Quantum communications course 2022: written part of the exam

One of these tasks will be randomly assigned to you to be completed at home over a week or so. We expect an extensive, analytical written treatment of the questions asked, using all the material in the course and, possibly, additional sources. Please use drawings and tables where appropriate.

The examiner may subsequently ask you questions about your written answer.

A1

Compare quantum cryptography with classical (mathematical) cryptography. What are the advantages and disadvantages / limitations of each?

The worldwide economic investment into quantum key distribution has probably exceeded a milliard euro by now. This level of expenditure goes far beyond an academic curiosity. Why are the governments (in at least some countries) and industry so much interested in the commercialisation and practical use of this technology, given its today's limitations? Explain the motivations that drive this technology development.

(Note that A1 is a difficult question that will require you to seek additional information outside the course, especially about the modern cryptography, and form your own justified opinion.)

A2

Explain the threat model in (a) point-to-point quantum key distribution and (b) quantum key distribution networks of different types. I.e., what parts of the system and network, what knowledge and technology do we assume an adversary has and has not access to? What the adversary can and cannot do to the equipment and communication lines (according to our security model's assumptions)?

Pick one attack attempt that fails (e.g., leads to a QBER above the threshold) and one hacking attack based on an implementation imperfection that succeeds. Make a detailed list of resources and knowledge the adversary uses in the execution of each attack.

(Note that in A2, you should think like an engineer designing the eavesdropping equipment. Your answer should not be at a conceptual level, but rather be a complete list of technical and engineering requirements.)

A3

Compare free-space and fiber QKD realisations. Discuss advantages, disadvantages, and challenges of each transmission medium. Give numerical values of important parameters for fiber and free-space optical transmission lines and discuss how they impact QKD.

A4

List <u>all</u> uses of entanglement in experimental quantum communication you know from this course. In each case, explain what advantages the use of an entangled photon source imparts or why it is essential for the protocol, device, or scheme.

A5

Explain the principle of an optical Trojan-horse attack. Give an example of adversary's scheme for remote readout of a phase modulator inside the system and explain how it measures the phase.

What other modulator parameters can Eve read (in various schemes you know from this course)?

List all QKD schemes and protocols you know from this course. Discuss whether each of them is vulnerable to the Trojan-horse attack or not. If it is vulnerable, what is required to protect it and how technologically difficult would it be to implement the protection?

A6

In some QKD implementations, Alice needs to randomly choose and send four polarisation states (↕, ↔, ⤢, ⤡) of single photons or attenuated laser pulses. Draw schemes of at least three different optical source types that can be used to prepare these polarisation states.

Discuss which hacking attacks you know from this course may be applied to each source scheme.

A7

Where are the losses in a free-space link?

In a prepare-and-measure QKD scheme, Alice starts by attempting to prepare random states at a high rate. By the time Bob detects Alice's photons, only few get detected, owing to various losses and component imperfections. The post-processing of Bob's raw detection data reduces if further. The resulting secret key passed to an application has a much lower rate than Alice's initial bit rate at the time of preparing the states.

Assume the optical scheme is a ground-to-satellite free-space link.

List all the individual losses and inefficiencies in QKD, both in the optical scheme and the post-processing. Give a typical numerical value or a range of values of each loss component.

Assuming Alice has a 1 Gbit/s random state source, estimate the final secret key rate based on your above analysis. Make plausible assumptions on component and link parameters.

A8

Where are the losses in a fiber link?

In a prepare-and-measure QKD scheme, Alice starts by attempting to prepare random states at a high rate. By the time Bob detects Alice's photons, only few get detected, owing to various losses and component imperfections. The post-processing of Bob's raw detection data reduces if further. The resulting secret key passed to an application has a much lower rate than Alice's initial bit rate at the time of preparing the states.

Assume the channel between Alice and Bob consists of the standard single-mode optical fiber.

List all the individual losses and inefficiencies in QKD, both in the optical scheme and the post-processing. Give a typical numerical value or a range of values of each loss component.

Assuming Alice has a 1 Gbit/s random state source, estimate the final secret key rate based on your above analysis. Make plausible assumptions on component and link parameters.

A9

Explain a general scheme for quantum teleportation.

Draw and explain the scheme of a particular ground-to-satellite quantum teleportation experiment in [J.-G. Ren *et al.,* Nature **549**, 70 (2017)]. While you can simplify the scheme from this paper, it's important to show all the steps that process photons.

Now, suppose an adversary with unlimited space-flying capabilities (i.e., can place optics anywhere in the beam between the ground station and satellite) wants to attack this particular experimental implementation to learn all the quantum states that get teleported and registered in the satellite, without raising a suspicion and leaving any trace in the experimental data. Can she do this using a bright-light detector control attack on the satellite? Why?

If you conclude that such attack is possible, draw a scheme of the adversary's optical and electronic equipment and explain how it would work.

A10

Which attacks based on equipment imperfections that you know from this course are in principle applicable to the twin-field QKD scheme [M. Lucamarini *et al.,* Nature **557**, 400 (2018)], and which attacks are not? List all the attacks and explain why each is applicable or not.

Pick one attack that might work. Draw a scheme of Eve's equipment and explain Eve's step-by-step protocol of executing this attack on the twin-field QKD system.

B1

What is the difference between pure and mixed quantum states? Provide mathematical description of both. How one can convert a pure state into a mixed one and vice versa? Provide an optical scheme to do this task.

B2

How can one use different degrees of freedom of a single photon to transmit quantum information? Show examples of QKD protocols (e.g., BB84) based on temporal, spatial, and phase encoding/decoding.

B3

Consider a potentially existing faster-than-light communication setup based on entanglement. Which physical principles this setup violates? What would happen if these principles turn out to be not legit?

B4

How can one perform a measurement in the Bell basis? How to distinguish between either three out of four Bell states? How to distinguish between all four Bell states?

B5

How can one prove that the source of light is a true single photon source? Design an optical setup and provide its mathematical description to do this task.

B6

Explain how QKD can make use of Bell inequality. Consider examples of Ekert 1991 (E91) and Bennett-Brassard-Mermin 1992 (BBM92) protocols. If they are not covered in the course then, well, search for additional literature.

B7

Are single photons absolutely necessary for QKD? Can one use other optical states for this purpose? What are the main advantages and disadvantages of the “non-single-photon” QKD protocols?

B8

Imagine you want to establish QKD over 1000 km long optical fiber. What protocols and principal components do you need? Explain how your setup should work.