Exam Format

- Wednesday 1st May 2024; 13:00-15:00 (UK time)
- “Notes Permitted, calculators permitted”. You can have 3-pages of A4 notes (6 sides).
- Simplify expressions when possible (but no need for exact numerical values without calculator).
- Choose Two Questions out of Three
- Each Question has many sub-questions. Read Carefully all parts before deciding
- In each question there is varying difficulty in the sub-questions. Marks of each sub-part are stated
- Choose “strategically”. E.g. differently if aiming for max marks Vs aiming to pass Vs aiming for 70-ish
Contacts for questions:

- For Lectures: Petros, petros.wallden@ed.ac.uk and Mina mdoosti@ed.ac.uk
- For Tutorials: Piazza (or TA Marine, marine.demarty@ed.ac.uk)

Material:
- 'Course Materials' tab in opencourse.inf.ed.ac.uk or Learn page
- Slides (links in the Schedule)
- Videos (links in the Lecture Recordings Learn page)

Very important to be able to solve these (or similar) questions

Assignment (link in the Schedule). Q1 & Q2 Solutions (and marks) will be released later (when all SC extensions have passed)

Past exam paper (years 2019-2020, 2021-2022, 2022-2023) (format of exams has changed back and forth)

Next: Go through each Lecture.
Contacts for questions:

- For Lectures: Petros, petros.wallden@ed.ac.uk and Mina mdoosti@ed.ac.uk
- For Tutorials: Piazza (or TA Marine, marine.demarty@ed.ac.uk)

Material: @ ‘Course Materials’ tab in opencourse.inf.ed.ac.uk/qcs or Learn page

- Slides (links in the Schedule).
- Videos (links in the Lecture Recordings Learn page)
- Tutorials (links in the Schedule). Very important to be able to solve these (or similar) questions
- Assignment (link in the Schedule). Q1 & Q2
  Solutions (and marks) will be released later (when all SC extensions have passed)
- Past exam paper (years 2019-2020, 2021-2022, 2022-2023) (format of exams has changed back and forth)
Contacts for questions:
- For Lectures: Petros, petros.wallden@ed.ac.uk and Mina mdoosti@ed.ac.uk
- For Tutorials: Piazza (or TA Marine, marine.demarty@ed.ac.uk)

Material: @ ‘Course Materials’ tab in opencourse.inf.ed.ac.uk/qcs or Learn page
- Slides (links in the Schedule).
- Videos (links in the Lecture Recordings Learn page)
- Tutorials (links in the Schedule). Very important to be able to solve these (or similar) questions
- Assignment (link in the Schedule). Q1 & Q2
  Solutions (and marks) will be released later (when all SC extensions have passed)
- Past exam paper (years 2019-2020, 2021-2022, 2022-2023) (format of exams has changed back and forth)

Next: Go though each Lecture.
Quantum Information Background (L2 and L4 - L7 and L19)

- **Main source**: Slides & Textbook (Nielsen and Chuang)
- What is needed for later (especially things needed for solving questions in Tutorials or Lectures)
Main source: Slides & Textbook (Nielsen and Chuang)

What is needed for later (especially things needed for solving questions in Tutorials or Lectures)

Lecture 2 and Lecture 4 - 7:

- Basics: e.g. Notation, Pure states, Density Matrices and Mixed States (ensembles), Expectation Values (see Tutorials)
- Measurements
- Operations/ Quantum Channels (Unitary and CPTP maps)
- Composite Systems: Tensor Products (how to act on such states), Partial Trace, Entanglement, Reduced Density Matrix
- Closeness of Quantum States: Fidelity (able to compute when one state is pure), Trace-Distance and Relations (be able to bound Trace-Distance using Fidelity). See also Tutorials
- Elements of (Classical/Quantum) Information Theory: Classical and Quantum Entropies (focus on what is used in QKD lectures and Tutorials – be able to compute those).
Main source: Slides & Textbook (Nielsen and Chuang)

What is needed for later (especially things needed for solving questions in Tutorials or Lectures)

Lecture 19:

- Theorems and Implications: Know the basic quantum properties (indistinguishability, no-cloning, monogamy of entanglement, teleportation) and what these mean for crypto.
- Not essential to know the proofs of all statements.
Main Source: Slides & ‘Advances in Quantum Cryptography’

Main idea and task of QKD
Main Source: Slides & ‘Advances in Quantum Cryptography’

Main idea and task of QKD

Classical Post-Processing (Information Reconciliation, Privacy Amplification – same for all protocols)
Main Source: Slides & ‘Advances in Quantum Cryptography’

Main idea and task of QKD

Classical Post-Processing (Information Reconciliation, Privacy Amplification – same for all protocols)

A number of different QKD protocols: (BB84, Six-State, B92, BBM92, E91) and related Wisner’s quantum money and quantum coin-flipping.

