PRG

February 22, 2023

Let us assume that the Discrete Logarithm Problem (DLP) is a one-way function, and let msb denote its highest-order bit.

Claim For all Probabilistic Polynomial Time Machines (PPTMs) A, the following claim can be proven:

$$\Pr_{x \in \{0,1\}^n}(\text{predicting all bits of } G(x)) = (1/2)^{l(n)} + \text{negl}(n)$$

where $G(x)$ is a function of x defined as follows:

$$G(x) = h(f^{l(n)-1}(x))||\cdots||h(f^2(x))||h(f(x))||h(x)$$

Proof Assuming that $f(x)$ is the DLP and $h(x)$ is its msb, we can proceed as follows. Let PPTM A be any algorithm that predicts the msb(x). Then, we can say that:

$$\Pr(\text{predicting } h(x)|f(x)) \leq 1/2 + \text{negl}(n)$$

Similar, for any $i \in 2, \ldots, l(n)$.

Now, we can consider the probability of predicting all the bits of $G(x)$. By using the above bounds, we get:

$$\begin{aligned}
\Pr(\text{predicting all bits of } G(x)) &\leq \prod_{i=1}^{l(n)} \Pr(\text{predicting } h(f^{i-1}(x))|f^i(x)) \\
&\leq \prod_{i=1}^{l(n)} (1/2 + \text{negl}(n)) \\
&= (1/2 + \text{negl}(n))^{l(n)} \\
&\leq (1/2)^{l(n)} + \text{negl'}(n)
\end{aligned}$$

where the last inequality follows from the fact that $1/2 + \text{negl}(n) \leq 1/2$ for sufficiently large n. Therefore, the claim is proved. Here, we have shown that the probability of predicting all bits of $G(x)$ is exponentially small in $l(n)$. Hence, we can say that $G(x)$ is a pseudorandom generator.

In summary, the proof shows that under the assumption that the DLP is a one-way function, we can construct a pseudorandom generator $G(x)$ using the highest-order bit of the output of the DLP. The proof also shows that the output of $G(x)$ is indistinguishable from random for any PPTM A. Thus, we can use $G(x)$ as a secure cryptographic primitive.