Quantum Cyber Security
Lecture 1: Introduction

Petros Wallden

University of Edinburgh

14th January 2025

This Lecture

1. Logistics
2. Motivation: Quantum Computers and Security
3. Quantum Cyber Security: Definition and Course Content

Logistics

Contacts

- **Petros Wallden** (Course Organiser & Lecturer)

  petros.wallden@ed.ac.uk
- Sean Thrasher (TA & Tutor)

  s.thrasher@sms.ed.ac.uk
- Laura Lewis (Tutor)

  l.l.l.lewis@sms.ed.ac.uk

Structure of Course

- Lectures
  - Two per week

    (Tuesday at 11:10 - 12:00; Thursday at 10:00 - 10:50)
  - In-person at: Lister-Learning-and-teaching-centre LLTC 2.3
  - Recoding (and live-streaming) available

- Tutorials
  - Once per week (Group 1 Wednesday 10:00 - 10:50; Group 2 Wednesday 11:10 - 12:00)
  - Two groups (randomly allocated)
  - In-person at: AT 2.07 **MAY CHANGE**
  - **Starts at week 3** (29th January)

- Q& A after classes (altern. contact us via email or at Teams)

Assessment

- Coursework 25%
  - One assignment released 7th March 2025
  - Due at 21st March 2025 (details to follow)
- Exam 75%
  - Two questions to choose out of three
  - Further advice at the revision lecture (last)

Resources

1. **Main textbook** (additional references and resources will be given for each topic if not covered in this):

   "Quantum Computation and Quantum Information"
   by Michael A. Nielsen & Isaac L. Chuang

2. Review paper: Advances in Quantum Cryptography (link here)

3. **Lecture Notes:**
   `https://opencourse.inf.ed.ac.uk/qcs/schedule`.
   Recordings from the Learn page of the course.

4. You can also register at the piazza of the course for questions (mainly for students interactions)

Motivation: Quantum Computers and Security

Quantum Computers

- Quantum Physics is a very successful theory
- Quantum Physics has many **counter-intuitive properties**
- Size of transistors in microchip are approaching quantum scale

Quantum Computers

- Quantum Physics is a very successful theory
- Quantum Physics has many **counter-intuitive properties**
- Size of transistors in microchip are approaching quantum scale

Main Question

Can we built a computer using as **basic information elements quantum systems**, and will this give us **extra power**?

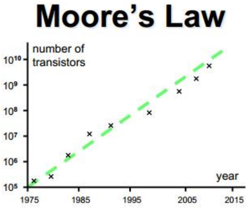
Quantum Computers

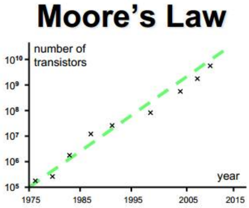
- Quantum Physics is a very successful theory
- Quantum Physics has many **counter-intuitive properties**
- Size of transistors in microchip are approaching quantum scale

Main Question

Can we built a computer using as **basic information elements quantum systems**, and will this give us **extra power**?

- Q: What computational power would a QC have?
- A: Greater than classical probabilistic $\mathrm{BPP} \subseteq \mathrm{BQP}$
- Q: Is it possible to built such computing device?
- A: Yes! No fundamental reason stopping us (engineering)


Moore's Law
number of transistors
10^{10}
10^9
10^8
10^7
10^6
10^5
year
1975
1985
1995
2005
2015



Bit	**Qubit**
Takes values either 0 or 1	Can behave as being simultaneously 0 and 1: $\alpha \|0\rangle + \beta \|1\rangle$
Measurement reveals value	Measurement disturbs
Can be copied	*Cannot* be copied
Strings are described w.r.t. single bits (local)	Strings cannot be described w.r.t. single qubits (non-local)
Behave probabilistically	"Complex probabilities"

Quantum Computers: Is it a serious threat?

- Quantum Computers can solve efficiently **factoring** and **discrete log** (Factoring, RSAP, Discrete Log, DHP)
- Intractable problems (classical hardness guarantees security)
  $\Rightarrow$ Tractable problems (for Quantum Computers)

Quantum Computers: Is it a serious threat?