What each protocol (Actions of Alice, Bob, communication, differences w.r.t. BB84).
Quantum Key Distribution and Related (L3 and L8 - L11)

- Main Source: Slides & ‘Advances in Quantum Cryptography’
- Main idea and task of QKD
- Classical Post-Processing (Information Reconciliation, Privacy Amplification – same for all protocols)
- A number of different QKD protocols: (BB84, Six-State, B92, BBM92, E91) and related Wisner’s quantum money and quantum coin-flipping.
- What each protocol (Actions of Alice, Bob, communication, differences w.r.t. BB84).
- Be able to compute key-rate (when expression is given, or an attack is described – see Tutorial Examples)
- Be able to use Quantum Info background when required (e.g. Unitary/CPTP maps, measurements, Von Neuman entropy, Conditional Entropies, expectation values, CHSH inequalities)
Main Source: Slides

Secure Two-Party Functionalities (L12)

- What it means, understanding of SMPC
- Basic primitives. Oblivious Transfer (security; importance of OT). Bit Commitment (Binding, Concealing)
- Impossibility of classical and quantum BC (information theoretic). Example of wrong protocol (and why it fails).
- Maths: Schmidt decomposition (in Lo-Chau & Mayers Thm)

Quantum Encryption (L12). Correctness and security – avg. ciphertext. QOTP example. [Maths: Decomposition of matrices to Pauli's, commutations, be able to compute the quantum ciphertext and the average quantum ciphertext]

Authentication of Quantum Messages (L10). Correctness. TQAS example. [Maths: Be able to produce Auth given input state and keys.]
Lecture 12 and Lecture 13

- **Main Source:** Slides

- **Secure Two-Party Functionalities** (L12)
  - What it means, understanding of SMPC
  - Basic primitives. Oblivious Transfer (security; importance of OT). Bit Commitment (Binding, Concealing)
  - Impossibility of classical and quantum BC (information theoretic). Example of wrong protocol (and why it fails).
  - Maths: Schmidt decomposition (in Lo-Chau & Mayers Thm)

- **Quantum Encryption** (L12). Correctness and security – av. ciphertext. QOTP example. [Maths: Decomposition of matrices to Pauli’s, commutations, be able to compute the quantum ciphertext and the average quantum ciphertext].
Lecture 12 and Lecture 13

- **Main Source**: Slides

- **Secure Two-Party Functionalities** (L12)
  - What it means, understanding of SMPC
  - Basic primitives. Oblivious Transfer (security; importance of OT). Bit Commitment (Binding, Concealing)
  - Impossibility of classical and quantum BC (information theoretic). Example of wrong protocol (and why it fails).
  - Maths: Schmidt decomposition (in Lo-Chau & Mayers Thm)

- **Quantum Encryption** (L12). Correctness and security – av. ciphertext. QOTP example. [Maths: Decomposition of matrices to Pauli’s, commutations, be able to compute the quantum ciphertext and the average quantum ciphertext].

- **Authentication of Quantum Messages** (L10). Correctness and security. TQAS example. [Maths: Be able to produce Auth_k given input state and keys. ]
Main Source: Slides (q-algorithms also Textbook)

Intro and Quantum Access to Classical protocols (L15)
- Quantum Algorithms abilities. Basic Q-algorithms: able to read a quantum circuit
- Quantum Access to Classical protocols
  - Simpler/harder to implement quantum access
  - Turn classical function to Unitary
  - (Quantum) Random Oracle
  - Example: Quantum Access to OT (check circuit and claim)
Post-Quantum Cryptography (L15, L17-L18)

- **Main Source:** Slides (q-algorithms also Textbook)
- **Intro and Quantum Access to Classical protocols** (L15)
  - **Quantum Algorithms** abilities. Basic Q-algorithms: able to read a quantum circuit
  - **Quantum Access to Classical protocols**
    - Simpler/harder to implement quantum access
    - Turn classical function to Unitary
    - (Quantum) Random Oracle
    - Example: Quantum Access to OT (check circuit and claim)
- **Lattice-based Crypto: General and Regev’s** (L17)
  - LWE versions and SVP versions (and relations)
  - Regev’s Public-Key Encryption Schemes: KeyGen; Enc; Dec; Correctness; intuition for security (and reductions).
  - Be able to work out simple examples (see tutorial).
- **Lattice-based Crypto: NTRU** (L18)
  - NTRU Public-Key Encryption Schemes: KeyGen; Enc; Dec; Correctness; intuition for security.
  - Be able to work out simple examples (see lecture).