Cryptography
Lecture 4

Lecture by Dr. Alon Rosen
Typeset by Steven Karas

2019-03-26
Last edited 18:06:02 2019-03-26

Disclaimer These notes are based on the lectures for the course Cryptography, taught by Dr. Alon Rosen at IDC Herzliyah in the spring semester of 2018/2019. Sections may be based on the lecture slides prepared by Dr. Alon Rosen.

1 Agenda

- Computational security

2 Computational security - Private key

2.1 Definition: Computationally indistinguishable encryptions

(G, E, D) over $\mathcal{P} = \cup_n \mathcal{P}_n$ has computationally indistinguishable encryptions if for any PPT A there exists a negligible function ε such that $\forall m_1, m_2 \in \mathcal{P}$:

$$\Pr[A(E_k(m_0)) = 1] - \Pr[A(E_k(m_1)) = 1] \leq \varepsilon(n)$$

We define a negligible function if it holds for any $\text{poly}(n)$:

$$\text{neg}(n) \leq \frac{1}{\text{poly}(n)}$$

Note that we set the length of the encrypted messages to a constant value. There is a real-world case of Google's autocomplete being broken based on the length of repeated messages. [1].

Academically, we discuss asymptotic negligibility. In practice, we care that something is negligible to within $1/2^{128}$

2.2 Definition: Semantic Security

(G, E, D) over $\mathcal{P} = \cup_n \mathcal{P}_n$ satisfies semantic security if for any PPT A there exists a PPT A' for any distribution M over $\mathcal{P}_n$ such that $\forall f : \mathcal{P}_n \to \{0,1\}^*$ it holds that:

$$\Pr[A(E_k(M)) = f(M)] \leq \Pr[A'(1^n) = f(M)] + \text{neg}(n)$$

Note that we give A' an input in unary to make it fair, as A gets an input in $\text{poly}(n)$. For example, consider the following functions:

- $f(m) = m$
- $f(m) = m_i$ for any i
- Note that $f(m) = |m|$ is allowed, as this is not considered secret by definition.

2.3 Theorem: Equivalency

(G, E, D) satisfies computationally indistinguishable encryption iff it satisfies semantic security.

[1] The game-based alternative definition will not be covered, but appears in both the lecture notes and in Katz-Lindell

Computationally indistinguishable encryption implies semantic security Let A be a PPT, M be any distribution over $\mathcal{P}_n$ and f be any function. Fix any $m_0 \in \mathcal{P}_n$ and let $A'(1^n)$ work as follows:

1. $k \xleftarrow{R} G(1^n)$
2. Run $A(E_k(m_0))$

$$\begin{aligned}\Pr_{M,K}[A(E_k(M)) = f(M)] &\leq_* \Pr[A(E_k(m_0)) = f(M)] + \text{neg}(n) \\ &= \Pr[A'(1^n) = f(M)] + \text{neg}(n)\end{aligned}$$

Consider some message m' that maximizes the probability:

$$\Pr[A(E_k(M)) = f(M)] = \sum_{m' \in \mathcal{P}} \Pr[A(E_k(m')) = f(m') \mid M = m'] \cdot \Pr[M = m']$$

Suppose towards negation that * is false. This implies that the average (the left side) is greater than the total. This implies the existence of a message for which it holds. Which means that we can break the encryption.

Therefore, there exists a PPT B that violates indistinguishable encryption:

$$B(c) = \begin{cases} 1 & A(c) = f(m) \\ 0 & A(c) \neq f(m) \end{cases}$$

This contradicts our assumption, so we have shown that * must be true.

3 Pseudorandom generators and secure encryption

Our goal in this section is to present encryption schemes that use keys that are much shorter, yet we consider them to be sufficiently secure. First, we need to define a random stream of bits. A random stream should satisfy at least (all these are computationally efficient tests):

- each bit should be "almost" unbiased
- fraction of 1s should be around 50%
- longest run of 1s should be $O(\log n)$
- incompressible

There is a publicly available test suite called the "Die-Hard" that runs many different statistical tests.

3.1 Definition: Pseudorandom generators

$G : \{0,1\}^* \to \{0,1\}^*$ is a pseudorandom generator if:

- G can be computed in polytime
- $|G(x)| = \ell(|x|)$ for $\ell(n) > n$
- for any PPT D there exists $\text{neg}\,\varepsilon$ such that:

$$\Pr[D_{U_n}(G(U_n)) = 1] - \Pr_{U_{\ell(n)}}[D(U_{\ell(n)}) = 1] \leq \varepsilon$$

Note: we denote n uniformly random bits as U_n.

Proposition: If G is a PRG, then Pr[fraction of 1s in $G(U_n)$ is $< 1/3$] $< \text{neg}(n)$.