- Quantum Computers can solve efficiently **factoring** and **discrete log** (Factoring, RSAP, Discrete Log, DHP)
- Intractable problems (classical hardness guarantees security)
  $\Rightarrow$ Tractable problems (for Quantum Computers)

Take-home message

If a scalable quantum computer is built, most of current cryptography breaks (from emails, bank transactions to national security secrets)!

Quantum Computers: Is it a serious threat?

- Quantum Computers can solve efficiently **factoring** and **discrete log** (Factoring, RSAP, Discrete Log, DHP)
- Intractable problems (classical hardness guarantees security) $\Rightarrow$ Tractable problems (for Quantum Computers)

Take-home message

If a scalable quantum computer is built, most of current cryptography breaks (from emails, bank transactions to national security secrets)!

- Known since 1990's
- Requires unprecedented control of quantum systems

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: Google, IBM, Microsoft, Amazon, Intel, D-Wave, Rigetti, IonQ, etc
  Governments: UK, EU, USA, China, Canada, etc (£billions)
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: Google, IBM, Microsoft, Amazon, Intel, D-Wave, Rigetti, IonQ, etc
  Governments: UK, EU, USA, China, Canada, etc (£billions)
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real
- Security can be broken **retrospectively**

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: Google, IBM, Microsoft, Amazon, Intel, D-Wave, Rigetti, IonQ, etc
  Governments: UK, EU, USA, China, Canada, etc (£billions)
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real
- Security can be broken **retrospectively**
- **Years** (possibly decades), are needed to develop/replace all protocols with "quantum-safe" protocols

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: Google, IBM, Microsoft, Amazon, Intel, D-Wave, Rigetti, IonQ, etc
  Governments: UK, EU, USA, China, Canada, etc (£billions)
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real
- Security can be broken **retrospectively**
- **Years** (possibly decades), are needed to develop/replace all protocols with "quantum-safe" protocols

Take-home message

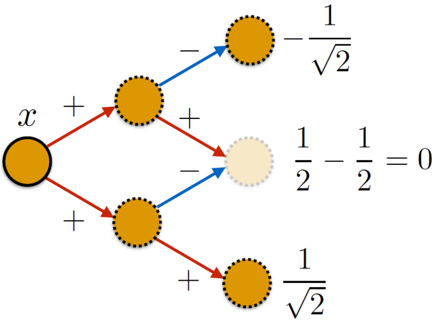
There is a serious medium-time threat that scalable quantum computers will become available. Counter-actions should start now.

How it works

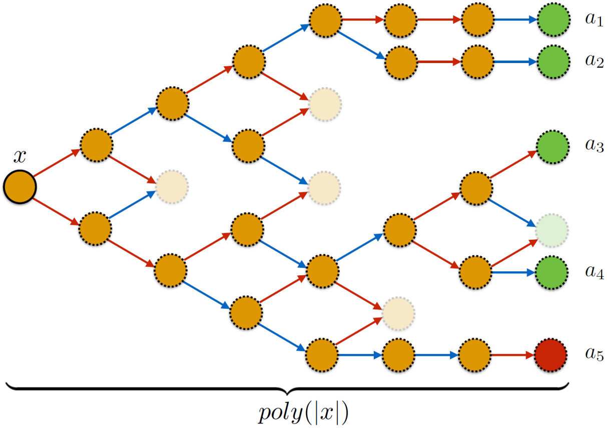
- Could offer significant computational speed-ups
- Can perform more types of operations
- Quantum computers behave as probabilistic computers but with complex-valued "probabilities"

How it works

- Could offer significant computational speed-ups
- Can perform more types of operations
- Quantum computers behave as probabilistic computers but with complex-valued "probabilities"
- Probability is the mod square of the sum of the complex amplitudes



How it works



How it works

- For **speed-up**: need an algorithm that many terms cancel each other
- Non-trivial: need **suitable algorithm design** for each task

How it works

- For **speed-up**: need an algorithm that many terms cancel each other

- Non-trivial: need **suitable algorithm design** for each task

- $|\sum_i a_i|^2 = \sum_i |a_i|^2 + \sum_{i\neq j} a_i^* a_j$

  First term: classical probabilities

  Second term: Amplify or cancel probability (interference)

