CS 127/CSCI E-127: Introduction to Cryptography

Prof. Salil Vadhan | Fall 2013

**Lecture Notes 3:**

**Perfect Secrecy**

**Reading.**

- Katz–Lindell, Chapter 2.
- What does it mean for an encryption scheme to be secure? Some attempts:
  - Adversary can't determine key from ciphertext.
  - Adversary can't determine plaintext.
  - Adversary can't determine any symbol of plaintext.
  - Adversary can't determine "any information" about plaintext.
- **Definition 1 (perfect indistinguishability)** *Encryption scheme satisfies* perfect indistinguishability *if ...*
  - Intuition:
  - Why focus on only two messages?
- **Proposition 2** *Shift and Substitution ciphers do not satisfy perfect indistinguishability for messages of length* $> 1$.

  **Proof:**
- **Proposition 3** *One-time pad satisfies perfect indistinguishability.*

  **Proof:**
- **Definition 4 (Shannon secrecy (called "perfect secrecy" in KL))** *Let $M$ be a distribution on $\mathcal{M}$. An encryption scheme satisfies* Shannon secrecy *with respect to $M$ if ...*

  Intuition:

- **Proposition 5** *An encryption scheme satisfies perfect indistinguishability if and only if it satisfies Shannon secrecy (with respect to any $M$ s.t. $\Pr[M = m] > 0$ for all $m \in \mathcal{M}$). Thus we refer to both as* perfect secrecy *(or* perfect security*).*

  **Proof:** We only prove that perfect indistinguishability implies Shannon secrecy. The converse is Lemma 2.3 in the 1st edition of Katz–Lindell (Exercise 2.4 in the 2nd edition). By Bayes' Law,

  $$\Pr\left[M = m | \mathsf{Enc}_K(M) = c\right] = \frac{\Pr\left[\mathsf{Enc}_K(M) = c | M = m\right] \cdot \Pr\left[M = m\right]}{\Pr\left[\mathsf{Enc}_K(M) = c\right]}$$

  We need to prove that $\Pr\left[\mathsf{Enc}_K(M) = c|M = m\right] = \Pr\left[\mathsf{Enc}_K(M) = c\right]$, i.e. $\Pr\left[\mathsf{Enc}_K(m) = c\right] = \Pr\left[\mathsf{Enc}_K(M) = c\right]$. This follows from perfect indistinguishability. ■

- **Definition 6 (perfect adversarial indistinguishability)** *An encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies* perfect adversarial indistinguishability *if for every adversary $\mathcal{A}$, the probability that $\mathcal{A}$ succeeds in the following "game" is at most* $1/2$*:*

- **Proposition 7** *An encryption scheme satisfies perfect indistinguishability iff it satisfies perfect adversarial indistinguishability.*

- Why isn't this course over?

- **Theorem 8** *If an encryption scheme is perfectly secure, then the number of keys is at least the size of the plaintext space.*

  **Proof:**

- How to get around this limitation? Can we relax the security definition, or does violating perfect secrecy necessarily correspond to a potential attack?

- "Statistical" security: only require encryptions of all messages to be statistically close.

  - Let $X$ and $Y$ be random variables taking values in a set $S$. $X$ and $Y$ are called *statistically $\varepsilon$-indistinguishable* if for every event $T \subseteq S$

    $$\left|\Pr\left[X \in T\right] - \Pr\left[Y \in T\right]\right| \leq \varepsilon.$$

    $T$ is also called a *statistical test.*

  - **Definition 9 (statistical secrecy)** *Encryption scheme satisfies* statistical $\varepsilon$-indistinguishability *if for every two $m_1, m_2 \in \mathcal{M}$, the random variables $\mathsf{Enc}_K(m_1)$ and $\mathsf{Enc}_K(m_2)$ are statistically $\varepsilon$-indistinguishable. (These random variables are taken over $K \xleftarrow{R} \mathsf{Gen}$ and the coin tosses of $\mathsf{Enc}$.)*
  - Intuitively, adversary has probability at most $\varepsilon$ of getting information about the plaintext.
  - Equivalent to allowing a success probability of at most $(1+\varepsilon)/2$ in the adversarial indistinguishability game.
  - Insufficient to go beyond the barrier we have with Shannon secrecy: requires $|\mathcal{K}| \geq (1-\varepsilon) \cdot |\mathcal{M}|$.

- "Computational" security: only protect against adversaries with *limited computational resources*, i.e. efficient adversaries with a reasonable amount of computational power $\Rightarrow$ REST OF THIS COURSE.

- Other communication settings — quantum cryptography, beacon of random bits,...