



Chapter 2: Shannon's Theory

COMP 7120-8120
Lih-Yuan Deng
lihdeng@memphis.edu



Shannon's Theory

- Introduction
- Elementary Probability Theory
- Perfect Secrecy
- Entropy
- Properties of Entropy
- Spurious Keys and Unicity Distance
- Product Cryptosystems



Cryptosystem

- Five-tuples: (P, C, K, E, D)
- P : finite set of possible plaintexts
- C : finite set of possible ciphertexts
- K : keyspace, finite set of possible keys
- E : set of $e_k(m)$: encryption $P \rightarrow C$
- D : set of $d_k(c)$: decryption $C \rightarrow P$ such that $d_k(e_k(m)) = m$.



Security of Cryptosystems

- Various common criteria to evaluate security:
 1. Computational security
 2. Provable security
 3. Unconditional security



Computational security

- N = number of operations required for the best breaking algorithm.
 - where N is a specified large number.
- Problem: no known practical cryptosystem can be proved under this definition.
 - In practice, we study some specific attack (e.g. exhaustive key search).
 - security against one attack may not be secure against another attack!



Provable security

- provide evidence of security via reduction.
- the cryptosystem can be broken if some well-known hard problem can be solved.
 - e.g. RSA can be broken if one can easily factor a large integer.
 - no polynomial time algorithm is known.



Unconditional security

- the system cannot be broken, even with infinite computational resources.
 - e.g. Shift or Substitution Cipher that is used for only one (or very few) plaintext in ciphertext only.
 - e.g. Vigenere Cipher with keyword length m , if the key is used for only one plaintext. (one-time pad)



Shift Cipher

- Shift ciphers:
 - $e_k(x) = x + k \pmod{m}$
 - $d_k(y) = y - k \pmod{m}$
 - $k=3$ (Caesar cipher)
- For English alphabets, we can choose $m=26$ and $P=C=K=Z_{26}$.
 - $A \leftrightarrow 0, B \leftrightarrow 1, \dots, Z \leftrightarrow 25.$
 - $Z_m = \{0, 1, 2, \dots, m-1\}.$



Security and theory of cryptosystems

- Attack models (?) should be considered for any security discussion.
 - a cryptosystem can be secure under one type of attack model but highly insecure under another attack model.
 - e.g. ?
- We will develop theory of unconditional security against ciphertext-only attack.

Elementary Probability Theory

- X : discrete random variable.
- $\Pr[x] = \Pr[\mathbf{X}=x]$ = probability of \mathbf{X} taking the value x .
- Properties of Probability:
 1. $0 \leq \Pr[x] \leq 1$.
 2. $\sum \Pr[x] = 1$.
 3. $\Pr(E) = \sum_{x \in E} \Pr[x]$, E : event.

Example 2.1

- Toss a pair of dice.
- Random variable (vector) $\mathbf{Z} = (Z_1, Z_2)$ taking possible values:
 $\{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$.
- Event S_i = sum of Z_1 and Z_2 is i
 - $S_4 = \{(1,3), (2,2), (3,1)\}$
 - $\Pr[S_4] = \Pr[Z_1 + Z_2 = 4] = 1/12$.
- $\Pr[S_i] = ?$ $i=2,3,\dots, 11, 12$.

Independence between X, Y

- \mathbf{X} and \mathbf{Y} be two random variables.
- $\Pr[x,y] = \Pr[\mathbf{X}=x, \mathbf{Y}=y]$ be the joint probability.
- \mathbf{X} and \mathbf{Y} are **independent** if and only if $\Pr[x,y] = \Pr[x] \Pr[y]$ for all x and y .
 - $\mathbf{Z} = (Z_1, Z_2)$ in Example 2.1 are independent. [show!]
- See Definition 2.2 (page 47)



Conditional Probability

- Let A and B be two events. We define $P(A|B) = P(A \text{ and } B)/P(B)$.
- $\Pr[x|y] = \Pr[x,y]/\Pr[y]$
- $\Pr[X=x|Y=y] = \Pr[X=x \text{ and } Y=y] / \Pr[Y=y]$
- If X and Y are independent if and only if $\Pr[x|y] = \Pr[x]$.



