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. The deadline of the optional report is July 31.

2009-13-1

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 $H(X|Y)$.

Realization of Distributed Data Compression

$\vec{x}$: n-bit string to be compressed
H_1: $nH(X|Y) \times n$ sparse binary matrix

$H_1\vec{x}$ is the compressed data

$\vec{x}$ can be efficiently recovered with high probability from $\vec{y}$ and $H_1\vec{x}$ 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 H_1X^n.

2. Bob recoveres X^n from H_1X^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 $(Z, H_1 X^n)$.

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.

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.