How it works

- For **speed-up**: need an algorithm that many terms cancel each other
- Non-trivial: need **suitable algorithm design** for each task
- $|\sum_i a_i|^2 = \sum_i |a_i|^2 + \sum_{i\neq j} a_i^* a_j$

  First term: classical probabilities

  Second term: Amplify or cancel probability (interference)
- **Classical systems:** random amplitudes $\rightarrow$ interference $\approx$ zero

On the Power of Quantum Computation

Myth 1

Quantum Computers are much faster in performing operations than Classical Computers

On the Power of Quantum Computation

Myth 1

Quantum Computers are much faster in performing operations than Classical Computers

Reality

Quantum computers are **not** faster. Speed-up is obtained because quantum theory allows algorithms/operations impossible for classical computers.

On the Power of Quantum Computation

Myth 2

Quantum Computers simultaneously perform all branches of a (probabilistic) computation and can use all that information

On the Power of Quantum Computation

Myth 2

Quantum Computers simultaneously perform all branches of a (probabilistic) computation and can use all that information

Reality

QC span the space of possibilities in a peculiar way (behave as complex probabilities). However, at the end of the computation the result is obtained by a **single read-out/measurement** and "unrealised" paths do not contribute.

On the Power of Quantum Computation

Myth 3

Quantum Computers give equally impressive computational speed-up to all problems

On the Power of Quantum Computation

Myth 3

Quantum Computers give equally impressive computational speed-up to all problems

Reality

Quantum computers can give from exponential speed-up (factoring) to much smaller quadratic speed-up (search). The exact optimal quantum algorithm depends on the problem and is crucial for quantum cryptanalysis.

What it takes to be Quantum-Safe

Myth 4

No crypto protocol based on computational assumptions can be secure against quantum attacks. Therefore we can only use information theoretic security

What it takes to be Quantum-Safe

Myth 4

No crypto protocol based on computational assumptions can be secure against quantum attacks. Therefore we can only use information theoretic security

Reality

Quantum computers give speed-ups, but are real devices with well defined limitations. Can base crypto on quantum computational assumptions provided (i) there isn't an efficient quantum algorithm, as for some major cryptosystems (RSA, EC-DSA) and (ii) new security analysis is performed and security parameters are chosen

What it takes to be Quantum-Safe

Myth 5

Using problems that are hard for a quantum computer suffices to make a crypto protocol secure against any quantum attack

What it takes to be Quantum-Safe

Myth 5

Using problems that are hard for a quantum computer suffices to make a crypto protocol secure against any quantum attack

Reality

This is **necessary but not sufficient** condition. New quantum cryptanalysis, new security definitions and new proof techniques are also needed.

Part III

Quantum Cyber Security: Definition and Course Content

Quantum Cyber Security (QCS)

Definition

Quantum Cyber Security is the field that studies *every* impact of the development of quantum technologies on the security and privacy of communications and computations

Quantum Cyber Security (QCS)

Definition

Quantum Cyber Security is the field that studies *every* impact of the development of quantum technologies on the security and privacy of communications and computations

- **Disruptive**: Adversaries with Quantum Computers or QTech
  E.g. Quantum computers solve efficiently factoring and discrete log $\Rightarrow$ RSA, DSA, ECDSA break

If a scalable quantum computer is built, most of current crypto breaks (from emails, bank transactions to national security secrets)!

Quantum Cyber Security (QCS)

Definition

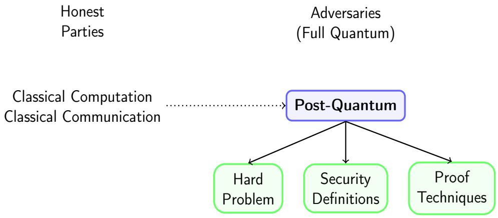
Quantum Cyber Security is the field that studies *every* impact of the development of quantum technologies on the security and privacy of communications and computations

- **Disruptive**: Adversaries with Quantum Computers or QTech
  E.g. Quantum computers solve efficiently factoring and discrete log $\Rightarrow$ RSA, DSA, ECDSA break

If a scalable quantum computer is built, most of current crypto breaks (from emails, bank transactions to national security secrets)!

