Topics in this course

Applications of quantum mechanics to

- computation,
- communication, and
- cryptography.

Specifically,

- Quantum cryptography
- Quantum teleportation
- Superdense coding
- (Quantum algorithm for prime factorization)
- (Quantum error-correcting code)
- ...

Your understanding of quantum mechanics **IS NOT** required.

Grade evaluation (成績評価)

Exercises will be given after each lecture. Grade evaluation is given according to those exercises.

You can submit an optional report when score is below 60 and you want the course credit.

Exercises are given after every lecture. Please bring A4 papers.

You can ask questions in Japanese. If you don't know an English word (e.g. polarization), feel free to ask it.

Quantum Key Distribution (QKD) protocols

Goal: Distant two persons (Alice and Bob) share a secret common random bit string, while Eve (an adversary) can eavesdrop all of their communication.

Shared random bits allow completely secure communication (by the one-time pad).

Advantage of QKD protocols

- The security of QKD protocols relies only on the correctness of the postulates in the quantum mechanics.

- That of many conventional cryptographies (e.g. RSA, ElGamal, etc.) relies on the conjectured difficulty of certain computational problems. (e.g. integer factorization)

$\Longrightarrow$ QKD protocols seem more secure than conventional ones.

Disadvantages of QKD protocols

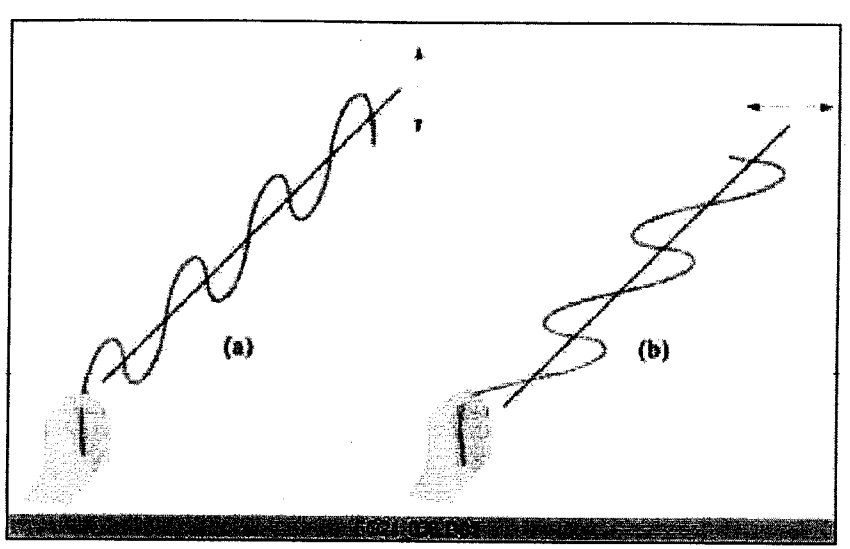
Expensive and slow (with the current technologies)

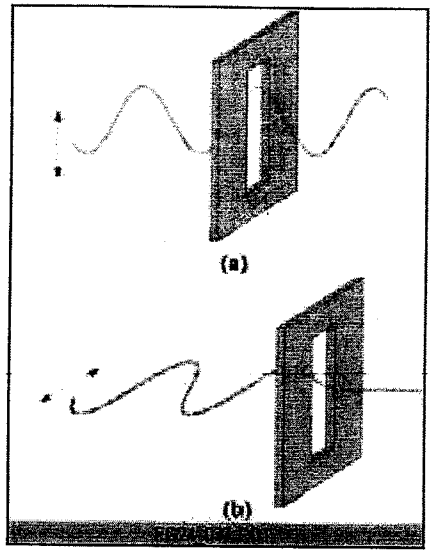
A prototype QKD machine (recently built by NEC)

- costs 100,000 USD.
- shares bits with 60 M bits/sec.
  over a 16 kilometer existing optical cable.

Polarization

Transverse waves that vibrate in a plane are called plane-polarized waves.
Horizontally polarized waves cannot pass through a vertical slit.





← passed

← absorbed

For light, the polarization plane is defined as the plane in which the electric field vibrates.

Light intensity is decreased unless polarization and slit are parallel.

Photon

Light is regarded as a collection of particles, called photons.

What happens if a polarized photon is going through a slit?

Photon polarization and slit

polarization	slit	probability of pass	new polarization
	|	1	|
|	/	0.5	/
	—	0	no photon
	|	0.5	|
/	/	1	/
	—	0.5	—

45 degree slanted

QKD protocol 1 — transmission of photons

1. Alice (the sender) generates the random bits.

2. She encodes the bits to photon polarization,

bit	0	1
rule 1	—	|
rule 2	/	\

where the encoding rules 1 and 2 are randomly selected.

