Grade evaluation

If you do not submit at least two reports after the 8th lecture, then you will NOT have evaluation (credit is not given).

The score will be twice the sum of report scores.

You can increase score by submitting the optional report, in which you give answers to selected exercises in

Michael A. Nielsen and Isaac L. Chuang, “Quantum Computation and Quantum Information,” ISBN: 0521635039.

和訳: 量子コンピュータと量子通信〈1〉　〈３〉, ISBN: 4274200094, 4274200086, 4274200094

You can freely choose exercises in Chapter 2 or later. Each correct answer increases the final score by two.

2009-12-1

Complete proof of the quantum key distribution

I will give a sketch of the complete proof of the quantum key distribution introduced by R. Renner in

R. Renner. Security of quantum key distribution. *International Journal on Quantum Information*, 6(1):1–127, Feb. 2008. (originally published as Ph.D thesis, ETH Zürich, Switzerland, 2005). arXiv:quant-ph/0512258, doi:10.1142/S0219749908003256

His proof is a natural extension of the information theoretical key agreement introduced by Maurer:

U. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory*, 39(3):733–742, May 1993. doi:10.1109/18.256484

Therefore, I will first review the information theoretical key agreement.

The papers with “arxiv” can be downloaded from http://arxiv.org, and “doi” from http://dx.doi.org

2009-12-2

Probability distribution

Let X_i be a random variable whose values belong to a finite set $\mathscr{X}$. The joint probability for the event that X_i takes the value $x_i \in \mathscr{X}$ for $i = 1, \ldots, n$ is denoted by

$$\Pr[X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n].$$

This joint probability will be abbreviated as

$$P_{X_1 \cdots X_n}(x_1, \ldots, x_n).$$

The joint probability $P_{X_1 \cdots X_n}(x_1, \ldots, x_n)$ **cannot** generally written as the product

$$P_{X_1}(x_1) \times \cdots \times P_{X_n}(x_n),$$

where $P_{X_i}(x_i)$ is the probability distribution of X_i. If the distribution of $(X_1, \ldots, X_n)$ is written as the above product form, it is said to be *statistically independent*.
Assume $(X_1, \ldots, X_n)$ are statistically independent. Additionally, if there exists a function $Q : \mathscr{X} \to [0, 1]$ such that $P_{X_i}(x_i) = Q(x_i)$ for all $i = 1, \ldots, n$, then $(X_1, \ldots, X_n)$ are said to be *i.i.d. (identically and independently distributed)*.

Sattelite model

Suppose that there are legitemate users Alice and Bob, and the eavesdropper Eve. Suppose also that Alice, Bob and Eve receive signals from a common sattelite (or wireless LAN access point) from time 1 to n. Such received signals can be mathematically described as random variables.

X_i: Alice's signal at time i

Y_i: Bob's signal at time i

Z_i: Eve's signal at time i

If the signal transmission and the reception processes are the same for all $i = 1, \ldots, n$, then (X_i, Y_i, Z_i) is i.i.d., that is, There exists $Q : \mathscr{X} \times \mathscr{Y} \times \mathscr{Z} \to [0,1]$ such that

$$P_{X_1 \ldots X_n Y_1 \ldots Y_n Z_1 \ldots Z_n}(x_1, \ldots, x_n, y_1, \ldots, z_n) = \prod_{i=1}^{n} Q(x_i, y_i, z_i).$$

Note that (X_i, Y_i, Z_i) is dependent on each other.

We assume the existence of authenticated public channel between Alice and Bob with which Eve can listen all of the content. Alice and Bob want to share a common secret random string by conversation over the public channel. Notice the similarity to the BB84 protocol, with which existence of the public channel is assumed.

Security criterion

Suppose that Alice and Bob produced common string S_n from $X^n = (X_1, \ldots, X_n)$ and $(Y_1, \ldots, Y_n)$. They want S_n to be secret from Eve. Mathematically, this can be formulated that S_n and Z^n are statistically independent. Consider the following joint probability distribution:

$A \setminus E$	a	b
a	0.2	0.3
b	0.2	0.3

Then the above is a statistically independent probability distribution, because

$$\Pr[A = u, E = v] = \Pr[A = u] \times \Pr[E = v]$$

for all $u \in \{a, b\}$ and $v \in \{a, b\}$. Observe also that knowing the value of E does not help guessing the value of A.

Suppose that Eve knows $E = a$. Since

$$\Pr[A = a | E = a] = \Pr[A = b | E = a] = 0.5,$$

Eve knows nothing about the value of A. The situation is the same for $E = b$.

Consider the following joint probability distribution:

$A \setminus E$	a	b
a	0	0.5
b	0.5	0

Then the above is a statistically dependent probability distribution, because

$$\Pr[A = u, E = v] \neq \Pr[A = u] \times \Pr[E = v]$$

for some $u \in \{a, b\}$ and $v \in \{a, b\}$. Observe also that knowing the value of E allows one to determine the value of A.

