

QIP Course 1: Qunatum Key Distribution

Ryutaroh Matsumoto

Nagoya University, Japan

Send your comments to ryutaroh.matsumoto@nagoya-u.jp

August 2019

@ Tokyo Tech.

The slides include a figure from the <http://openstaxcollege.org/>.
Materials presented here can be reused under the Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by/4.0>.



About this lecture

Applications of the quantum mechanics to communication and computation are explained. Specifically,

- 1 Quantum key distribution
- 2 Basics of QIP (quantum information processing)
- 3 Quantum teleportation
- 4 Quantum superdense coding
- 5 Matrix expression of quantum state, and partial trace
- 6 Interpretation of the elementary probability theory as a commutative special case of the quantum theory
- 7 Quantum factorization algorithm breaking the RSA public key cryptosystem
- 8 Refuting the local realism view of the universe
- 9 Homeworks for getting the course credit

will be covered. If there is spare time, I will also cover

- 10 Quantum error-correcting (really tough! only for someone needs QEC)

About this lecture 2

Understanding of QIP requires one to do lots of computations **by your hand!**

⇒ Time for solving exercises is included in this lecture.

Without solving exercises, your NON-understanding is certain.

Understanding of QIP only comes through mathematics and computation.

↑ Why?

Our intuition and of the reality is optimized for the classical macroscopic physics, for survival reason.

So everything in QIP is **counter-intuitive**. Only math (and experiments) can uncover its nature.

Grade evaluation will be done by several small questions given on the final day. You need to submit answers of them. Normal exercises (during the lecture) will not be used for grade evaluation.

Your questions

You can ask questions **any time**.

You are also welcome to take photos of the blackboards by smartphones.

I assume that you are familiar with linear algebra using complex numbers. If you are new to complex linear algebra, you are welcome to give questions when you get lost.

The slides are prepared for those who has **complete 100%** understanding of linear algebra taught in the undergraduate using real numbers. I am not sure if this is a right assumption. If you need to review linear algebra, you are welcome to request the lecturer to do so.

Course schedule

10:45–16:35 (270 minutes), August 26, 2019

10:45–16:35 (270 minutes), August 30, 2019

10:45–16:35 (270 minutes), September 2, 2019

10:45–16:35 (270 minutes), September 3, 2019

10:45–16:35 (270 minutes), September 9, 2019.

This is a Ph.D course, so non-Ph.D students might not be able to get a course credit. Please contact the university administration if you have any question about your eligibility of getting the course credit.

Warning for professional mathematicians

Quantum mechanics is connected to the mathematics (at least) as follows:

Quantum state: a vector $|\varphi\rangle$ in separable complex Hilbert space \mathcal{H}

Observable: A self-adjoint operator A on \mathcal{H}

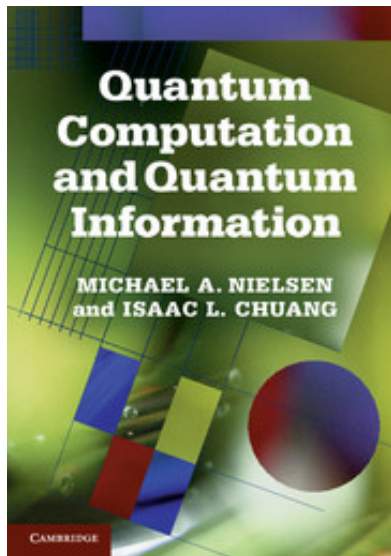
When A is measured, the measurement outcome λ (eigenvalue of A) is obtained with a probability $\|P_\lambda|\varphi\rangle\|^2$, where P_λ is the projection onto the eigenspace belonging to λ .

The above gave motivations for studying the spectrum of operators, various kinds of operator algebras, etc.

Warning: **BUUUUT**

- In this course, \mathcal{H} is assumed to be **finite-dimensional**, which is sufficient for explaining the results in this course.
- First two units may include lots of reviews on linear algebra, which is **boring** to professionals.

Suggested textbook



Quantum Computation and Quantum Information




ISBN: 9780511985249

The course is a subset of the suggested textbook.

Quantum Information Processing (2019) 18:116
<https://doi.org/10.1007/s11128-019-2234-5>



Entanglement-assisted quantum error-correcting codes over arbitrary finite fields

Carlos Galindo¹  · Fernando Hernando¹  · Ryutaroh Matsumoto^{2,3}  ·
Diego Ruano⁴ 

Received: 11 December 2018 / Accepted: 25 February 2019 / Published online: 4 March 2019
© The Author(s) 2019

Abstract

We prove that the known formulae for computing the optimal number of maximally entangled pairs required for entanglement-assisted quantum error-correcting codes (EAQECCs) over the binary field hold for codes over arbitrary finite fields as well. We also give a Gilbert–Varshamov bound for EAQECCs and constructions of EAQECCs coming from punctured self-orthogonal linear codes which are valid for any finite field.

Purpose of this unit in the lecture

- Introduce concrete quantum phenomenon by using the BB84 quantum key distribution protocol as an example.
- Allow the audience to judge if this lecture is interesting/useful/worth studying.

There is NO math in this unit.

One-time pad

M : message to be sent secretly

K : a key secretly shared between Alice and Bob

$M \oplus K$ is sent over a public channel (\oplus : bit-wise exclusive-or)
public = anyone can see the transmitted contents

Eve can see $M \oplus K$ on the public channel but cannot guess M .
(draw a figure here)

⇒ Shared secret random bit string enables secure communication.

