Constructing a Computationally Secure Scheme

Pseudorandomness

Foundations of Cryptography
Computer Science Department
Wellesley College

Fall 2016

Table of contents

Introduction

Pseudorandom generators

Secure Encryption Scheme

Multiple Encryptions
Pseudorandomness

- A *pseudorandom* string* looks like a uniformly distributed string, as long as the entity that is "looking" runs in polynomial time.
- Just as indistinguishability is a computational relaxation of perfect secrecy, pseudorandomness is a computational relaxation of true randomness.

*Technically no one string can be “pseudorandom”; pseudorandomness refers to a distribution $D$ of strings that indistinguishable from the uniform distribution.

Why study pseudorandomness?

- If a ciphertext looks random, then no adversary can learn any information from it about the plaintext. This is the intuition behind the one-time pad.
- If a one-time pad used a pseudorandom string instead of a truly random one, this should not make any difference to a polynomial-time observer.
- The advantage is that a long pseudorandom string can be generated from a relatively short random seed. Thus, a short key can be used to encrypt a long message.
**Pseudorandom Generators**

**Definition 3.14.** Let $\ell(\cdot)$ be a polynomial and let $G$ be a deterministic polynomial-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 probabilistic polynomial-time distinguishers $D$, there exists a negligible function $\text{negl}$ such that:

$$|\Pr[D(r) = 1] - \Pr[D(G(s)) = 1]| \leq \text{negl}(n),$$

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 $s$.

**Not a pseudorandom generator**

To understand what makes for a secure pseudorandom generator, let’s examine a rather poor one.

**Example 3.15.** Define $G(s)$ to output $s$ followed by $\bigoplus_{i=1}^{n} s_i$ with expansion factor $\ell(n) = n + 1$.

Consider the distinguisher $D$ that on input $w$, outputs 1 if and only if the final bit of $w$ is equal to the XOR of all preceding bits.

Since all strings output by $G$ have this property, $\Pr[D(G(s)) = 1] = 1$. On the other hand, if $w$ is uniform, its final bit is uniform and so $\Pr[D(w) = 1] = \frac{1}{2}$. 
Pseudorandom generators are a far cry from random

- Consider $G$ that doubles the length of its inputs, that is, $\ell(n) = 2n$.

- The uniform distribution over $\{0, 1\}^{2n}$ chooses each of the $2^{2n}$ possible strings with equal probability.

- In contrast, given an input of length $n$, the number of different possible strings in $G$’s range is at most $2^n$.

- The probability that a given random string is in the range of $G$ is at most $2^n/2^{2n} = 2^{-n}$.

- Unlimited time works its magic*

    - Consider the distinguisher $D$ that works as follows: Upon input string $w$, distinguisher $D$ outputs 1 iff there exists an $s \in \{0, 1\}^n$ such that $G(s) = w$.

    - If $w$ was generated by $G$, then $D$ outputs 1 with certainty. In contrast, if $w$ is uniformly distributed in $\{0, 1\}^{2n}$ then the probability that there is an $s$ with $G(s) = w$ is at most $2^{-n}$.

    - We have

      $$|\Pr[D(r) = 1] - \Pr[D(G(s)) = 1]| \geq 1 - 2^{-n},$$

      which is large.

*Distinguisher $D$ is our old friend Brute, and this type of attack is called brute force attack. Polynomial-time distinguishers do not have the time to carry out such an attack.
Yes, Virginia ...

- We do not know how to unequivocally prove the existence of pseudorandom generators.
- Nevertheless, we still believe in them.
- We base this belief in part upon the fact that they exist if one-way functions do.

*An assumption rather weaker than the existence of the tooth fairy if that is any comfort.

Constructing a secure encryption scheme

- We construct a fixed-length encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.
- Our scheme is very similar to the one-time pad, except a pseudorandom string is used as the “pad” rather than a random string.
The encryption scheme

Construction 3.17. 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
  \[ m := G(k) \oplus c. \]

Claim of indistinguishable encryptions in the presence of an eavesdropper*

Theorem 3.18. Let $G$ be a pseudorandom generator, then Construction 3.17 is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.

