Cryptography
Lecture 3

Lecture by Dr. Mor Weiss
Typeset by Steven Karas

2019-03-19
Last edited 18:13:46 2019-03-19

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 Perfect secrecy

We will provide an alternative defition of perfect security, and discuss the tradeoff between computational complexity and security.

A cryptosystem is a 3-tuple of (G, E, D) where G is a key generation algorithm $k \leftarrow^R G$, E is the encryption function $c \leftarrow^R E(k, m)$, and D is the decryption function $m \leftarrow D(k, c)$.

1.1 Definition: Perfect Indiguishability

(G, E, D) satisfies perfect indistinguishability if for $\forall m_o, m_1 \in \mathcal{P}$ and $k \leftarrow^R G$, it holds that:

$$\forall c \in \mathcal{C} \quad \Pr[E(k, m_0) = c] = \Pr[E(k, m_1) = c]$$

Note that we do not set the randomness of E, and we can consider it to be part of the key for the purposes of this definition.

Example: One-time pad Let $m_0, m_1 \in \{0,1\}^l$ and a ciphertext $c \in \{0,1\}^l$. Note that $k_0 = m_0 \oplus c$ and $k_1 = m_1 \oplus c$. However, we selected the key $G : k \leftarrow^R \{0,1\}^l$ with uniform probability, so this holds perfect security.

1.2 Shannon Security

Let M be a distribution over $\mathcal{P}$. Let C be a distribution over $\mathcal{C}$. (G, E, D) satisfies Shannon secrecy with respect to M if $\forall m \in \mathcal{P}$ and $\forall c \in \mathcal{C}$:

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

In other words, knowing the ciphertext gives us no information about the plaintext from all other plaintexts.

1.3 Equivalency

We will show that if (G, E, D) satisfies perfect indistinguishability iff it also satisfies Shannon secrecy.

Perfect indistinguishability implies Shannon secrecy Assume that (G, E, D) satisfies perfect indistinguishability. Recall Bayes' Rule:

$$\Pr[B \mid A] = \frac{\Pr[A \mid B] \Pr[B]}{\Pr[A]}$$

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]}$$

We want to show that $\Pr[C = c \mid M = m] = \Pr[C = c]$

The other direction The full proof can be found in Katz and Lindell[3, Section 2.1]

1.4 Sufficient keyspace

If (G, E, D) is perfect indistinguishability then $|\mathcal{K}| \geq |\mathcal{P}|$

Proof Assume towards negation that $|\mathcal{K}| < |\mathcal{P}|$. Let M be the uniform distribution[1] over $\mathcal{P}$. Let $m_0 \in \mathcal{P}$ and $c \in Supp(E(\cdot, m_0))$ (c such that $\exists k \in \mathcal{K} : E(k, m) = c$). Let $M_c = \{m' : \exists k' D(k', c) = m'\}$ However, $|M_c| = |\mathcal{K}| < |\mathcal{P}|$.

$$\Pr[M = m_1 \mid C = c] = 0 \neq \frac{1}{|\mathcal{P}|} = \Pr[M = m]$$

1.5 Statistical distance

Let X, Y be random variables over S. For some decider $D : s \to \{0, 1\}$ for some sample $s \in S$.

$$SD(X, Y) = \max_{D:S\to\{0,1\}} |\Pr[D(X) = 1] - \Pr[D(Y) = 1]|$$

Example: Unfair coins Let X be a fair coin, and Y be an unfair coin that turns up heads with probability 2/3.

Define the decider as:

$$D(s) = \begin{cases} 1 & s = \text{heads} \\ 0 & s = \text{tails} \end{cases}$$

$$SD(X, Y) \geq |\underbrace{\Pr[D(X) = 1]}_{1} - \underbrace{\Pr[D(Y) = 1]}_{2}|$$

$$\begin{aligned} \Pr[D(X) = 1] &= \Pr[D(X) = 1 \mid x = \text{heads}] \cdot \overbrace{\Pr[X = \text{heads}]}^{\frac{1}{2}} \\ &\quad + \Pr[D(X) = 1 \mid x = \text{tails}] \cdot \overbrace{\Pr[D(X) = \text{tails}]}^{\frac{1}{2}} \\ &= \frac{1}{2}\left(\Pr[D(\text{heads}) = 1] + \Pr[D(\text{tails}) = 1]\right) \end{aligned}$$

$$\Pr[D(Y) = 1] = \frac{1}{3}\Pr[D(\text{heads}) = 1] + \frac{2}{3}\Pr[D(\text{tails}) = 1]$$

$$\begin{aligned} SD(X, Y) &\geq \Big|\frac{1}{2}\left(\Pr[D(\text{heads}) = 1] + \Pr[D(\text{tails}) = 1]\right) \\ &\quad - \frac{1}{3}\Pr[D(\text{heads}) = 1] + \frac{2}{3}\Pr[D(\text{tails}) = 1]\Big| \\ &= \ldots = |1/3 - 1/6| = 1/6 \end{aligned}$$