Define a polytime D:

$$D(y) = \begin{cases} 1 & \text{if fraction of 1s is } < 1/3 \\ 0 & \text{else} \end{cases}$$

$$\begin{aligned}\Pr[D(U_{\ell(n)}) = 1] &\leq \exp(-c\ell(n)) \\ \Pr[D(G(U_n) = 1] &\leq \exp(-c\ell(n)) + \text{neg}(n) = \text{neg}(n)\end{aligned}$$

3.2 From PRG to Encryption

Given a PRG G build an encryption scheme (G_{Enc}, E, D):

- the key k is a random seed for G
- $E_k(m)$ is defined as:
  1. $k' = G(k)$
  2. $c = k' \oplus m$

3.3 Theorem: Stream ciphers are secure

If G is a PRG, then $(G_{\text{Enc},E,D})$ satisfies indistinguishable secrecy.

Let A be any PPT algorithm and let $m_0, m_1 \in \mathcal{P}$ be any two messages.

Define 4 distributions:

1. $\text{Real}_0 : E_k(m_0) = G(k) \oplus m_0,\ k \leftarrow U_n$
2. $\text{Real}_1 : E_k(m_1) = G(k) \oplus m_1,\ k \leftarrow U_n$
3. $\text{Ideal}_0 : k' \oplus m_0,\ k' \leftarrow U_{\ell(n)}$
4. $\text{Ideal}_1 : k' \oplus m_1,\ k' \leftarrow U_{\ell(n)}$

where $|k| = n$ and $|m_0| = |k'| = \ell(n)$.

We want to show that Real_0 and Real_1 are computationally indistinguishable.

$\text{Real}_0 \equiv_c \text{Ideal}_0$ because G is a PRG. $\text{Ideal}_0 \equiv \text{Ideal}_1$ because one-time pads satisfy perfect secrecy. $\text{Ideal}_1 \equiv_c \text{Real}_1$ because G is a PRG.

However, we have not proven that computational indistinguishability is transitive.

This approach is common in modern crypto, where we design a scheme in an ideal world, and show that any attacks that can be done in the real world can be done in the ideal world, and then show that there are no attacks in the ideal world, such that the scheme is secure.

Lemma If G is a PRG then for any PPT A:

$$|\Pr[A(\text{Real}_0) = 1] - \Pr[A(\text{Ideal}_0) = 1]| < \text{neg}$$

Suppose that there exists some PPT A for some nonnegligible ε such that:

$$|\Pr[A(\text{Real}_0) = 1] - \Pr[A(\text{Ideal}_0) = 1]| > \varepsilon$$

Define $D_{m_0}(y) = A(y \oplus m_0)$.

Then:

$$\begin{aligned}\Pr[D_{m_0}(U_\ell) = 1] &= \Pr[A(U_\ell \oplus m_0) = 1] \\ &= \Pr[A(\text{Ideal}_0) = 1] \\ &= \Pr[D_{m_0}(G(U_n)) = 1] \\ &= \Pr[A(G(U_n) \oplus m_0) = 1] \\ &= \Pr[A(\text{Real}_0) = 1]\end{aligned}$$

$$|\Pr[D_{m_0}(U_\ell) = 1] - \Pr[D_{m_0}(G(U_n)) = 1]| > \varepsilon$$

Which contradicts the definition of a PRG, and therefore such an A cannot exist.

Back to the proof

$$\begin{aligned}&|\Pr[A(\text{Real}_0) = 1] - \Pr[A(\text{Real}_1) = 1]| \\ \leq &|\Pr[A(\text{Real}_0) = 1] - \Pr[A(\text{Ideal}_0) = 1]| \\ + &|\Pr[A(\text{Ideal}_0) = 1] - \Pr[A(\text{Ideal}_1) = 1]| \\ + &|\Pr[A(\text{Ideal}_1) = 1] - \Pr[A(\text{Real}_1) = 1]|\end{aligned}$$

which is $\text{neg} + 0 + \text{neg}$.

3.4 Intuition

We've shown that PRGs are secure, and that one-time pads are secure. However, we haven't shown that a PRG even exists! We'll focus on one-way functions that imply the existence of PRGs.

Informal definition $x \mapsto f(x)$ is easy, but $f(x) \mapsto f^{-1}(f(x))$ is hard on average. Intuitively, we assume that such functions exist.

Notably, a PRG must be a OWF:

$$x \mapsto G(x)$$

which is easy, but this should be hard:

$$G(x) \mapsto x$$

Notably, if we map 2^n length keys into a space of 2^{2n}, the image is at most 2^n, which implies the existence of a naive decider that with likelihood $1 - 2^{-n}$ is correct, which is our epsilon.

References

[1] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition.* Chapman & Hall/CRC, 2nd edition, 2014.