*Note that our claim is not unconditional. Rather we reduce the security of the encryption scheme to the properties of $G$ as a pseudorandom generator.
Before the proof, a brief review is in order

The experiment is defined for any private-key encryption scheme \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \), any adversary \( \mathcal{A} \), and any value \( n \) for the security parameter:

**The eavesdropping indistinguishability experiment** \( \text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) \)

1. The adversary \( \mathcal{A} \) is given \( 1^n \), and outputs a pair of message \( m_0, m_1 \in M \) of the same length.

2. A key \( k \) is generated by running \( \text{Gen}(1^n) \), and a random bit \( b \leftarrow \{0, 1\} \) is chosen. A **challenge ciphertext** \( c \leftarrow \text{Enc}_k(m_b) \) is computed and given to \( \mathcal{A} \).

3. \( \mathcal{A} \) outputs a bit \( b' \).

4. The output of the experiment is defined to be 1 if \( b' = b \), and 0 otherwise. We write \( \text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) = 1 \) if the output is 1 and in this case we say that \( \mathcal{A} \) **succeeded**.

---

**Adversarial indistinguishability**

**Definition 3.8.** An encryption scheme \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \) had **indistinguishable encryption in the presence of an eavesdropper** if for all probabilistic polynomial-time adversaries \( \mathcal{A} \) there exists a negligible function \( \text{negl} \) such that

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

where the probability is taken over the random coins used by \( \mathcal{A} \), as well as the random coins used by the experiment (for choosing the key, the random bit \( b \), and any random coins used in the encryption process).
**Claim of indistinguishable encryptions in the presence of an eavesdropper**

*Theorem 3.18.* Let $G$ be a pseudorandom generator, then Construction 3.17 is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.

*Proof.* Let $\Pi$ denote Construction 3.17. We show that if there exists a probabilistic polynomial-time adversary $A$ for which Definition 3.8 does not hold, then we can construct a probabilistic polynomial-time algorithm that distinguishes the output $G$ from a truly random one.

Let $A$ be a probabilistic polynomial-time adversary. We use $A$ to construct the following distinguisher $D$ for the pseudorandom generator $G$.

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

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

- Define a modified encryption scheme $\tilde{\Pi} = (\tilde{\text{Gen}}, \tilde{\text{Enc}}, \tilde{\text{Dec}})$ that is exactly the one-time pad encryption scheme, except that we now incorporate a security parameter that determines the length of the messages to be encrypted.
- $\tilde{\text{Gen}}(1^n)$ outputs a random key of length $\ell(n)$, and the encryption of a message $m \in \{0,1\}^{\ell(n)}$ using the key $k \in \{0,1\}^{\ell(n)}$ is the ciphertext $c := k \oplus m$.
- By perfect secrecy of the one-time pad,
  \[
  \Pr \left[ \text{PrivK}_{\mathcal{A},\tilde{\Pi}}^\text{eav}(n) = 1 \right] = \frac{1}{2}.
  \]

Analysis of the distinguisher

1. If $w$ is chosen uniformly from $\{0,1\}^{\ell(n)}$, then the view of $\mathcal{A}$ when run as a sub-routine by $D$ is distributed identically to the view of $\mathcal{A}$ in experiment $\text{PrivK}_{\mathcal{A},\tilde{\Pi}}^\text{eav}(n)$. Thus,
  \[
  \Pr_{w \leftarrow \{0,1\}^{\ell(n)}}[D(w) = 1] = \Pr \left[ \text{PrivK}_{\mathcal{A},\tilde{\Pi}}^\text{eav}(n) = 1 \right] = \frac{1}{2}.
  \]

2. If $w$ is equal to $G(k)$ for $k \leftarrow \{0,1\}^n$ chosen uniformly at random, then the view of $\mathcal{A}$ when run as a sub-routine by $D$ is distributed identically to the view of $\mathcal{A}$ in experiment $\text{PrivK}_{\mathcal{A},\tilde{\Pi}}^\text{eav}(n)$ and
  \[
  \Pr_{w \leftarrow \{0,1\}^{\ell(n)}}[D(G(k)) = 1] = \Pr \left[ \text{PrivK}_{\mathcal{A},\tilde{\Pi}}^\text{eav}(n) = 1 \right].
  \]
Therefore
\[
\left| \Pr_{w \leftarrow \{0,1\}^\ell(n)}[D(w) = 1] - \Pr_{w \leftarrow \{0,1\}^\ell(n)}[D(G(k)) = 1] \right| \leq \negl(n).
\]