More Conditional Probability

- Recall $\Pr[x|y] = \Pr[x,y]/\Pr[y]$
- Another variation:
 - $\Pr[x,y] = \Pr[x|y] \Pr[y]$
 - $\Pr[x,y] = \Pr[y|x] \Pr[x]$
- Bayes' Theorem: (page 48)
 - $\Pr[x|y] = \Pr[y|x] \Pr[x]/\Pr[y]$.



Bayes' Theorem

- $\Pr[x|y] = \Pr[y|x] \Pr[x]/\Pr[y]$.
 - $\Pr[y] = \sum_x \Pr[x',y] = \sum_x \Pr[y|x'] \Pr[x']$
- Common application in cryptosystem:
 - $\Pr[X=x]$ = probability distribution of plaintext.
 - $\Pr[K=k]$ = probability of choosing key=k over a key space.
 - $\Pr[x|y] = \Pr[X=x|Y=y]$ = probability of plaintext X=x given ciphertext Y=y.

Example 2.3 (page 49)

- Plaintext= $\{a,b\}$
- Ciphertext= $\{1,2,3,4\}$
- Key space= $\{K_1, K_2, K_3\}$
- $\Pr[a]=1/4, \Pr[b]=3/4$
- $\Pr[K_1]=1/2, \Pr[K_2]=\Pr[K_3]=1/4$.
- Encryption matrix as given:

	a (1/4)	b (3/4)
K_1 (1/2)	1	2
K_2 (1/4)	2	3
K_3 (1/4)	3	4

Example 2.3 (page 49)

- $\Pr[1] = \Pr[X=a, K=K_1] = 1/2 \times 1/4 = 1/8$.
- $\Pr[2] = 1/2 \times 3/4 + 1/4 \times 1/4 = 7/16$.
- $\Pr[3] = 1/4 \times 3/4 + 1/4 \times 1/4 = 4/16$.
- $\Pr[4] = 1/4 \times 3/4 = 3/16$.

	a (1/4)	b (3/4)
K_1 (1/2)	1	2
K_2 (1/4)	2	3
K_3 (1/4)	3	4

Example 2.3 (page 49)

$\Pr[a 1]=\Pr[a,1]/\Pr[1]=\Pr[a, K_1]/(1/8) = 1.$	$\Pr[b 1]=\Pr[b,1]/\Pr[1]=0.$
$\Pr[a 2]=1/7$ (show!)	$\Pr[b 2]=6/7$
$\Pr[a 3]=1/4$	$\Pr[b 3]=3/4$
$\Pr[a 4]=0$	$\Pr[b 4]=1$

	a (1/4)	b (3/4)
K_1 (1/2)	1	2
K_2 (1/4)	2	3
K_3 (1/4)	3	4

Perfect Secrecy

- A cryptosystem has perfect secrecy if $\Pr[x|y]=\Pr[x]$ for all $x \in P$ and $y \in C$.
- Given ciphertext y will not change the distribution of plaintext x .
- Posterior distribution=prior distribution
- X and Y are independent.

Shift cipher and perfect secrecy

- Theorem 2.3 (page 51).
- Choose **one** letter $X=x$ with any probability distribution $\Pr[x]$ and
- choose key $K=k$ with **equal** probability distribution $\Pr[K=k]=1/26$.
- The, $y = e_k(x) = x + k \text{ mod } 26$ will have
- $\Pr[x|y]=\Pr[x]$ (perfect secrecy)

Perfect Secrecy Example

- Plaintext= $\{a,b,c\}$
- Ciphertext= $\{1,2,3\}$
- Key space= $\{K_1, K_2, K_3\}$
- $\Pr[a]=1/7, \Pr[b]=2/7, \Pr[c]=4/7$.
- $\Pr[K_i] = 1/3, i=1,2,3$.
- Encryption matrix as given: (shift cipher)

	a (1/7)	b (2/7)	c (4/7)
K_1 (1/3)	1	2	3
K_2 (1/3)	2	3	1
K_3 (1/3)	3	1	2



Perfect Secrecy Example

- Show that $\Pr[X]=\Pr[X|Y]$ for any x and y .
- e.g. $\Pr[X=a]=1/7$. Need show
 - $\Pr[X=a|Y=i]=1/7, i=1,2,3$.
- $\Pr[Y=1]=\Pr[X=a, K=K_1]+ \Pr[X=c, K=K_2]+ \Pr[X=b, K=K_3]$.
- $\Pr[Y=1]=\Pr[X=a] \PrK=K_1]+ \Pr[X=c] \PrK=K_2]+ \Pr[X=b] \PrK=K_3] = 1/3$. (show!)
- Uneven distribution of X into uniform distribution of Y !!!

