

Understanding the definition:

1. Can we ask for security against all adversaries (when $n \gg \lambda$)?

No! Consider inefficient adversary that outputs 1 if t is the image of G and 0 otherwise.

- $W_0 = 1$

- $W_1 = \Pr[t \in \{0,1\}^n : \exists s \in \{0,1\}^\lambda : G(s) = t] = \frac{1}{2^{n-\lambda}}$

} $\text{PRGAdv}[A, G] = 1 - \frac{1}{2^{n-\lambda}} \approx 1$ if $n \gg \lambda$

2. Can the output of a PRG be biased (e.g., first bit of PRG output is 1 w.p. $\frac{2}{3}$)?

No! Consider efficient adversary that outputs 1 if first bit of challenge is 1.

- $W_0 = \frac{2}{3}$

- $W_1 = \frac{1}{2}$

} $\text{PRGAdv}[A, G] = \frac{1}{6}$ Not NEGLIGIBLE!

More generally, no efficient statistical test can distinguish output of a secure PRG from random.

3. Can the output of a PRG be predictable (e.g., given first 10 bits, predict the 11th bit)?

No! If the bits are predictable w.p. $\frac{1}{2} + \epsilon$, can distinguish with advantage ϵ (since random string is unpredictable)

In fact: unpredictable \Rightarrow pseudorandom

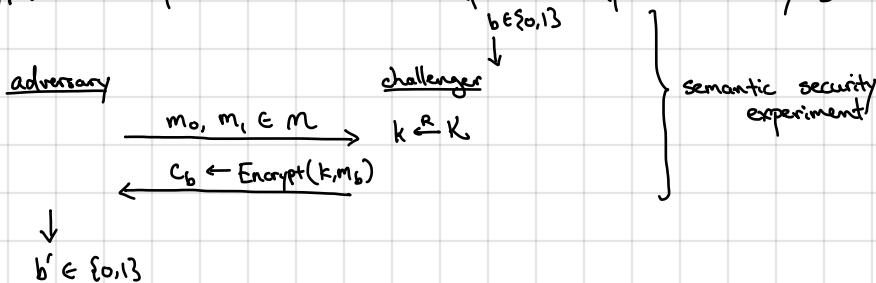
Take-away: A secure PRG has the same statistical properties as the one-time pad to any efficient adversary.

\Rightarrow Should be able to use it in place of one-time pad to obtain a secure encryption scheme (against efficient adversaries)

Need to define security of an encryption scheme.

Goal is to capture property that no efficient adversary can learn any information about the message given only the ciphertext. Suffices to argue that no efficient adversary can distinguish encryption of message m_0 from m_1 , even if m_0, m_1 are adversarially-chosen.

Let $(\text{Encrypt}, \text{Decrypt})$ be a cipher. We define two experiments (parameterized by $b \in \{0,1\}$):



Adversary chooses two messages and receives encryption of one of them. Needs to guess which one (i.e., distinguish encryption of m_0 from encryption of m_1)

Let $W_0 := \Pr[b' = 1 \mid b = 0]$ } probability that adversary guesses 1

$W_1 := \Pr[b' = 1 \mid b = 1]$ } (if adversary is good distinguisher, these two should be very different)

Define semantic security advantage of adversary A for cipher $\Pi_{SE} = (\text{Encrypt}, \text{Decrypt})$

$\text{SSAdv}[A, \Pi_{SE}] = |W_0 - W_1|$

Definition. A cipher $\Pi_{SE} = (\text{Encrypt}, \text{Decrypt})$ is semantically secure if for all efficient adversaries A ,

$\text{SSAdv}[A, \Pi_{SE}] = \text{negl}(\lambda)$

$\leftarrow \lambda$ is a security parameter (here, models the bit-length of the key)

Understanding the definition:

Can we learn the least significant bit of a message given only the ciphertext (assuming a semantically-secure cipher)

No! Suppose we could. Then, adversary can choose two messages m_0, m_1 that differ in their least significant bit and distinguish with probability 1.

This generalizes to any efficiently-computable property of the two messages.

How does semantic security relate to perfect secrecy?

Theorem. If a cipher satisfies perfect secrecy, then it is semantically secure.

Proof. Perfect secrecy means that $\forall m_0, m_1 \in \mathcal{M}, c \in \mathcal{C}$:

$$\Pr[k \xleftarrow{R} K : \text{Encrypt}(k, m_0) = c] = \Pr[k \xleftarrow{R} K : \text{Encrypt}(k, m_1) = c]$$

Equivalently, the distributions

$$\underbrace{\{k \xleftarrow{R} K : \text{Encrypt}(k, m_0)\}}_{D_0} \quad \text{and} \quad \underbrace{\{k \xleftarrow{R} K : \text{Encrypt}(k, m_1)\}}_{D_1}$$

are identical ($D_0 \equiv D_1$). This means that the adversary's output b is identically distributed in the two experiments, and so $\text{SSAdv}[A, \Pi_{SE}] = |W_0 - W_1| = 0$.

