Example - Secure PRG & Semantic Security

Theorem: Assume that one can efficiently sample an element from the uniform distribution of $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{C}$ in the following statement. If $G(s) : \{0,1\}^l \to \{0,1\}^n$ is a secure PRG, then the cipher $\mathcal{E} = (Enc, Dec)$ defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C}) = (\{0,1\}^l, \{0,1\}^n, \{0,1\}^n)$ where $Enc(k,m) = G(k) \oplus m$ is semantically secure.

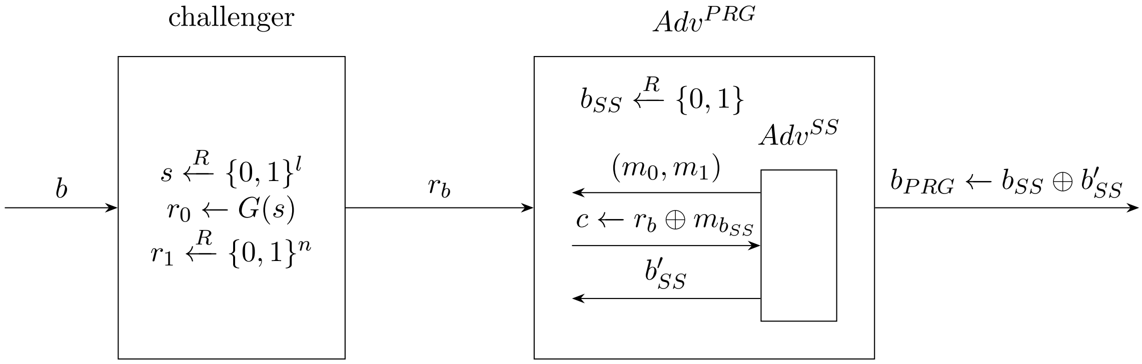
Proof

We will prove this theorem by contrapositive.

Assume that $\mathcal{E}$ is not semantically secure. In other words, there exists a polynomial $poly(n)$ and a polynomial-bounded adversary Adv^{SS} such that $\left|\Pr[Exp^{SS}(0) = 1] - \Pr[Exp^{SS}(1) = 1]\right| \geq \frac{1}{poly(n)}$.

Our goal is to use Adv^{SS} to construct an adversary of the secure PRG game. We will show that the new adversary can win secure PRG game with non-negligible advantage, which means $G(s)$ is not a secure PRG.

Construct an adversary Adv^{PRG}, using Adv^{SS} as a subroutine, to play the experiment b of the secure PRG game:



1. The challenger samples $s \xleftarrow{R} \{0,1\}^l$, $r_1 \xleftarrow{R} \{0,1\}^n$, and computes $r_0 \leftarrow G(s)$.
2. The challenger sends r_b to Adv^{PRG}.
3. Adv^{PRG} starts using Adv^{SS} as a subroutine.
   (a) Adv^{PRG} receives (m_0, m_1) from Adv^{SS}.
   (b) Adv^{PRG} samples $b_{SS} \xleftarrow{R} \{0,1\}$ and sends $c \leftarrow r_b \oplus m_{b_{SS}}$ to Adv^{SS}.
   (c) Adv^{PRG} receives b'_{SS} from Adv^{SS}.
4. Adv^{PRG} outputs $b_{PRG} \leftarrow b_{SS} \oplus b'_{SS}$.

First of all, the things Adv^{PRG} does consist of only sampling and communicating with Adv^{SS}. From the assumption, sampling is efficient. Besides, Adv^{SS} is a polynomial-bounded adversary. Hence, Adv^{PRG} is also polynomial-bounded.

Then, we calculate the advantage of Adv^{PRG}:

$$
\begin{aligned}
&\left|\Pr[Exp^{PRG}(0) = 1] - \Pr[Exp^{PRG}(1) = 1]\right| \\
&= \left|\Pr[b_{SS} \oplus b'_{SS} = 1 | b = 0] - \Pr[b_{SS} \oplus b'_{SS} = 1 | b = 1]\right|
\end{aligned}
$$

