James Howe

Curriculum Vitae

Centre for Secure Information Technologies,
Queen's Road, Queen's Island,
Belfast, BT3 9DT, UK
✉ *jhowe02@qub.ac.uk*

Education

2013– **PhD Computer Science**, *Queen's University*, Belfast.
Currently researching post-quantum cryptography in collaboration with Thales UK and SAFEcrypto. The research mainly focuses on secure and practical lattice-based cryptography, implementing in hardware and software. Supervised by Professor Máire O'Neill.

2011–2012 **MSc Mathematics of Cryptography & Communications**, *Royal Holloway, University of London*, Surrey.
Thesis titled 'The Cryptanalysis of Block Ciphers' obtained distinction, supervised by Professor Sean Murphy. Modules focused on pure mathematics, cryptography, and coding theory.

2008–2011 **BSc (Hons) Mathematics**, *University of Greenwich*, London.
Obtaining a first class degree. Thesis concentrated on the theory and practicality of modern cryptography. Modules focused on applied mathematics, probability, and statistics.

Work Experience

2016– **Research Assistant**, *Queen's University*, Belfast.
Researching hardware designs of lattice-based cryptoschemes with SAFEcrypto at CSIT.

2013– **Teaching Assistant**, *Queen's University*, Belfast.
Demonstrating in mathematics and applied cryptography lectures at for EEECS master's students.

2009–2011 **University Ambassador**, *University of Greenwich*, London.
Assisted college-level mathematics classes in schools across Greater London in partnership with the university. Also worked as an employee of the university; giving talks to prospective students in schools, giving tours of the campus, and participating at open days.

2010–2011 **Statistical Analyst**, *University of Greenwich*, London.
Worked with a number of major databases in the university's statistics department. Produced reports and presentations to use in meetings with the Chancellor and Vice-Chancellor. Updated statistics published on the university's website.

Achievements

Publications.
(1) Howe, James, *et al.* "Practical Lattice-based Digital Signature Schemes." *ACM Transactions on Embedded Computing Systems (TECS)* 14.3 (2015): 41.
(2) Howe, James, *et al.* "Lattice-based Encryption Over Standard Lattices in Hardware." *Design Automation Conference (DAC)*, 2016.
(3) O'Neill, Máire *et al.* "Secure Architectures of Future Emerging Cryptography SAFEcrypto", *ACM International Conference on Computing Frontiers*, 2016.
(4) Khalid, Ayesha *et al.* "Time-Independent Discrete Gaussian Sampling For Post-Quantum Cryptography." *Field-Programmable Technology (FPT)*, 2016.
(5) Howe, James, *et al.* "On Practical Discrete Gaussian Samplers For Lattice-Based Cryptography." *IEEE Transactions on Computers*, 2016.
(6) Howe, James, *et al.* "Compact and Provably Secure Lattice-Based Signatures in Hardware." *IEEE ISCAS*, 2017.
(7) Howe, James and O'Neill, Máire "GLITCH: A Discrete Gaussian Testing Suite For Lattice-Based Cryptography" *SECRYPT*, 2017.

Paper Reviews.
Reviewed papers for ACM TECS, IEEE ToC, SAC 2016, WAHC 2015, and Security and Communication Networks.

Conferences.
Presented at conferences ISCAS 2017, DAC 2016, FPT 2016, and on modern cryptography at 'Tomorrow's Mathematicians Today' conference in London, 2009.

Awards.
Received COST Action IC1306 stipend (2014) and COST Action IC1306 STSM grant (2015).

IT Skills.
Proficient in all major operating systems (OSX/Linux/Windows) as well as mathematical tools such as Mathematica, Matlab, and Minitab. Very competent with VHDL (ISE & Vivado), Python, C/C++, with some Java experience.

Research Statement

My research aims to bring principles and techniques from lattice-based cryptography to the design and implementation of secure and correct systems. To this end, I became an expert in the theory of lattice-based cryptography, and then designed architectures using optimisations which target specific devices such as FPGAs. In the past, I have studied applied mathematics during my bachelor's degree and pure mathematics during my master's degree, so I am very familiar with the mathematical side of cryptography. I am now looking to use my expertise to make cryptography (ideally, lattice-based cryptography) more practical, to be used in real-world applications, for the benefit of secure communications.

I completed a research visit in 2015 at Bochum with Thomas Poeppelmann and Tim Gueneysu, funded by COST. For this research we investigated new techniques for the discrete Gaussian sampling component, as well as techniques to check the samplers validity and correct functionality. This collaboration also resulted in a joint journal publication on lattice-based digital signature schemes.

I also completed an internship with Thales (Research and Technology) in 2015 with Adrian Waller. During this internship, I targeted a highly secure lattice-based cryptoscheme: standard LWE encryption. It was previously believed that this scheme, in fact any standard lattice-based scheme, would perform badly in hardware. The hardware designs I proposed in fact competed with the corresponding encryption scheme over ideal lattices, with a slight increase in hardware resource consumption. This has been further improved after publication for inclusion in my PhD thesis, in which the design consumes less area.

As a PhD student and Research Assistant, I also work with SAFEcrypto (http://www.safecrypto.eu), which has ties with a number of European research centres. The main outputs of this collaboration was a comprehensive evaluation of discrete Gaussian samplers in hardware and a low-area hardware design of Ring-TESLA, an ideal lattice-based signature scheme. The discrete Gaussian samplers proposed better all previous work in hardware, as well as offering constant run-time which is preferable due to side-channel analysis. The hardware designs of Ring-TESLA provide generic hardware architectures, which allows ease of use with a number of different parameter sets. This hardware architecture has the potential for high throughput with a fast NTT multiplier.

If you require any references, please use these contacts:

- Prof. Maire O'Neill: `m.oneill@ecit.qub.ac.uk`
- Dr. Francesco Regazzoni: `regazzoni@alari.ch`