School of Informatics Teaching Course Proposal Form

This version was generated **May 9, 2018**. User 'pwallden@inf.ed.ac.uk' verified.

Proposal

Course Name: Quantum Cyber Security
Proposer's Name: Petros Wallden
Email Address: pwallden@inf.ed.ac.uk
Course Year: 5
Names of any courses that this new course replaces :

Course Outline

Course Level: 11
Course Points: 10
Subject area: Informatics
Programme Collections:
Computer Science.

Teaching / Assessment

Number of Lectures: 20
Number of Tutorials / Lab Sessions: 8
Identified Pre-requisite Courses: N/A
Identified Co-requisite Courses: Either having done a Computer Security course (as INFR10067) or taking the Research Methods in Security, Privacy & Trust (compulsory MSc Security and Privacy course) or having done a Quantum Computing course (INFR11067 or equivalent)
Identified Prohibited Combinations: N/A

Assessment Weightings:
Written Examination: 90%
Assessed Coursework: 10%
Oral Presentations: 0%

Description of Nature of Assessment:

Exam: Questions that test all five Learning Objectives. The knowledge and ability to use quantum information concepts are tested in all questions (LO1), the understanding of quantum speed-ups (LO1) and meaning of security in a quantum adversary model (LO2), is tested both with theoretical questions and with questions involving critical judgement. LO3 is tested both in the coursework and exam, with questions that the student is requested to analyse the security of simple classical protocols using the tools and methods learned in the lectures. LO4 concerns with security of quantum protocols and is tested by considering variations of examples presented in class and requiring from the student to be able to adjust and express the effect that different physical implementations of each protocol have. Finally (LO5), security notions and definitions of quantum information are tested again both in theory and in practical examples and with questions requiring critical thinking.

Coursework: Will be an assignment, based on exercises based on Learning Outcomes 2 and 3 (going through security analysis of a specific classical protocol against quantum attackers with different levels of

quantum abilities and adversarial models).

Course Details

Brief Course Description:

Motivation: There is a global intense initiative on Quantum Technologies by governments, big companies and numerous start-ups. This will change the landscape of research, specifically in Cyber Security, as Quantum Computation and Quantum Communications are disruptive innovations. UK was the first to realise the potential new opportunities as well as the threats that come with Quantum Technologies and launched a 270 million EPSRC Quantum Technologies Initiative in 2014. The relevance to the Cyber Security research was recognised by the Blackett Review (review by the UK government on Quantum Technologies) and GCHQ. Future research and applications in Cyber Security both in Universities and Industry, would need to be ready to address, learn and adjust to the quickly developing new Quantum Technologies. By having a solid background offered by this course, our graduates will be placed in an advantageous position. Moreover, such a course is likely to attract ambitious students and distinguish our MSc Programme in Security and Privacy from competitors.

Description: In this course we cover a broad range of effects that the development of quantum technologies bring on the security and privacy of communication and computation. In particular we consider (i) post-quantum security: security of classical protocols when the adversaries have access to quantum computers or other quantum technologies and (ii) quantumly-enhanced security: when quantum technologies are used by honest parties to achieve better (in terms of security or efficiency) performance. We give an overview of the field, while in each case we focus on selected examples to illustrate how to handle security in a world with quantum technologies.

Detailed list of Learning Objectives:

1: Understanding the power and limitations of quantum computation and obtain knowledge and ability to use the basic mathematical formalism for quantum information and quantum cryptography

2: Understanding of what it takes for a classical cryptosystem to be secure against quantum attacks

3: Develop the ability to analyse quantum attacks to classical protocols

4: Be able to understand the security of quantum cryptography and to analyse how different implementations affect the performance

5: Understand security notions for quantum information, such as encryption and authentication, and their application to blind quantum computation

Syllabus Information:

- Analysis of which problems and in what extend quantum computers offer speed-up compared to classical computers
- Quantum Information: qubits, mixed states, operations, distance measures, teleportation, no-cloning
- The Learning-with-Errors cryptosystem
- Superposition attacks, quantum indistinguishability and the quantum random oracle model
- The BB84 quantum key distribution protocol. Security proof and the effects of different implementations
- The impossibility of information theoretic secure, quantum bit-commitment
- Quantum encryption and quantum authentication. Definitions and protocols.
- Blind quantum computing

Recommended Reading List:

The lecture notes as main source and as supplementary reading:

Quantum Computation and Quantum Information by Nielsen and Chuang

Quantum Information by Stephen Barnett

Post-Quantum Cryptography Editors Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen

Any additional case for support information:

To be considered to start in year 2019-2020, as part of the MSc in Security and Privacy