Cryptography

Lecture 3

Announcements

- HW1 due Wednesday, 2/7 at beginning of class
- Discrete Math Readings/Quizzes due Wednesday, 1/31 @ 11:59pm

Agenda

- Last time:
  - Perfect Secrecy (K/L 2.1)
  - One time pad (OTP) (K/L 2.2)
- This time:
  - Limitations of perfect secrecy (K/L 2.3)
  - Shannon's Theorem (K/L 2.4)
  - The Computational Approach (K/L 3.1)

The One-Time Pad Scheme

1. Fix an integer $\ell > 0$. Then the message space M, key space K, and ciphertext space C are all equal to $\{0,1\}^\ell$.
2. The key-generation algorithm Gen works by choosing a string from $K = \{0,1\}^\ell$ according to the uniform distribution.
3. Encryption Enc works as follows: given a key $k \in \{0,1\}^\ell$, and a message $m \in \{0,1\}^\ell$,output $c := k \oplus m$.
4. Decryption Dec works as follows: given a key $k \in \{0,1\}^\ell$, and a ciphertext $c \in \{0,1\}^\ell$, output $m := k \oplus c$.

Security of OTP

Theorem: The one-time pad encryption scheme is perfectly secure.

$\mathcal{K} = \{0,1\}^\ell \qquad \mathcal{M} = \{0,1\}^\ell$

Gen outputs random $K \xleftarrow{\$} \mathcal{K}$

$Enc(K, m) = K \oplus m$

$Dec(K, c) = K \oplus c$

Perfect Indistinguishability

- Lemma: An encryption scheme (Gen, Enc, Dec) over a message space M is perfectly secret if and only if for every probability distribution over M, every $m_0, m_1 \in M$, and every ciphertext $c \in C$: $\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1]$.

OTP is Perfectly secret

Proof: Fix an arbitrary dist over $\mathcal{M}$

fix $m_0, m_1 \in \mathcal{M}$

fix $c \in \mathcal{C}$

$$\Pr[C=c \mid M=m_0] = \Pr[K \oplus M = c \mid M = m_0]$$ by def of OTP

Using Prob facts:

$$= \frac{\Pr[K \oplus M = c \wedge M = m_0]}{\Pr[M=m_0]} = \frac{\Pr[K \oplus m_0 = c \wedge M = m_0]}{\Pr[M=m_0]}$$ Events are equivalent

Re-writing:

$$= \frac{\Pr[K = m_0 \oplus c \wedge M = m_0]}{\Pr[M=m_0]} = \frac{\Pr[K = m_0 \oplus c] \cdot \Pr[M=m_0]}{\Pr[M=m_0]}$$ by independence

$$= \frac{1}{|\mathcal{K}|} = \frac{1}{2^\ell}$$

by def of Gen; $|\mathcal{K}|$: cardinality (size)

Everything the same for $\Pr[C=c \mid M=m_1] = \frac{1}{2^\ell}$

$\therefore \Pr[C=c \mid M=m_0] = \Pr[C=c \mid M=m_1]$

☑

Proof

Proof: Fix some distribution over M and fix an arbitrary $m \in M$ and $c \in C$. For one-time pad:

$$\Pr[C = c | M = m] = \Pr[M \oplus K = c \mid M = m]$$

$$= \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = \frac{1}{2^\ell}$$

Since this holds for all distributions and all m, we have that for every probability distribution over M, every $m_0, m_1 \in M$ and every $c \in C$

$$\Pr[C = c \mid M = m_0] = \frac{1}{2^\ell} = \Pr[C = c | M = m_1]$$

Drawbacks of OTP

- Key length is the same as the message length.
  - For every bit communicated over a public channel, a bit must be shared privately.
  - We will see this is not just a problem with the OTP scheme, but an inherent problem in perfectly secret encryption schemes.
- Key can only be used once.
  - You will see in the homework that this is also an inherent problem.

$$c_0 = K \oplus m_0$$

$$c_1 = K \oplus m_1$$

$$c_0 \oplus c_1 = m_0 \oplus m_1$$

Limitations of Perfect Secrecy

Theorem: Let (Gen, Enc, Dec) be a perfectly-secret encryption scheme over a message space $\boldsymbol{M}$, and let $\boldsymbol{K}$ be the key space as determined by Gen. Then $|\boldsymbol{K}| \geq |\boldsymbol{M}|$. q

p

Proof by Contradiction: Assume that an enc scheme has $|K| < |M|$. Prove that the scheme is not perfectly secret.

