1. Quantum Cyber Security - a Testbed for Novel Quantum Security Network Architectures

The security of the current Internet and applications that run on it is not based on provable security. For example, public private key cryptography depends on the computational complexity of factoring prime number pair (the private key, and the public key). That is, the communication link and data sent through it are deemed secure because it is not computationally feasible for an adversary to break the security. In other words, the security depends on the computing limitations of the adversary's resources, not because it is secure inherently.

With the power of Quantum computing, not only will future communication be breakable, but also it will also be possible to decrypt data previously encrypted using the current cryptographic techniques. This has big ramifications for lots of private and public data whose secrecy is supposed to be protected by policy. Because secure communication cannot be guaranteed with the existing cryptography based approaches, it is crucial to develop unconditional security (provable security) suitable for the post-quantum. This project aims to develop a testbed in order to analyse novel quantum cyber Security techniques such as photon based random number traffic generation in a typical client server model.

This project requires either a programming or a networks configuration background. Training will be provided.

Supervisor: Dr Athanasios Tsokanos (a.tsokanos@herts.ac.uk)

2. Quantum Random Number Traffic Generator (QRNG) for Cyber Security

How can QRNG be integrated with Cryptography? The unique characteristic of Quantum RNG is that it offers provable security. For example, in a client and server model the client and the server are connected via two different channels: the quantum channel (shielded optic fibre) capable of conducting single photons of light, and the second one unsecured Internet link. With true randomness with QRNG, an attacker simply has no enough information to break through even with a lot of computing resources. Similar applications of QRNG for encryption, digital signatures, one-time-pad and other cryptographic requirements is possible. This work aims to extend the knowledge on current hardware based Quantum Random Number Traffic Generators and to build a novel model for their performance evaluation.

This project requires either a programming or a networks configuration background. Training will be provided.

Supervisor: Dr Athanasios Tsokanos (a.tsokanos@herts.ac.uk)

Entry Requirements

Applicants are expected to hold a very good first or upper-second class degree in a relevant discipline (or equivalent overseas qualification), and/or a good Master's degree (or equivalent experience/qualifications). Prior scientific publications are particularly desirable but not essential. Non UK/EU nationals without an academic degree from the UK or EU (taught in English) will normally be required to have IELTS of 6.5 or above (or equivalent) with at least 6.0 in each individual component. The position is open to home and overseas students.

How to Apply

Download the application form and find further details from:

https://www.herts.ac.uk/study/schools-of-study/computer-science/our-research/the-phd-programme-in-computer-science

Please note: You must download the application form to your computer before you complete it. If you complete the form in the browser window, the information you have entered may be lost when the form is saved. The application form should be returned to:

Mrs Emma Thorogood Research Student Administrator University of Hertfordshire College Lane Hatfield, Herts AL10 9AB tel: +44 (0)1707 286083 doctoralcollegeadmissions@herts.ac.uk

Applications should also include two references and transcripts of previous academic degrees as well as a cover letter and a CV. We also accept applications for self-funded places in various computer science related topics throughout the year.

For informal enquiries please contact Dr Athanasios Tsokanos (a.tsokanos@herts.ac.uk).