QIP Course 12: QKD and key agreement by using the wireless communication

Ryutaroh Matsumoto

Nagoya University

September 2019

Acknowledgment and Copyright

Sketch of omplete proof f 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.

Satellite 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 satellite (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 $i = 1, ..., n$, then (X_i, Y_i, Z_i) is i.i.d., that is, there exists $Q : \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} \to [0, 1]$ such that

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

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

Public channel

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 $X^n = (X_1, ..., X_n)$ and $(Y_1, ..., Y_n)$. 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 $E = b$.

Contrasting insecure example

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

Mutual information of the previous examples

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.

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 $H(A|E) = 1$, which indicates that Eve has 1-bit ambiguity about Alice's information A.

No ambiguity of the insecure example

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

$H(A|E) = 0$, which indicates that Eve has no ambiguity about Alice's information A.

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

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 $\mathcal{F}$ be the family of all the additive (or linear when $\mathcal{X}^n$ and $\mathcal{S}_n$ are linear spaces) functions from $\mathcal{X}^n$ to $\mathcal{S}_n$, where a function f is said to be additive if $f(\vec{x} + \vec{y}) = f(\vec{x}) + f(\vec{y})$ for all $\vec{x}, \vec{y}$. If n is sufficiently large and $\log_2 |\mathcal{S}_n|/n < H(X|Z)$ then for almost all $f \in \mathcal{F}$, $I(f(X^n); Z^n)$ is almost zero.

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

Exercise

1. List all the additive functions from $\mathbf{F}_2^3$ to $\mathbf{F}_2$. Note: $\mathbf{F}_2^3$ is NOT $GF(8)$.
2. Let X_1, X_2 be i.i.d uniform random variables, and $Z = X_2$. Write the joint probability distribution $P_{X_1X_2Z}$ for all 8 values $(x_1, x_2, z) \in \mathbf{F}_2^3$.
WRONG answer: Since $X_2 = Z$, $P_{X_1X_2} = P_{X_1X_2Z}$.
$P_{X_1X_2}$ takes TWO arguments while $P_{X_1X_2Z}$ does THREE. Thus, they cannot be the same function.
3. 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.
4. Identify **all the** additive maps f from $\mathbf{F}_2^2$ to $\mathbf{F}_2$ such that $I(f(X_1, X_2); Z) = 0$.

Data Compression

Conventional Data Compression: X^n can be compressed to $nH(X)$ bits. (Draw a figure.)

Distributed Data Compression:

- There exists another information source Y^n correlated to X^n.
- Decompressor can exploit Y^n to restore X^n from the compressed data.
- Compressor cannot see Y^n.
- (Draw a figure)

Y^n improves the compression rate from $H(X)$ to $H(X|Y)$.

Implementation of Distributed Data Compression

$\vec{x}$: n-bit string to be compressed
M: $nH(X|Y) \times n$ sparse binary matrix

$M\vec{x}$ is the compressed data

$\vec{x}$ can be efficiently recovered with high probability from $\vec{y}$ and $M\vec{x}$ by the so-called belief propagation algorithm.

Application to key agreement

Recall the situation in the key agreement. (Draw a figure)
In order to make Y^n identical to X^n, do the following

1. Alice sends MX^n.
2. Bob recoveres X^n from MX^n and Y^n.

The process of making Y^n identical to X^n is called the information reconciliation.

The amount of secret key

If $X^n = Y^n$ and we do not do information reconciliation, we can extract $nH(X|Z)$ bits of secret key from X^n by applying a hash function.

However, $nH(X|Y)$ bits of information is leaked over public channel in information reconciliation.

We have to shrink the number of bits in the result of hash functions to $n(H(X|Z) - H(X|Y))$ from $nH(X|Z)$ in order to compensate the information leakage. If the length of secret key is $\leq n(H(X|Z) - H(X|Y))$, then the secret key is almost statistically independent of (Z^n, MX^n).

Correspondence to BB84

X^n: the information possessed by the sender Alice (not discarded nor announced)
Y^n: the information possessed by the receiver Bob (not discarded nor announced)
Z^n: content of eavesdropper's quantum memory, all noises in quantum channel is assumed to be caused by eavesdropping.

The original BB84 explained in the first lecture does not work with channel noise. Information reconciliation and privacy amplification make the BB84 usable with channel noise.

Difference between the QKD and the satellite model

The largest problem in the ordinary key agreement is that Alice and Bob must know P_{XYZ} in order to compute $H(X|Z)$, but P_{XYZ} is often unavailable because estimation of P_{XYZ} needs cooporation by the eavesdropper Eve (Why does Eve cooporate with Alice and Bob??).

In contrast to this, in the BB84, any eavesdropping causes noise in the quantum channel. P_{XYZ} can be known by Alice and Bob by watching channel noise in the quantum channel between Alice and Bob.

Actual protocols

- model the quantum channel between Alice and Bob as an i.i.d. (independently and identically distributed) channel, and
- estimate the channel by using the disclosed information in Step 7 of BB84 (see Unit 1) as pilot symbols for the channel estimation.

Answers to Exercise

1. List all the additive maps from $\mathbf{F}_2^3$ to $\mathbf{F}_2$. Note: $\mathbf{F}_2^3$ is NOT $GF(8)$.
Answer was given on blackboard at the last lecture.

2. Let X_1, X_2 be i.i.d uniform random variables, and $Z = X_2$. Write the joint probability distribution $P_{X_1X_2Z}$ for all 8 values $(x_1, x_2, z) \in \mathbf{F}_2^3$.
WRONG answer: Since $X_2 = Z$, $P_{X_1X_2} = P_{X_1X_2Z}$.
$P_{X_1X_2}$ takes TWO arguments while $P_{X_1X_2Z}$ does THREE. Thus, they cannot be the same function.
The answer will be given on the blackboard.

3. 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.
Answer: $I(X_1, X_2; Z) = 1$, and $H(X_1, X_2|Z) = 1$
4. Identify **all the** additive maps f from $\mathbf{F}_2^2$ to $\mathbf{F}_2$ such that $I(f(X_1, X_2); Z) = 0$.
There are three correct answers: $f(X_1, X_2) = 0$ (which is useless to generate a secret key), $f(X_1, X_2) = X_1 + X_2$, and $f(X_1, X_2) = X_1$.
In every case of f, Eve has no information on $f(X_1, X_2)$.