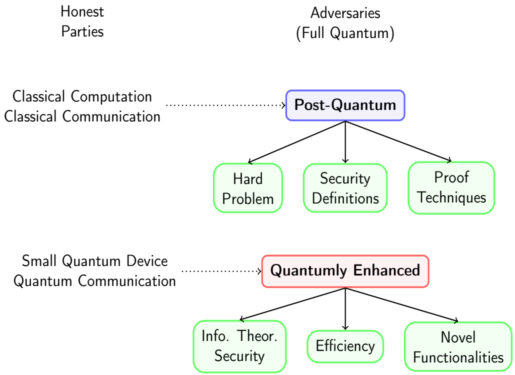
- **New Opport**: Honest with QTech better security/efficiency
  E.g. Quantum Key Distribution (QKD). Quantumness used to enable Key Distribution with information theoretic security

Quantum Cyber Security Landscape: Three Categories



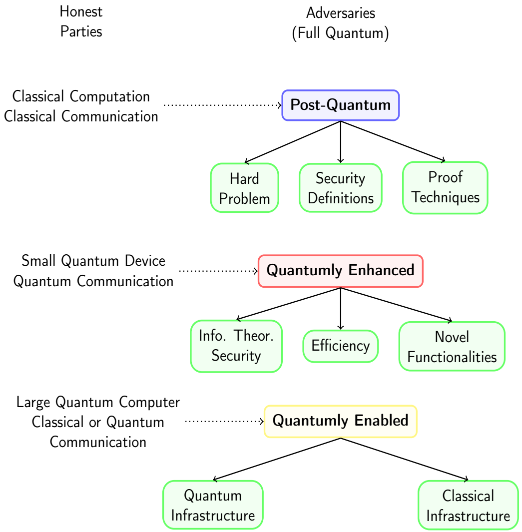
See our review "Cyber Security in the Quantum Era" in CACM

Quantum Cyber Security Landscape: Three Categories



See our review "Cyber Security in the Quantum Era" in CACM

Quantum Cyber Security Landscape: Three Categories



See our review "Cyber Security in the Quantum Era" in CACM

Contents of the Course

- Introduction to Quantum Information & Computation (6 Lectures)

Contents of the Course

- Introduction to Quantum Information & Computation (6 Lectures)
- Quantum Key Distribution (4 Lectures). **First QKD lecture next week** (before completing background).

Contents of the Course

- Introduction to Quantum Information & Computation (6 Lectures)
- Quantum Key Distribution (4 Lectures). **First QKD lecture next week** (before completing background).
- Quantum Coin Flipping (1 Lecture)
- Quantum secure two-party functionalities (1 Lecture)
- Quantum Encryption & Quantum Authentication (1 Lecture)
- Other functionalities, protocols (1 Lectures)

Contents of the Course

- Introduction to Quantum Information & Computation (6 Lectures)
- Quantum Key Distribution (4 Lectures). **First QKD lecture next week** (before completing background).
- Quantum Coin Flipping (1 Lecture)
- Quantum secure two-party functionalities (1 Lecture)
- Quantum Encryption & Quantum Authentication (1 Lecture)
- Other functionalities, protocols (1 Lectures)
- Post-quantum cryptography (3 Lectures)
- Guest Lecture (tbc), Revision (2 Lectures)

About the course

- First part is heavy in maths, but the purpose (cyber security) will become clearer in later parts
- Practically, once used in the notation, it becomes much more easy to follow and use

About the course

- First part is heavy in maths, but the purpose (cyber security) will become clearer in later parts
- Practically, once used in the notation, it becomes much more easy to follow and use
- Bear with us

About the course

- First part is heavy in maths, but the purpose (cyber security) will become clearer in later parts
- Practically, once used in the notation, it becomes much more easy to follow and use
- Bear with us

- My favourite starting quote in a maths book:

  "(the reader) should not be discouraged if (they) find (they) do not have the prerequisites for reading the prerequisites"

About the course

- First part is heavy in maths, but the purpose (cyber security) will become clearer in later parts
- Practically, once used in the notation, it becomes much more easy to follow and use
- Bear with us

- My favourite starting quote in a maths book:

  "(the reader) should not be discouraged if (they) find (they) do not have the prerequisites for reading the prerequisites"
- But this is NOT the case in this course!

  We hope you will enjoy it!