1.6 Statistical secrecy

(G, E, D) satisfies statistical secrecy if $\forall m_0, m_1 \in \mathcal{P}$:

$$SD(E(K, m_0), E(K, m_1)) \leq \varepsilon$$

It is possible to prove that if (G, E, D) is ε-statistically secret then $|\mathcal{K}| \geq (1 - \varepsilon)|\mathcal{P}|$

[1] There is loss of generality, but it is possible to extend this proof to cover any distribution

1.7 Asymptotic security

For some security parameter n, consider a cryptosystem (G, E, D). Let $k \leftarrow G(1^n)$, meaning that we give G an unary input of length n. We want G, E, D to run in $\text{poly}(n) \equiv \exists c\, O(n^c)$ time.

We define our security against all adversaries that run in $\text{poly}(n)$ time and obtain an advantage $\varepsilon = \text{negl}(n)$.

$\varepsilon(n) : \mathbb{N} \to \{0,1\}$ is negligible if $\forall c \exists n_0$ such that $\forall n > n_0, \varepsilon(n) < \frac{1}{n^c}$.

For all future definitions, assume that messages have the same length: $\forall n$ all messages $\mathcal{P}_n$ have the same length.

1.7.1 Asymptotically indistinguishable encryption

Let (G, E, D) be an encryption scheme over $\mathcal{P} = \cup_n \mathcal{P}_n$. (G, E, D) has ε-indistinguishable encryptions if $\forall$ nonuniform probabilistic polytime[2] decider A, $\exists \text{negl}(\varepsilon)$ such that $\forall m_0, m_1 \in \mathcal{P}_n$:

$$\varepsilon \geq |\Pr[A(E(k, m_0)) = 1] - \Pr[A(E(k, m_1)) = 1]|$$

Example: shift cipher Consider the case of a shift cipher. Because the same letter is always shifted the same amount, it follows that given a message of sufficient length (say longer than 26 letters), then we slowly gain a larger advantage.

Example: biased one-time pad

$$G : \forall 1 \leq i \leq n \quad k_i = \begin{cases} 1 & 0.49 \\ 0 & 0.51 \end{cases}$$

$$E(k, m) = k \oplus m$$

Even this small bias very quickly gives an adversary sufficient advantage to be asymptotically insecure

Example:

$$\mathcal{P}_n = \{0,1\}^{2n}$$

$$G : \text{pick } k \leftarrow^R \{0,1\}^n;\ \text{output } k$$

$$E(k, m) : \text{pick } i_1, \ldots, i_{2n} \leftarrow^R [n];\ \text{output } (i_1, \ldots, i_{2n}, m_1 \oplus k_{i_1}, \ldots, m_{2n} \oplus k_{i_{2n}})$$

In this case as well, it's sufficient that at least one bit of the key be reused for an adversary to gain an advantage.

Consider $m, m' \leftarrow \{0,1\}^{2n}$:

$$c = (i_1, \ldots, i_{2n}, c_1, \ldots, c_{2n})$$

$$c' = (i_1, \ldots, i_{2n}, c'_1, \ldots, c'_{2n})$$

1.7.2 Concrete indistinguishable encryption

Let (G, E, D) be an encryption scheme over $\mathcal{P}$. (G, E, D) is (t, ε)-secure if $\forall A$ that runs in time $\leq t$ and $\forall m_0, m_1 \in \mathcal{P}$:

$$\varepsilon \geq |\Pr[A(E(k, m_0)) = 1] - \Pr[A(E(k, m_1)) = 1]|$$

2 Next week

Next week we will give an alternative definition of computational security.

[2] hereafter abbreviated PPT

References

[1] Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson. *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd edition, 2001.

[2] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*, volume 1. Cambridge University Press, 2000.

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