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

The Nisan-Wigderson generator

Prof. Dr. Joachim von zur Gathen

Definition. *Let* k, n, s*, and* t *be integers. A* (k, n, s, t)*-design* D *is a sequence* $D = (S_1, \ldots, S_n)$ *of subsets of* $\{1, \ldots, k\}$ *such that for all* $i, j \leq n$ *we have*

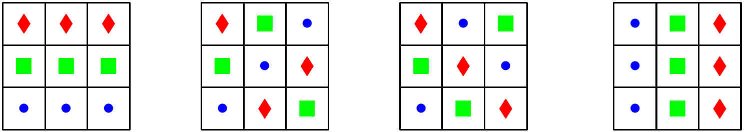
i. $\#S_i = s$,

ii. $\#(S_i \cap S_j) \leq t$ *if* $i \neq j$.

Example. We take $k = 9$, $n = 12$, $s = 3$, and $t = 1$, and arrange the nine elements of $\{1, \ldots, 9\}$ in a 3×3 square:

7	8	9
4	5	6
1	2	3

.



Thus $S_1 = \{1, 2, 3\}$, $S_2 = \{4, 5, 6\}$, $S_3 = \{7, 8, 9\}$, $S_4 = \{1, 5, 9\}$, $S_5 = \{3, 4, 8\}$, $S_6 = \{2, 6, 7\}$, $S_7 = \{1, 6, 8\}$, $S_8 = \{2, 4, 9\}$, $S_9 = \{3, 5, 7\}$, $S_{10} = \{1, 4, 7\}$, $S_{11} = \{2, 5, 8\}$, and $S_{12} = \{3, 6, 9\}$.

Now $D = \{S_1, \ldots, S_{12}\}$ is an $(9, 12, 3, 1)$-design as one easily verifies. As an example, $S_1 \cap S_5 = \{3\}$ has only one element.

If D is a (k, n, s, t)-design as above and $f\colon \mathbb{B}^s \longrightarrow \mathbb{B}$ a Boolean function, we obtain a Boolean function $f_D\colon \mathbb{B}^k \longrightarrow \mathbb{B}^n$ by evaluating f at the subsets of the bits of x given by S_1, ..., S_n. More specifically, if $x \in \mathbb{B}^k$ and $S_i = \{v_1, \ldots, v_s\}$, with $1 \leq v_1 < v_2 < \cdots < v_s \leq k$, then the ith bit of $f_D(x)$ is $f(x_{v_1}, \ldots, x_{v_s})$.

EXAMPLE. We consider the parity function $f\colon \mathbb{B}^3 \longrightarrow \mathbb{B}$, so that $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ is the sum of x_1, x_2, and x_3 modulo 2. With the design from above, the value of $f_D\colon \mathbb{B}^9 \longrightarrow \mathbb{B}^{12}$ at $x = 011110001 \in \mathbb{B}^9$ is

$$f_D\left(\begin{array}{|c|c|c|}\hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline 0 & 1 & 1 \\ \hline\end{array}\right) = 001001010100.$$

For example, the second of the twelve values is computed as $f_D(x)_2 = f(x_4, x_5, x_6) = f(110) = 1 \oplus 1 \oplus 0 = 0$.

THEOREM. *Let* k, n, s *be positive integers,* $s \geq 2$, $t = \lfloor \log_s n \rfloor - 1$, $f\colon \mathbb{B}^s \longrightarrow \mathbb{B}$ *with hardness at least* $2n^2$, *and* D *an* (k, n, s, t)*-design. Then* $f_D\colon \mathbb{B}^k \longrightarrow \mathbb{B}^n$ *is an* (n^{-1}, n)*-resilient pseudorandom generator.*

$$
\begin{aligned}
1/2+\varepsilon &\le \rho_{\mathcal{P}}(X) \\
&= \sum_{y\in\mathbb{B}^{i-1}} \operatorname{prob}\{y \xleftarrow{\text{⚄⚅}} (X_1,\ldots,X_{i-1})\}\cdot \operatorname{prob}\{\mathcal{P}(y) \xleftarrow{\text{⚄⚅}} X_i(y)\} \\
&= \sum_{\substack{x'\in\mathbb{B}^s, x''\in\mathbb{B}^{k-s} \\ y=f_D(x',x'')_{1\ldots i-1}\in\mathbb{B}^{i-1}}} \operatorname{prob}\{x' \xleftarrow{\text{⚄⚅}} U_s\}\cdot \operatorname{prob}\{x'' \xleftarrow{\text{⚄⚅}} U_{k-s}\} \\
&\qquad\qquad \cdot \operatorname{prob}\{f(x') \xleftarrow{\text{⚄⚅}} \mathcal{P}(y)\} \\
&= 2^{-(k-s)} \sum_{x''\in\mathbb{B}^{k-s}} r(x''),
\end{aligned}
$$

where $f_D(x',x'')_{1\ldots i-1}$ stands for $(f_D(x',x'')_1,\ldots,f_D(x',x'')_{i-1})\in\mathbb{B}^{i-1}$, and

$$
r(x'') = 2^{-s} \sum_{\substack{x'\in\mathbb{B}^s \\ y=f_D(x',x'')_{1\ldots i-1}}} \operatorname{prob}\{f(x') \xleftarrow{\text{⚄⚅}} \mathcal{P}(y)\}.
$$

ALGORITHM. Circuit $\mathcal{A}$ that approximates f.

Input: $x' = (x_1, \ldots, x_s) \in \mathbb{B}^s$.
Output: 0 or 1.

1. For $j = 1, \ldots, i-1$ do step 2.
2. $\quad y_j \longleftarrow f_D(x', z)_j$, with $z \in \mathbb{B}^{k-s}$ satisfying **??**.
3. Return $\mathcal{P}(y_1 \ldots, y_{i-1})$.