Corollary. The one-time pad is semantically secure.

$$\begin{array}{l} \text{encryption key (PRG seed)} \\ \downarrow \\ c \leftarrow G(s) \oplus m \\ m \leftarrow G(s) \oplus c \end{array}$$

seems straightforward, but takes some care to prove

Theorem. Let G be a secure PRG. Then, the resulting stream cipher constructed from G is semantically secure.

Proof. Consider the semantic security experiments:

Experiment 0: Adversary chooses m_0, m_1 and receives $c_0 = G(s) \oplus m_0$
Experiment 1: Adversary chooses m_0, m_1 and receives $c_1 = G(s) \oplus m_1$

Want to show that adversary's output in these two experiments are indistinguishable

Let $W_0 = \Pr[A \text{ outputs } 1 \text{ in Experiment } 0]$

$W_1 = \Pr[A \text{ outputs } 1 \text{ in Experiment } 1]$

Idea: If $G(s)$ is uniform random string (i.e., one-time pad), then $W_0 = W_1$. But $G(s)$ is like a one-time pad!

Define Experiment $0'$: Adversary chooses m_0, m_1 and receives $c_0 = t \oplus m_0$ where $t \xleftarrow{R} \{0,1\}^n$

Experiment $1'$: Adversary chooses m_0, m_1 and receives $c_1 = t \oplus m_1$ where $t \xleftarrow{R} \{0,1\}^n$

Define W'_0, W'_1 accordingly.

First, observe that $W'_0 = W'_1$ (one-time pad is perfectly secure).

Now we show that $|W_0 - W'_0| = \text{negl}$ and $|W_1 - W'_1| < \text{negl}$.

$$\begin{aligned} \Rightarrow |W_0 - W_1| &= |W_0 - W'_0 + W'_0 - W'_1 + W'_1 - W_1| \\ &\leq |W_0 - W'_0| + |W'_0 - W'_1| + |W'_1 - W_1| \quad \text{by triangle inequality} \\ &= \text{negl.} + \text{negl.} = \text{negl.} \end{aligned}$$

Show. If G is a secure PRG, then for all efficient A , $|W_0 - W'_0| = \text{negl}$.

Common proof technique: prove the contrapositive.

Contrapositive: If A can distinguish Experiments 0 and $0'$, then G is not a secure PRG.

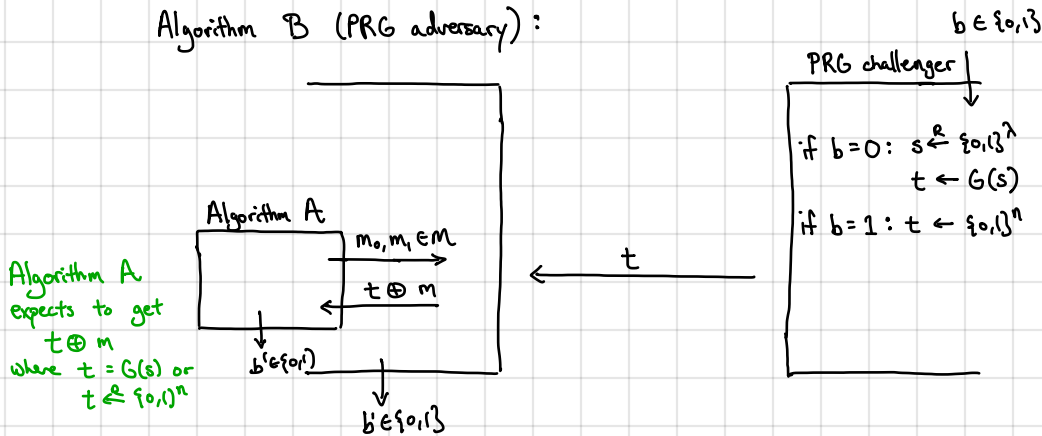
Suppose there exists efficient A that distinguishes Experiment 0 from $0'$

\Rightarrow We use A to construct efficient adversary B that breaks security of G .

\hookrightarrow this step is a reduction

[we show how adversary (i.e., algorithm) for distinguishing Exp. 0 and $0'$ \Rightarrow adversary for PRG]

Algorithm B (PRG adversary):



Running time of $B =$ running time of $A =$ efficient

Compute $\text{PRGAdv}[B, G]$.

$\Pr[B \text{ outputs } 1 \text{ if } b=0] = W_0 \leftarrow$ if $b=0$, then A gets $G(s) \oplus m$ which is precisely the behavior in Exp. 0

$\Pr[B \text{ outputs } 1 \text{ if } b=1] = W'_0 \leftarrow$ if $b=1$, then A gets $t \oplus m$ which is precisely the behavior in Exp. $0'$

$\Rightarrow \text{PRGAdv}[B, G] = |W_0 - W'_0|$, which is non-negligible by assumption. This proves the contrapositive.

Important note: Security of above schemes shown assuming message space is $\{0,1\}^n$ (i.e., all messages are n -bits long)

In practice: We have variable-length messages. In this case, security guarantees indistinguishability from other messages of the same length, but length itself is leaked [inevitable if we want short ciphertexts]

\hookrightarrow can be problematic - see traffic analysis attacks!

So far, we have shown that if we have a PRG, then we can encrypt messages efficiently (stream cipher)