For the left part,

$$
\begin{aligned}
&\Pr[b_{SS} \oplus b'_{SS} = 1 | b = 0] \\
=&\Pr[b_{SS} \oplus b'_{SS} = 1 | Adv^{SS} \text{ plays } Exp^{SS}] \\
=&\Pr[b'_{SS} = 1 | b_{SS} = 0 \wedge Adv^{SS} \text{ plays } Exp^{SS}] \cdot \Pr[b_{SS} = 0 | Adv^{SS} \text{ plays } Exp^{SS}] \\
&+ \Pr[b'_{SS} = 0 | b_{SS} = 1 \wedge Adv^{SS} \text{ plays } Exp^{SS}] \cdot \Pr[b_{SS} = 1 | Adv^{SS} \text{ plays } Exp^{SS}] \\
=&\Pr[Exp^{SS}(0) = 1] \cdot \frac{1}{2} + \Pr[Exp^{SS}(1) = 0] \cdot \frac{1}{2} \\
=&\Pr[Exp^{SS}(0) = 1] \cdot \frac{1}{2} + (1 - \Pr[Exp^{SS}(1) = 1]) \cdot \frac{1}{2} \\
=&\frac{1}{2} + \frac{1}{2} \cdot (\Pr[Exp^{SS}(0) = 1] - \Pr[Exp^{SS}(1) = 1])
\end{aligned}
$$

And for the right part, if we see from the point of view of Adv^{SS}, the security game becomes exactly the same game of one-time-pad encryption. To be more specific, Adv^{SS} sends two messages (m_0, m_1) and receives the cipher $c \leftarrow r_1 \oplus m_{b_{SS}}$, where r_1 is random sampled from the key space. Since the one-time-pad encryption is semantically secure, we know that there exists a negligible function $negl(n)$ such that

$$
\left| \Pr[Exp^{SS}_{otp}(0) = 1] - \Pr[Exp^{SS}_{otp}(1) = 1] \right| < negl(n)
$$

For simplicity, we can rewrite the above inequality as

$$
\Pr[Exp^{SS}_{otp}(0) = 1] - \Pr[Exp^{SS}_{otp}(1) = 1] = \pm negl(n)
$$

Continuing on the right part,

$$
\begin{aligned}
&\Pr[b_{SS} \oplus b'_{SS} = 1 | b = 1] \\
=&\Pr[b'_{SS} = 1 | b_{SS} = 0 \wedge b = 1] \cdot \Pr[b_{SS} = 0] \\
&+ \Pr[b'_{SS} = 0 | b_{SS} = 1 \wedge b = 1] \cdot \Pr[b_{SS} = 1] \\
=&\Pr[Exp^{SS}_{otp}(0) = 1] \cdot \frac{1}{2} + \Pr[Exp^{SS}_{otp}(1) = 0] \cdot \frac{1}{2} \\
=&\Pr[Exp^{SS}_{otp}(0) = 1] \cdot \frac{1}{2} + (1 - \Pr[Exp^{SS}_{otp}(1) = 1]) \cdot \frac{1}{2} \\
=&\frac{1}{2} + \frac{1}{2} \cdot (\Pr[Exp^{SS}_{otp}(0) = 1] - \Pr[Exp^{SS}_{otp}(1) = 1]) \\
=&\frac{1}{2} \pm \frac{1}{2} \cdot negl(n)
\end{aligned}
$$

Combining the two parts, the advantage of Adv^{PRG} becomes

$$
\begin{aligned}
&\left| \Pr[b_{SS} \oplus b'_{SS} = 1 | b = 0] - \Pr[b_{SS} \oplus b'_{SS} = 1 | b = 1] \right| \\
=&\left| \left(\frac{1}{2} + \frac{1}{2} \cdot (\Pr[Exp^{SS}(0) = 1] - \Pr[Exp^{SS}(1) = 1]) \right) - \left(\frac{1}{2} + \frac{1}{2} \cdot negl(n) \right) \right| \\
=&\frac{1}{2} \cdot \left| \Pr[Exp^{SS}(0) = 1] - \Pr[Exp^{SS}(1) = 1] \mp negl(n) \right|
\end{aligned}
$$

As we have assumed before, $\left|\Pr[Exp^{SS}(0) = 1] - \Pr[Exp^{SS}(1) = 1]\right| \geq \frac{1}{poly(n)}$. Therefore, the advantage of Adv^{PRG} is non-negligible, which means that $G(s)$ is not a secure PRG. We have proved this theorem by contrapositive. ■