Definition of Perfect Secrecy

- An encryption scheme (Gen, Enc, Dec) over a message space $\boldsymbol{M}$ is perfectly secret if for $\forall$ every probability distribution over $\boldsymbol{M}$, every message $m \in \boldsymbol{M}$, and every ciphertext $c \in \boldsymbol{C}$ for which $\Pr[C = c] > 0$:

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

To show is NOT perfectly secret

$\exists$ dist over $\mathcal{M}$ (Hint: try uniform dist)

$\exists\, m \in \mathcal{M}$

$\exists\, c \in \mathcal{C}$ s.t. $\Pr[M=m \mid C=c] \neq \Pr[M=m]$

Proof. Assume (Gen, Enc, Dec) with $|\mathcal{K}| < |\mathcal{M}|$

Consider the uniform dist over $\mathcal{M}$

Pick any $c \in \mathcal{C}$.

Alg: Brute force search
try $Dec(k, c)$ with every $k \in \mathcal{K}$.
add resulting message to the set $\mathcal{M}(c)$.

$$\mathcal{M}(c) := \{ m' \mid m' = Dec(k, c) \text{ for some } k \in \mathcal{K} \}$$

Claim: $|\mathcal{M}(c)| \leq |\mathcal{K}|$ (justify @ home)

By Assumption: $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}| \rightarrow |\mathcal{M}(c)| < |\mathcal{M}|$.

By logical argument there must be some $m^* \in \mathcal{M}$
but $m^* \notin \mathcal{M}(c)$.

fix the message m^*

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

☑

Proof

Proof (by contradiction): We show that if $|\boldsymbol{K}| < |\boldsymbol{M}|$ then the scheme cannot be perfectly secret.

- Assume $|\boldsymbol{K}| < |\boldsymbol{M}|$. Consider the uniform distribution over $\boldsymbol{M}$ and let $c \in \boldsymbol{C}$.
- Let $\boldsymbol{M}(c)$ be the set of all possible messages which are possible decryptions of c.

$$\boldsymbol{M}(c) \coloneqq \{m' |\, m' = Dec_k(c) for\ some\ k \in \boldsymbol{K}\}$$

Proof

$$\boldsymbol{M}(c) := \{\ m' | m' = Dec_k(c) for\ some\ k \in \boldsymbol{K}\}$$

- $|\boldsymbol{M}(c)| \leq |\boldsymbol{K}|$. Why?
- Since we assumed $|\boldsymbol{K}| < |\boldsymbol{M}|$, this means that there is some $m' \in \boldsymbol{M}$ such that $m' \notin \boldsymbol{M}(c)$.
- But then

$$\Pr[M = m' |\ C = c] = 0 \neq \Pr[M = m']$$

And so the scheme is not perfectly secret.

Shannon's Theorem

Let (Gen, Enc, Dec) be an encryption scheme with message space $\boldsymbol{M}$, for which $|\boldsymbol{M}| = |\boldsymbol{K}| = |\boldsymbol{C}|$. The scheme is perfectly secret if and only if:

1. Every key $k \in \boldsymbol{K}$ is chosen with equal probability $1/|\boldsymbol{K}|$ by algorithm Gen.
2. For every $m \in \boldsymbol{M}$ and every $c \in \boldsymbol{C}$, there exists a unique key $k \in \boldsymbol{K}$ such that $Enc_k(m)$ outputs c.

**Theorem only applies when $|\boldsymbol{M}| = |\boldsymbol{K}| = |\boldsymbol{C}|$.

Example quiz question for Lecture 3 material

- Is the following scheme perfectly secret?
- Message space $\boldsymbol{M} = \{0,1,\ldots,n-1\}$. Key space $\boldsymbol{K} = \{0,1,\ldots,n-1\}$.
- Gen() chooses a key k at random from $\boldsymbol{K}$.
- $\text{Enc}_k(m)$ returns $m + k$.
- $Dec_k(c)$ returns $c - k$.

over int
no modular reduction

Cannot apply Shannon's theorem.
Prove not perfectly secret. Choose $m = 0$.
Consider uniform dist over $\mathcal{M}$.

no key is large enough to produce this ciphertext

$$\Pr[M = 0] = \frac{1}{n} \neq \Pr[M = 0 \mid C = 2n-2] = 0$$

Example quiz question for Lecture 3 material

- Is the following scheme perfectly secret?
- Message space $\boldsymbol{M} = \{0,1,\ldots,n-1\}$. Key space $\boldsymbol{K} = \{0,1,\ldots,n-1\}$.
- Gen() chooses a key k at random from $\boldsymbol{K}$. ✓
- $\mathrm{Enc}_k(m)$ returns $m + k \ mod\ n$.
- $Dec_k(c)$ returns $c - k \ mod\ n$.

We can apply Shannon's Th b/c $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$

Check: $\forall (m, c)$ $\exists$ a unique key k } ✓

$m + k = c \mod n$ $\quad k = (c - m) \mod n$

The Computational Approach

Two main relaxations:

1. Security is only guaranteed against efficient adversaries that run for some feasible amount of time.
2. Adversaries can potentially succeed with some very small probability.