4.8 The Impagliazzo-Naor Generator

Recall the knapsack problem (or subset sum problem):

Given positive integers $a_1, \ldots, a_n \in \mathbb{N}$ and $T \in \mathbb{N}$.

Wanted a subset $S \subseteq \{1, \ldots, n\}$ with

$$\sum_{i \in S} a_i = T.$$

This problem is believed to be hard. We know it is NP-complete. Building on it Impagliazzo and Naor developed a pseudorandom generator:

Let k and n be (sufficiently large) integers with $n < k < \frac{3n}{2}$. As parameters we choose random $a_1, \ldots, a_n \in [1 \ldots 2^k]$.

> Attention: quite a lot of big numbers.

The state space consists of the power set of $\{1, \ldots, n\}$. So the states are subsets $S \subseteq \{1, \ldots, n\}$. We represent them by bit sequences in $\mathbb{F}_2^n$ in the natural way. In each single step we form the sum

$$\sum_{i \in S} a_i \mod 2^k.$$

This is a k-bit integer. Output the first $k - n$ bits, and retain the last n bits as the new state, see Figure 4.5.

Thus state transition and output function are:

$$\begin{aligned} T(S) &= \sum_{i \in S} a_i \bmod 2^n \\ &\quad \text{(retain the rightmost } n \text{ bits)} \\ U(S) &= \left\lfloor \frac{\sum_{i \in S} a_i \bmod 2^k}{2^n} \right\rfloor \\ &\quad \text{output the leftmost } k - n \text{ bits} \end{aligned}$$

If this pseudorandom generator is not perfect, then the knapsack problem admits an efficient solution. Here we omit the proof. See

- R. Impagliazzo, M. Naor: Efficient cryptographic schemes provably as secure as subset sum. J. Cryptology 9 (1996), 199–216.

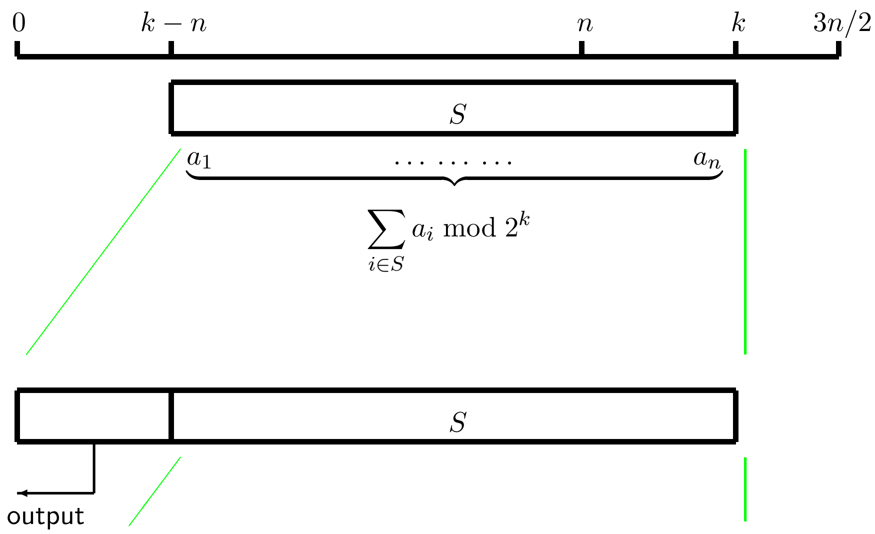

Figure 4.5: The Impagliazzo-Naor generator