Substituting values previously found for these probabilities, we see that
\[
\left| \frac{1}{2} - \Pr[\text{PrivK}_{A,\Pi}^{\text{eav}}(n) = 1] \right| \leq \negl(n)
\]
which implies \(\Pr[\text{PrivK}_{A,\Pi}^{\text{eav}}(n) = 1] \leq \frac{1}{2} + \negl(n)\). \hfill \square

---

## Security for multiple encryptions

- We have assumed that the adversary receives only a single ciphertext.
- In reality, communicating parties send multiple ciphertexts and an eavesdropper will see many of these.
- Some form of security upgrade is required.
The multiple-message eavesdropping experiment

The experiment is defined for any private-key encryption scheme \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \), an adversary \( \mathcal{A} \), and an a security parameter \( n \): 

**The multiple-message eavesdropping indistinguishability experiment**

\( \text{PrivK}_{\mathcal{A}, \Pi}^{\text{mult}}(n) \)

1. The adversary \( \mathcal{A} \) is given \( 1^n \), and outputs a pairs of vectors of messages \( \tilde{M}_0 = (m_{0,1}, \ldots, m_{0,t}) \) and \( \tilde{M}_1 = (m_{1,1}, \ldots, m_{1,t}) \) with \( |m_{0,i}| = |m_{1,i}| \) for all \( i \).

2. A key \( k \) is generated by running \( \text{Gen}(1^n) \), and a random bit \( b \in \{0, 1\} \) is chosen. For all \( i \), the ciphertext \( c_i \leftarrow \text{Enc}_k(m_{b,i}) \) is computed and the vector of ciphertexts \( \tilde{C} = (c_1, \ldots, c_t) \) given to \( \mathcal{A} \).

3. \( \mathcal{A} \) outputs a bit \( b' \).

4. The output of the experiment is defined to be 1 if \( b' = b \), and 0 otherwise.

**Indistinguishable multiple encryptions**

**Definition 3.19.** An encryption scheme \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \) had *indistinguishable multiple encryptions in the presence of an eavesdropper* if for all probabilistic polynomial-time adversaries \( \mathcal{A} \) there exists a negligible function \( \text{negl} \) such that

\[
\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{mult}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n),
\]

where the probability is taken over the random coins used by \( \mathcal{A} \), as well as the random coins used by the experiment (for choosing the key, the random bit \( b \), and any random coins used in the encryption process).

*It goes without saying that security for a single encryption may not imply security under multiple encryptions.*
**Bad news**

**Proposition 3.20.** There exists private-key encryption schemes that have indistinguishable encryptions in the presence of an eavesdropper, but do not have indistinguishable multiple encryptions in the presence of an eavesdropper.

**Proof.** The one-time pad is perfectly secret, and so also has indistinguishable encryptions in the presence of an eavesdropper. We show that it is not secure in the multiple ciphertext.*

*Reality Check: Students in CS342, Computer Security, are asked to decipher two messages sent with the same one-time pad given some basic C code for manipulating bits and several probable words. While tedious, most everyone broke both messages within a few days.

**In more detail**

**Proposition 3.20.** There exists private-key encryption schemes that have indistinguishable encryptions in the presence of an eavesdropper, but do not have indistinguishable multiple encryptions in the presence of an eavesdropper.

**Proof.** Consider an adversary $\mathcal{A}$ attacking the one-time pad encryption scheme (in the sense defined by experiment PrivK$^{\text{mult}}$): $\mathcal{A}$ outputs the vectors $\mathbf{M}_0 = (0^\ell, 0^\ell)$ and $\mathbf{M}_1 = (0^\ell, 1^\ell)$. Now let $\mathbf{C} = (c_1, c_2)$ be the vector of ciphertexts that $\mathcal{A}$ receives. If $c_1 = c_2$, then $\mathcal{A}$ outputs 0; otherwise $\mathcal{A}$ outputs 1.

The key observation here is that Construction 3.15 is deterministic, so that if the same message is encrypted multiple times then the same ciphertext results in each case.

...
The lesson here

**Theorem 3.21.** Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a (stateless) encryption scheme for which $\text{Enc}$ is a deterministic function of the key and the message. Then $\Pi$ does not have indistinguishable multiple encryptions in the presence of an eavesdropper.