B}^n$, and i and $\mathcal{P}$ as above.
Output: 0 or 1.

1. Compute $z \leftarrow \mathcal{P}(y_1, \ldots, y_{i-1})$.
2. Return $\neg(z \oplus y_i)$.

THEOREM 2. *If $\mathcal{P}$ is an (ε, s)-predictor for the ith bit under X, then $\mathcal{A}$ is an $(\varepsilon, s+1)$-distinguisher between X and U_n.*

THEOREM 3. *Let X be a random variable on $\mathbb{B}^n$, and $\mathcal{A}$ an (ε, s)-distinguisher between U_n and X. Then there exists an i with $1 \leq i \leq n$ and an $(\varepsilon/n, s+2)$-predictor for the ith bit under X.*

ALGORITHM 4. Predictor $\mathcal{P}$.

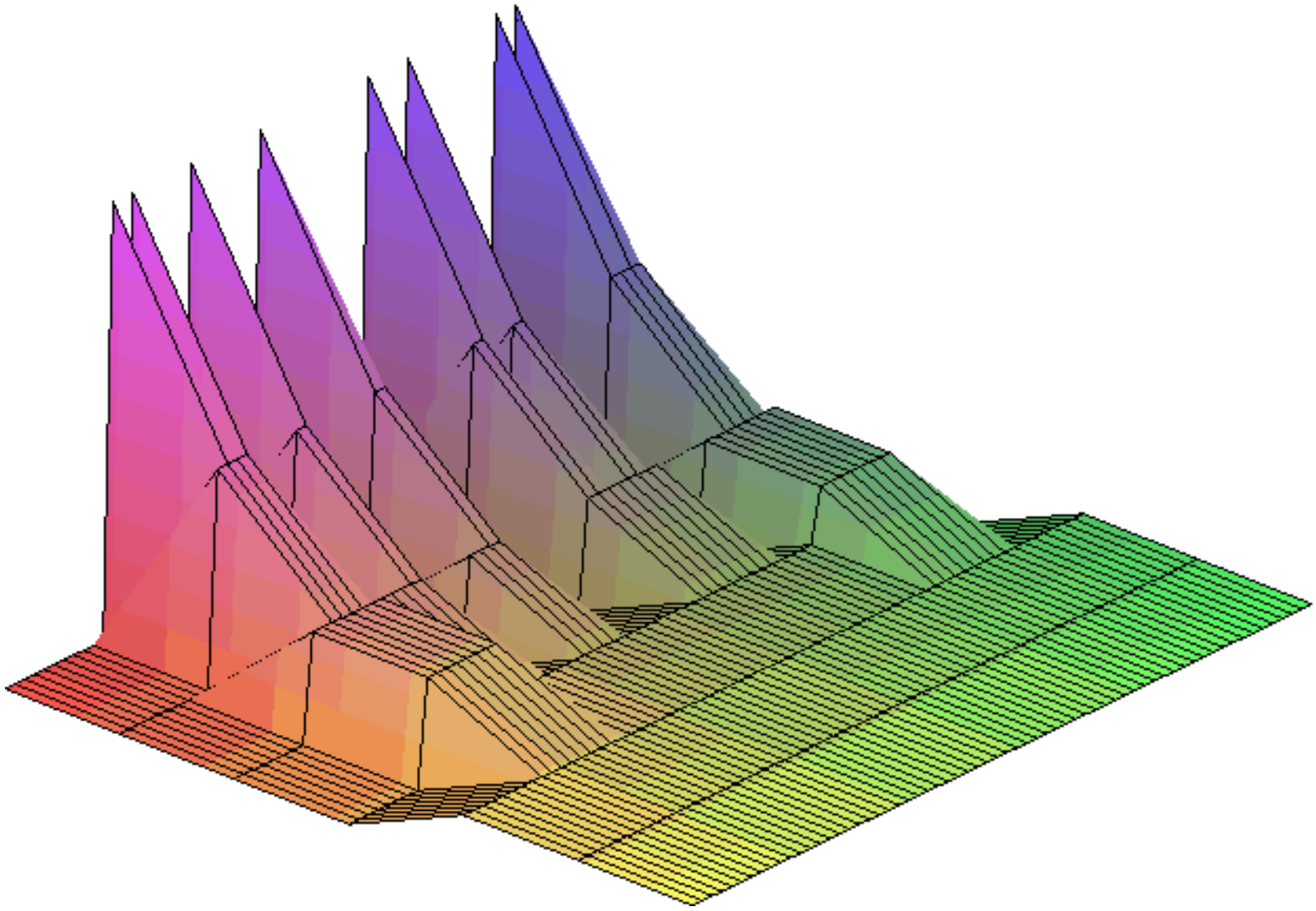
Input: $y \in \mathbb{B}^{i-1}$.

Output: 0 or 1.

1. Choose $y_i, \ldots, y_n \xleftarrow{\text{🎲}} \mathbb{B}$ uniformly and independently at random.
2. $y^* \longleftarrow (y, y_i, \ldots, y_n)$. [Thus $y^* \in \mathbb{B}^n$.]
3. $z \longleftarrow \mathcal{A}(y^*)$.
4. Return $\neg(y_i \oplus z)$.

COROLLARY. i. *Suppose that each bit of the generator* $f : \mathbb{B}^k \longrightarrow \mathbb{B}^n$ *is* (ε, s)*-unpredictable. Then* $f(U_k)$ *is* $(\varepsilon, s+1)$*-indistinguishable from* U_n*.*

ii. *Suppose that the generator* $g = (g_k)_{k\in\mathbb{N}}$ *is such that random bits (that is, for a sequence* $(i_k)_{k\in\mathbb{N}}$ *with* $i_k \xleftarrow{\text{🎲}} \{1, \ldots, n(k)\}$*, the* i_k*th bit of* g_k*) are computationally unpredictable. Then* g *is a pseudorandom generator.*



The following two tables give the values of the $c_i(f(x))$ and e_i.

x	$f(x)$	c_0	c_1	c_2	c_3	c_4	c_5	c_6
000	001101	20	10	4	3	2	1	1
001	001011	20	10	4	3	1	1	1
010	011010	20	10	6	3	2	1	1
011	010110	20	10	6	3	2	1	1
100	101100	20	10	6	3	1	1	1
101	100101	20	10	6	3	2	1	1
110	110100	20	10	4	3	1	1	1
111	110010	20	10	4	3	2	1	1

i	0	1	2	3	4	5	6
e_i	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{3}{8}$	$\frac{13}{32}$	$\frac{1}{2}$	1
$e_i - e_{i-1}$		0	0	$\frac{2}{32}$	$\frac{1}{32}$	$\frac{3}{32}$	$\frac{16}{32}$