	a (1/7)	b (2/7)	c (4/7)
K_1 (1/3)	1	2	3
K_2 (1/3)	2	3	1
K_3 (1/3)	3	1	2



Imperfect Secrecy Example Example 2.3 (page 49)

$\Pr[a 1]=\Pr[a,1]/\Pr[1]=1.$	$\Pr[b 1]=\Pr[b,1]/\Pr[1]=0.$		a (1/4)	b (3/4)
$\Pr[a 2]=1/7$	$\Pr[b 2]=6/7$	K_1 (1/2)	1	2
$\Pr[a 3]=1/4$	$\Pr[b 3]=3/4$	K_2 (1/4)	2	3
$\Pr[a 4]=0$	$\Pr[b 4]=1$	K_3 (1/4)	3	4



Condition for perfect secrecy

- Shift cipher may have perfect secrecy if $P=C=K$ and we choose $k \in K$ with equal probability, $1/|K|$.
- Reason: the encryption matrix become a "Latin square" (any row and any column in the square matrix has exactly one symbol). [See ex 2-2 (page 70)]

More on Condition for perfect secrecy

- If $P=C=K$ and we choose $k \in K$ with equal probability, $1/|K|$.
- Theorem 2.4 (page 52). Any other cipher will have perfect secrecy if the encryption matrix is a "Latin square".
- Show $\Pr[Y=i]=1/3$, for $i=1,2,3$ in both cases.

	a	b	c
K_1	1	2	3
K_2	2	3	1
K_3	3	1	2
	a	b	c
K_1	1	3	2
K_2	2	1	3
K_3	3	2	1

More on shift cipher and perfect secrecy

- If a **new random** key is used for every plaintext character, then the shift cipher is "unbreakable".
- However, if the **same** key is used for every plaintext character, then the shift cipher is very easy to "break".
- One-time pad is a well-known realization of perfect secrecy.

One-time Pad [Vernam cipher]

- Similar to Vigenere cipher, except the key stream is used **only once**.
- Cryptosystem 2.1 is a binary version.
 - $P=C=K=(\mathbb{Z}_2)^n$
 - keyword $\mathbf{k} = (k_1, k_2, \dots, k_n)$
 - plaintext $\mathbf{x} = (x_1, x_2, \dots, x_n)$
 - ciphertext $\mathbf{y} = (y_1, y_2, \dots, y_m)$
 - $e_k(x_i) = x_i + k_i \pmod{2}$,
 - $d_k(y_i) = y_i - k_i \pmod{2}$



Vigenere cipher

- Encrypt m characters at a time.
- $P=C=K=(\mathbb{Z}_{26})^m$
- keyword of length m : $\mathbf{k} = (k_1, k_2, \dots, k_m)$
- plaintext of length m : $\mathbf{x} = (x_1, x_2, \dots, x_m)$
- ciphertext of length m : $\mathbf{y} = (y_1, y_2, \dots, y_m)$
- $e_k(x_i) = x_i + k_i \pmod{26}$, $i = \text{'position'}$
- $d_k(y_i) = y_i - k_i \pmod{26}$



On the One-time Pad

- Key space is **at least as large** as its plaintext space.
- Same key cannot not be used **twice**. (why not ?) it can be broken easily with known-plaintext attack. (how?)
- a new key has to be generated and transmitted over a **secure** channel.
- used in military or diplomatic context.



Summary

- Various criteria to evaluate security of cryptosystem
- Random Variable and probability distribution
- Conditional probability
- Independence between random variables
- Bayes' Theorem
- Perfect Secrecy
- One-time pad.