Suppose that Eve knows $E = a$ (or b). Then she knows $A = b$ (or a) with certainty.

Mutual information and statistical independence

Mutual information is a concept used in the information theory developed by Claude Shannon in 1948. Some of you should have learnt that concept in the undergraduate course “通信理論” in the department of computer science.

The mutual information of two random variables A and E is defined by

$$I(A;E) = \sum_{a,e} \Pr[A = a, E = e] \log_2 \frac{\Pr[A = a, E = e]}{\Pr[A = a] \times \Pr[E = e]}.$$

Observe that the statistical independence of A and E implies $\Pr[A = a, E = e] = \Pr[A = a] \times \Pr[E = e]$ for all a and e and $I(A;E) = 0$.

Consider the following joint probability distribution:

$A \setminus E$	a	b
a	0.2	0.2
b	0.3	0.3

Then $I(A;E) = 0$.

On the other hand, consider the following joint probability distribution:

$A \setminus E$	a	b
a	0	0.5
b	0.5	0

$I(A;E) = 1$.

If $I(A;E)$ is close to zero, then A and E are **almost** statistically independent.

We can ensure the security if the mutual information is close to zero.

Family of two-universal hash functions

Let T_1, T_2 be two finite sets, and $\mathscr{F}$ be a set of mappings from T_1 to T_2. If for all $x \neq x' \in T_1$ we have

$$\frac{|\{f \in \mathscr{F} \mid f(x) = f(x')\}|}{|\mathscr{F}|} \leq \frac{1}{|T_2|},$$

then $\mathscr{F}$ is called a family of two-universal hash functions.

In other words, $\mathscr{F} \ni f$ rarely maps two different elements in T_1 to the same element in T_2.

For $n \geq m$, the set of all linear maps from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$ is a family of two-universal hash functions.

Family of two-universal hash functions

Recall that Alice and Bob want to make a secure key S_n statistically independent from Eve's information Z^n. For simplicity let's assume $X^n = Y^n$ (we remove this assumption in the next lecture.)

To do this, Alice randomly choose $f \in \mathscr{F}$, inform the choice of f to Bob, and the key is obtained as $S_n = f(X^n)$. Let $\mathscr{S}_n$ be the range of the function f. Then S_n is a random variable taking values in $\mathscr{S}_n$.

If the length of key S_n is shorter, i.e. $|\mathscr{S}_n|$ is smaller, then more information is lost by application of f to X^n. Thus, if key is shorter, S_n and Z^n become statistically more independent. The question is: How much we have to shorten X^n? To answer this question, I introduce the conditional entropy.

Conditional Entropy

The conditional entropy of a random variable A conditioned on another random variable E is defined by

$$H(A|E) = -\sum_{a,e} \Pr[A = a, E = e] \log_2 \Pr[A = a | E = e].$$

Consider the following joint probability distribution:

$A \setminus E$	a	b
a	0.2	0.3
b	0.2	0.3

Then $H(A|E) = 1$. Assume that Eve has E and Alice has A. In this example, from Eve's point of view, the value of A is ambiguous to Eve.

On the other hand, consider the following joint probability distribution:

$A \setminus E$	a	b
a	0	0.5
b	0.5	0

$H(A|E) = 0$. In this example, from Eve's point of view, the value of A is completely unambiguous to Eve.

The conditional entropy $H(A|E)$ quantitatively measures Eve's ambiguity on Alice's information A.

2009-12-11

Privacy Amplification Theorem

Recall that

X^n: Alice's information

Y^n: Bob's information

Z^n: Eve's information

$X^n = Y^n$ is assumed for simplicity

Goal: Compute $S_n = f(X^n)$ statistically independent of Z^n.

Theorem: Let $\mathscr{F}$ be a family of two-universal hash functions from $\mathscr{X}^n$ to $\mathscr{S}_n$. If n is sufficiently large and $\log_2 |\mathscr{S}_n|/n < H(X|Z)$ then for almost all $f \in \mathscr{F}$, $I(f(X^n); Z^n)$ is almost zero.

The above theorem shows how we can make secret key from X^n.

Exercise

Submit your answer to the box in front of Room 311, S3 building, by 17:00 Thursday, if you don't finish by 12:10.

1. List all the linear maps from $\mathbf{F}_2^2$ to $\mathbf{F}_2$.

2. Write whether or not the set of maps in Problem 1 is a family of two-universal hash functions, and also write the reason.

3. Let X_1, X_2 be i.i.d random variables, and $Z = X_2$. Write the joint probability distribution $P_{X_1X_2Z}$.

4. Compute $I(X_1, X_2; Z)$ and $H(X_1, X_2|Z)$. We are regarding X_1, X_2 as a single random varialbe in I and H.

5. Identify a linear map f from $\mathbf{F}_2^2$ to $\mathbf{F}_2$ such that $I(f(X_1, X_2); Z) = 0$.

6. If your answers to the previous exercises were evaluated as incorrect, please indicate whether or not you agree to that evaluation. Write which part in today's lecture was difficult for your understanding.