Introduction to Cryptology

Lecture 7
Announcements

• HW3 due Tuesday, 2/21
• Quiz Solutions up on Canvas
Agenda

• Last time:
  – The Computational Approach (K/L 3.1)
  – Defining computationally secure SKE (K/L 3.2)

• This time:
  – Defining PRG (K/L 3.3)
  – Exercise on PRG
  – Constructing computationally secure SKE (K/L 3.3)
  – Security proof for construction (K/L 3.3)
  – Discussion on Stream Ciphers
Pseudorandom Generator

• Functionality
  – Deterministic algorithm $G$
  – Takes as input a short random seed $s$
  – Outputs a long string $G(s)$

• Security
  – No efficient algorithm can “distinguish” $G(s)$ from a truly random string $r$.
  – i.e. passes all “statistical tests.”

• Intuition:
  – Stretches a small amount of true randomness to a larger amount of pseudorandomness.

• Why is this useful?
  – We will see that pseudorandom generators will allow us to beat the Shannon bound of $|K| \geq |M|$.
  – i.e. we will build a computationally secure encryption scheme with $|K| < |M|$.
Pseudorandom Generators

Definition: Let $\ell(\cdot)$ be a polynomial and let $G$ be a deterministic poly-time algorithm such that for any input $s \in \{0,1\}^n$, algorithm $G$ outputs a string of length $\ell(n)$. We say that $G$ is a pseudorandom generator if the following two conditions hold:

1. (Expansion:) For every $n$ it holds that $\ell(n) > n$.
2. (Pseudorandomness:) For all ppt distinguishers $D$, there exists a negligible function $negl$ such that:

$$\left| \Pr[D(r) = 1] - \Pr[D(G(s)) = 1] \right| \leq negl(n),$$

where $r$ is chosen uniformly at random from $\{0,1\}^{\ell(n)}$, the seed $s$ is chosen uniformly at random from $\{0,1\}^n$, and the probabilities are taken over the random coins used by $D$ and the choice of $r$ and $s$.

The function $\ell(\cdot)$ is called the expansion factor of $G$. 
Stream Cipher

• Practical instantiation of a pseudorandom generator (will talk more about them and how they are constructed later in the course).
• Pseudorandom bits of a stream cipher are produced gradually and on demand.
• Application can request exact number of bits needed.
• This improves efficiency.
Constructing Secure Encryption Schemes
A Secure Fixed-Length Encryption Scheme
The Encryption Scheme

Let $G$ be a pseudorandom generator with expansion factor $\ell$. Define a private-key encryption scheme for messages of length $\ell$ as follows:

- **Gen**: on input $1^n$, choose $k \leftarrow \{0,1\}^n$ uniformly at random and output it as the key.
- **Enc**: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^{\ell(n)}$, output the ciphertext
  \[ c := G(k) \oplus m. \]
- **Dec**: on input a key $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^{\ell(n)}$, output the plaintext message
  \[ m := G(k) \oplus c. \]
Recall: Indistinguishability in the presence of an eavesdropper

Consider a private-key encryption scheme $\Pi = (Gen, Enc, Dec)$, any adversary $A$, and any value $n$ for the security parameter.

The eavesdropping indistinguishability experiment $PrivK^{eav}_{A,\Pi}(n)$:

1. The adversary $A$ is given input $1^n$, and outputs a pair of messages $m_0, m_1$ of the same length.
2. A key $k$ is generated by running $Gen(1^n)$, and a random bit $b \leftarrow \{0,1\}$ is chosen. A challenge ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to $A$.
3. Adversary $A$ outputs a bit $b'$.
4. The output of the experiment is defined to be $1$ if $b' = b$, and $0$ otherwise. If $PrivK^{eav}_{A,\Pi}(n) = 1$, we say that $A$ succeeded.
Recall: Indistinguishability in the presence of an eavesdropper

Definition: A private key encryption scheme \( \Pi = (Gen, Enc, Dec) \) has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries \( A \) there exists a negligible function \( negl \) such that

\[
\Pr \left[ PrivK^{eav}_{A, \Pi}(n) = 1 \right] \leq \frac{1}{2} + negl(n),
\]

Where the prob. Is taken over the random coins used by \( A \), as well as the random coins used in the experiment.
Theorem: If $G$ is a pseudorandom generator, then the Construction above is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.
Security Analysis

- Proof by reduction method.
Security Analysis

Proof: Let $A$ be a ppt adversary trying to break the security of the construction. We construct a distinguisher $D$ that uses $A$ as a subroutine to break the security of the PRG.

Distinguisher $D$:

$D$ is given as input a string $w \in \{0,1\}^{\ell(n)}$.

1. Run $A(1^n)$ to obtain messages $m_0, m_1 \in \{0,1\}^{\ell(n)}$.
2. Choose a uniform bit $b \in \{0,1\}$. Set $c := w \oplus m_b$.
3. Give $c$ to $A$ and obtain output $b'$. Output 1 if $b' = b$, and output 0 otherwise.
Security Analysis

Consider the probability $D$ outputs 1 in the case that $w$ is random string $r$ vs. $w$ is a pseudorandom string $G(s)$.

• When $w$ is random, $D$ outputs 1 with probability exactly $\frac{1}{2}$. Why?

• When $w$ is pseudorandom, $D$ outputs 1 with probability $\Pr[\text{Priv}_{A,\Pi}^eav(n) = 1] = \frac{1}{2} + \rho(n)$, where $\rho$ is non-negligible.
Security Analysis

$D$’s distinguishing probability is:

$$\left| \frac{1}{2} - \left( \frac{1}{2} + \rho(n) \right) \right| = \rho(n).$$

This is a contradiction to the security of the PRG, since $\rho$ is non-negligible.