Course Syllabus

Quantum Cryptography

Index

1. Introduction

How can you tell a secret when everyone is able to listen in? In this course, you will learn how to use quantum effects, such as quantum entanglement and uncertainty, to implement cryptographic tasks with levels of security that are impossible to achieve classically. This interdisciplinary course is an introduction to the exciting field of quantum cryptography, developed in collaboration between QuTech at Delft University of Technology and the California Institute of Technology.

Prerequisites: this course assumes a solid knowledge of linear algebra and probability at the level of an advanced undergraduate. Basic knowledge of elementary quantum information (qubits and simple measurements) is also assumed, but if you are completely new to quantum information additional videos are provided for you to fill in any gaps.

Back to index

1.1. Learning objectives

By the end of this course you will:

- Be armed with a fundamental toolbox for understanding, designing and analyzing quantum protocols.
- Understand quantum key distribution protocols.
- Understand how untrusted quantum devices can be tested.
- Be familiar with modern quantum cryptography – beyond quantum key distribution.

Back to index

1.2. Course activities and resources

This is a 10 week course with an estimated workload of 6 to 8 hours per week, holding several learning activities and educational resources for you to study. The course is organized in a consistent way so you know what to expect in each week.

- **Video modules**. Each module consists of 2-3 video lectures. The first video will be an introduction, while the others will give you additional examples or work out something in more detail.
- **Quizzes**. Each video module is followed by a graded quiz.

- **Homework**. Pen and paper exercises.
- **Julia Labs**. Interactive notebook with which you can explore and perform calculations.
- **Lecture notes**. Providing more details and examples.

In Week 6 we will release the task **Programming a quantum network** (peer review assignment), where you have to submit your work and give feedback to your peers. Note that the homework of week 8 is optional and there is therefore no points to be earned from these exercises but one set of homework is droppable so your score is not affected by this.

Back to index

1.3. What we expect from you

As an online student we expect you to be an active participant, contributing to a positive atmosphere by questioning, sharing and helping out others using the discussion forum.

Quizzes, Homework and Julia Labs have only one final deadline. However, we recommend you complete these activities on a weekly basis and that you keep on track in order to benefit from learning within a community.

This course is meant to be a place where you learn with and from others. In this sense, we'd like you to experience collaboration and peer-feedback, so please make sure you follow with other participants in order to enrich the overall learning experience.

When communicating with your fellow learners and course team using Askalot make sure you take into account the Communication and Collaboration guidelines.

Back to index

1.4. What you can expect from us/the course team

The course team will release the weekly content, send important announcements, monitor and answer questions on a regular basis using the discussion forum. We'll try to have a daily presence, but as you might understand we cannot promise to quickly attend everyone, due to the thousands of learners participating in this course. But we'll do our best ;-)

Back to index

2. Course structure & Release Dates

Week 0. A crash course in quantum information (optional)

- What are quantum bits - qubits?
- Combining qubits using the tensor product
- Measuring qubits
- Performing operations on qubits
- The Bloch Sphere representation

Week 1. From essential tools to the first quantum protocol (12th November)

- Density matrices
- Encrypting (quantum) bits: the classical and quantum one time pad
- Combining density matrices using the tensor product
- Classical-quantum states
- Generalized measurements
- The partial trace

Week 2. The power of entanglement (19th November)

- What is quantum entanglement?
- Purification and Uhlman's theorem
- The Schmidt Decomposition
- Sharing a classical secret using entangled quantum states
- Verifying entanglement using a Bell test
- Monogamy of entanglement

Week 3. Quantifying information (26th November)

- What it means to be ignorant: ideal case
- Trace distance and its use in security definitions
- The (min)-entropy including the smooth min-entropy
- Uncertainty principles: simple version BB84
- Extended UR principles: tripartite version

Week 4. From imperfect information to (near) perfect security (3rd December)

- Privacy amplification
- Randomness extractors
- Randomness extraction using two-universal hashing
- The pretty-good measurement

Week 5. Distributing keys (10th December)

- Introduction to key distribution
- Key distribution with a limited Eve and perfect Bob

- Key distribution with noise on the channel

Guest video: David Elkouss (QuTech) – Practical error correction in key distribution protocols

Week 6. Quantum key distribution protocols (17th December)

- Quantum key distribution: definitions and concepts
- BB84 states and Six states
- BB84 Protocol
- Purifying protocols using entanglement
- Security from a guessing game
- Authentication

Guest video: Nicolas Gisin (University of Geneva) – Quantum key distribution in practice

Week 7. Quantum cryptography using untrusted devices (7th January)

- Device-independent quantum cryptography
- Testing devices using a Bell experiment
- Security of device-independent quantum key distribution against collective attacks
- Security against general attacks

Guest video: Ronald Hanson (QuTech, TU Delft) – The first loophole free Bell experiment

Week 8. Quantum cryptography beyond key-distribution (14th January)

- Secure Function Evaluation

- Oblivious transfer - the universal gate of cryptography
- Bit commitment
- Impossibility of bit commitment
- Coin flipping

Week 9. Perfect security from physical assumptions (21st January)

- Evading impossibility
- The noisy storage model
- Bit commitment in the noisy-storage model
- Security from quantum uncertainty
- A universal primitive: weak string erasure

Week 10. Further topics (28th January)

- Position verification
- Quantum computing in the cloud

Back to index

3. Assessment & Deadlines

To complete this course you have to score at least **60 points** of the total mark of 100. The different components count towards the total mark as:

- Quizzes - 10%
- Homework - 60%
- Julia Labs - 20%
- Programming a quantum network (peer review assignment) - 10%

Deadline for Quizzes, Homework and Julia Labs: Deadlines for quizzes, homework and labs will be 14 days after the material is released, i.e. Sunday at 23:59 UTC. See each week for exact date.

Deadlines for Peer Review Assignement:

1. Submit your assignment: 23:59 UTC, January 20, 2019

1. Review your peers: 23:59 UTC, January 30, 2019

Back to index

4. Resources & Tools

All educational resources will be available in the course. They consist of short videos and lecture notes with additional details and examples to support you in the completion of the weekly learning activities: quizzes, homework and labs.

Julia notebooks

Every week has an interactive Julia notebook activity. Julia is a very easy language to perform computations, and we will use it to explore quantum cryptography and to gain intuition. Check out the *Getting started > Julia Lab Exercises* page in the course for detailed information on how to setup and use Julia notebooks.

Back to index

5. Certificate

If you're interested in a certificate you can upgrade to a Verified Certificate. These certificates will indicate you have successfully completed the course, but will not include a specific grade. Certificates will be issued by edX under the name of Caltech and DelftX, designating the institutions from which the course originated.

Generating an ID verified certificate

Verified certificates will be issued a few days after the end of the course, to all participants who achieved at least 60% of the total grade. Certificates can be downloaded from your Student Dashboard (look for the Download button next to the name of our course).

Remember that in order to qualify for a certificate, you must achieve a **total grade of 60% or higher**. You can check your grade at any time under the course's Progress page. An ID verified Certificate of Achievement is available for $50. You can Upgrade on your edX Dashboard to Verified during the course.

Once produced, a certificate cannot be reissued, hence it is very important that you verify the way in which your name appears. Check that, in your edx.org account, your name is correctly spelled, since it will appear on the final certificate. Please note that no Honor Code certificates will be given out by edX for this course.

Back to index

***

LICENSE

***

Click the button to print the course syllabus.

Print course syllabus