School of Informatics Teaching Course Proposal Form

This version was generated **March 7, 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 :
N/A

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: Computer Security INFR10067. Recommended to have taken either Introduction to Quantum Computing INFR11067 or Introduction to Modern Cryptography INFR11131, or similar level courses
Identified Co-requisite Courses: N/A
Identified Prohibited Combinations: N/A

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

Description of Nature of Assessment:
based on Learning outcomes 2 and 3

Course Details

Brief Course Description:

In this course we cover aspects from all the range the effects that quantum technologies have on secure communication and computation. These effects are divided (i) when quantum adversaries attack classical protocols and (ii) 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:

I plan to propose this course as part of the suggested MSc in Security and Privacy.