QKD protocol 2 — reception of photons

3. Bob (the receiver) guesses the transmitted bits by the pass/absorption of photons by slits,

slit	pass/absorption	bit
—	passed	0
	absorbed	1
/	passed	0
	absorbed	1

where two directions of slits are selected randomly for each photon.

Relation between the encoding rule and the slit direction

encoding rule	original bit	polarization	slit	prob. of pass	guessed bit
+ or ×	0	+	+	1	0
	1	×		0	1
+ or ×	0	+	/	0.5	random
	1	×		0.5	random

When Bob uses / slit, he cannot guess the transmitted bit with probability 1, and his guessed bit has nothing to do with the transmitted bit.

Encoding rule and slit direction 2

encoding rule	original bit	polarization	slit	prob. of pass
/ or \	0	/	−	0.5
	1	\		0.5
/ or \	0	/	/	1
	1	\		0

While the slit − works good with the encoding rule "− or |", it does not work with "/ or \".

QKD protocol 3

4. Alice and Bob publicly announces their encoding rules and slit directions used for all bits.

5. They discard bits at which the encoding rule and the slit direction are incompatible and the transmitted bit has nothing to do with the guessed bit by Bob.

© The remaining bits of Alice and Bob should be the same unless photons are eavesdropped.

Simple eavesdropping strategy

Eve (the adversary) eavesdrops part of photons as follows:

1. Randomly select — or / slit for each eavesdropped photon.
2. Measure each polarization by the selected slit, and guess the encoded bit.
3. If the photon passes the slit, Eve sends it to Bob as it is. Otherwise she sends the polarization perpendicular to the slit.

Change of polarization by eavesdropping

Alice's polarization	Eve's slit	received polarization
— or |	/	/ or \
/ or \	—	— or |

The wrong choice of eavesdropping slit makes differences between the transmitted bits and the received bits. (with probability 0.5)

QKD protocol 4 — Detection of the eavesdropper

6. Alice and Bob publicly announce the half of bits not discarded at Step 5.

If there is a difference between bits, then they abort the protocol.

Problems in the simple QKD protocol

- It is assumed that polarizations do not change during transmission.
- Eve's strategy is assumed to be a very simple one. However, she can do whatever she likes on photons. E.g., she can try to copy polarizations and measure them after Alice and Bob finish the QKD protocol.
- Eve can successfully eavesdrop a single bit with probability $\frac{1}{8}$ without being noticed.

Exercise

Submit your answer to the box in front of the room 311 of the S3 bldg. before 17:00 Thursday. Please write your name, student number, and your department (名前と学籍番号と専攻を書いて下さい)

Suppose that eight photons are sent and four of them are eavesdropped as below.

sent photons	ー	|	／	＼	ー	|	／	＼
eavesdropping slit		ー		ー		／		／
receiver slit	ー	／	ー	／	ー	／	ー	／
photons publicly announced in Step 6				○				○

1. Which photons are discarded at Step 5? (Japanese translation：どの光子がステップ 5 で破棄されるか？)
2. Write a possible measurement outcome (pass or apsorption) in Step 3 of not discarded photons in Step 5. The correct answer is not unique. (Japanese

trans.: ステップ 5 で破棄されなかった光子についてステップ 3 でスリットを通過したかしないか答えよ。正しい解答は一つではない。)
3. Write the guesses by Bob at transmitted bits in Step 3 according to your answer to Q2. (ステップ 3 の Bob による送信ビットの推定値を問 2 にたいする答えにしたがって書け)
4. With the answer of Problem 2, can you detect the eavesdropper? Answer with yes or no and write the reason. (問 2 に対する答えに対して、盗聴者を検出できるか否か「はい」か「いいえ」で答え、理由を述べよ)
5. Assume that the eavesdropper is undetected and the protocol is not aborted. What are shared secret common random bits? Sender's bits and receiver's may be different because of eavesdropping. (盗聴者を検出せずプロトコルを中止しなかったと仮定する。送受信者で共有されるビット列を答えよ。)
6 (Optional). Write which part of today's lecture is difficult for you. How well did you understand quantum mechanics and linear algebra? What topic do you want to be included in this lecture? Write comments on this lecture, if any. (今日の授業で理解困難な部分はどこか？線形代数と量子力学をどの程度理

解しているか？どのような話題をこの講義で聞きたいか？何か他に今日の授業にコメントが有れば書いて下さい)