Goal and assumptions of the quantum key distribution (QKD) protocols

Goal: Sharing a random bit string secretly between Alice and Bob in presence of an adversary Eve

Assumptions (draw a figure):

- Authenticated public channel (transmitted contents are visible by everyone, but they cannot be forged or modified).
- Quantum channel with which Eve can do everything possible within the quantum mechanics

Advantages of QKD protocols

- The security of QKD protocols rely only on the correctness of the postulates in quantum mechanics.
- That of many conventional cryptographies (e.g. RSA) rely on the conjectured difficulty of certain computational problems (e.g. integer factorization).

⇒ QKD protocols remain secure even after a quantum computer is built, or after a faster integer factorization algorithm is found.

Disadvantages of QKD protocols

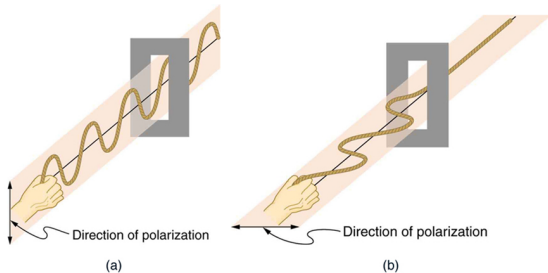
Slow Up to 100 Mbits/second.

Expensive At least 100K US\$.

Limited in distance A direct optical link without a repeater is necessary, which limits the distance between Alice and Bob ≤ 200 kilometers.

Polarization of light and slit

- Light (and electromagnetic wave) is vibration of electric field, whose direction of the vibration is orthogonal to the path of light.
- The direction of vibration is called **polarization** of light.
- Light intensity is decreased when light is passing through a slit.
- When the angle between polarization and a slit is 45 degree, the light intensity becomes half.
- The light passing through a slit has the same polarization as the slit direction.



©OpenStax College, excerpted from <http://cnx.org/contents/>

Light is a wave while it is a collection of particles!!!(?) A single particle of light is called a **photon**.

Q: What happens if single photon tries to pass through a slit whose direction differs by 45 degree with the photon polarization.

A: It passes with a probability 0.5.

It passes with a probability 1 (resp. 0) if they are parallel (resp. orthogonal).

BB84 Protocol 1

BB84 = Bennett & Brassard 1984

The original version is presented today, which assumes a error-free channel. It modern improvements can work with channel noise.

- 1 Alice generates the random bits.
- 2 She encodes each bit to a photon polarization by

bit	0	1
rule 1	–	
rule 2	/	\

where the encoding rules 1 &2 are chosen randomly for each bit, and / and \ denote 45-degree slanted polarizations.

- 3 For each photon, Bob randomly choose – or / slit, and see if the photon passes through the chosen slit.
- 4 He guesses the transmitted bits as follows:

slit	pass	absorption
–	0	1
/	0	1

Wrong choices of slits

- The horizontal slit gives no information about the transmitted bit if the encoding rule 2 is used.
- The diagonal slit gives no information about the transmitted bit if the encoding rule 1 is used.

Why? Explain what happens on the blackboard.

- 5 Alice and Bob publicly announces their encoding rules and slits used for all bits.
- 6 They discard bits at which
 - encoding rule 1 and slit / are used, or
 - encoding rule 2 and slit – are used,because Bob has NO useful information (see the last page).

Simple eavesdropping strategy

For Eve to obtain information, she can use the following tactics (draw a figure):

- 1 For each eavesdropped photon, randomly choose $-$ or $/$ slit.
- 2 Try to pass the photon to the chosen slit, and guess the bit by using the same rule as Bob.
- 3 When the photon is absorbed, she needs to inject the photon so that the number of received photons by Bob remains the same. When $-$ slit absorbed the photon, she sends $|$ polarization to Bob. When $/$ slit absorbed the photon, she sends \backslash polarization to Bob.

When

- Alice's encoding rule 1, Bob's slit $-$ and Eve's slit $/$ are used, or
- Alice's encoding rule 2, Bob's slit $/$ and Eve's slit $-$ are used,

Eve's measurement is detected with a probability 0.5 for that photon, **if Alice and Bob compare Alice's transmitted bit and Bob's guess.**

Why? (Draw a figure on a blackboard).

- 7 Alice and Bob publicly announce the half of the bits not discarded at Step 6. If there is single difference between their bits, then they abort the protocol and restart the protocol from the beginning.

Problems in the simple QKD protocol

- It is assumed that polarizations do not change over the channel.
- 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 into her storage and measure them **AFTER** Alice announces her encoding rules for all photons. Proving the security under such a scenario is much more difficult (but possible).
- Alice and Bob cannot decrease the average number of bits seen by Eve to almost zero.

Example similar to the exercise given later

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

sent photons	—		/	\	—		/	\
eavesdropping slit		—		—		/		/
receiver slit	—	/	—	/	—	/	—	/
photons publicly announced in Step 7				yes				yes

1. Which photons are discarded at Step 6?
2. Write a possible measurement outcome (pass or absorption) in Step 3 of not discarded photons in Step 6. The correct answer is not unique.
3. Write the guesses in Step 4 by Bob for transmitted bits according to your answer to Q2.
4. With the answer of Q2, can you detect the eavesdropper? Answer with yes or no and write the reason.

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. Also note that the bits disclosed in Step 7 cannot be secret.

Exercise (20–30 min.): Repeat Q1–5 with the below

Please discuss them with other students. You are also welcome to talk with the lecturer.

sent photons	–			\	–		/	\
eavesdropping slit		–		–		/		–
receiver slit	–	/	–	/	–	/	–	/
photons publicly announced in Step 7					yes			yes