James Howe

Curriculum Vitae

PQShield Ltd.,
Prama House, Summertown,
OX2 7HT, Oxford, UK.
james.howe@pqshield.com
www.jameshowe.eu

Education

2013–2017 **PhD Computer Science**, *Queen's University*, Belfast.
In collaboration with Thales UK and SAFEcrypto, the subject focused on post-quantum cryptography. The research concentrated on *practical lattice-based cryptography*, with designs 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

2019–Present **Crptography Researcher**, *PQShield*, Oxford.
Researching and designing implementations of NIST post-quantum standards.

2017–2019 **Research Associate**, *University of Bristol*, Bristol.
Researching a number of areas within software and hardware lattice-based cryptographic designs. Mainly analysing schemes with respect to side-channels and optimising schemes for hardware designs.

2016–2017 **Research Fellow**, *Queen's University*, Belfast.
Researching hardware designs of lattice-based cryptoschemes with SAFEcrypto at CSIT.

2015 **Internship**, *Thales Research and Technology*, Reading.
Collaborated on a project designing highly secure lattice-based encryption in hardware.

2015 **Research Visit**, *Ruhr-Universität*, Bochum.
Collaborated on the design and analysis of discrete Gaussian samplers for lattice-based cryptography.

2013–2017 **Teaching Assistant**, *Queen's University*, Belfast.
Demonstrating in mathematics and applied cryptography lectures at for EEECS master's students.

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

Conference Publications.

(1) Howe, James, *et al.* "Lattice-based Encryption Over Standard Lattices in Hardware." *Design Automation Conference (DAC)*, 2016.
(2) O'Neill, Máire *et al.* "Secure Architectures of Future Emerging Cryptography SAFEcrypto", *ACM International Conference on Computing Frontiers*, 2016.
(3) Khalid, Ayesha *et al.* "Time-Independent Discrete Gaussian Sampling For Post-Quantum Cryptography." *Field-Programmable Technology (FPT)*, 2016.
(4) Howe, James, *et al.* "Compact and Provably Secure Lattice-Based Signatures in Hardware." *IEEE ISCAS*, 2017.
(5) Howe, James and O'Neill, Máire "GLITCH: A Discrete Gaussian Testing Suite For Lattice-Based Cryptography" *SECRYPT*, 2017.
(6) Khalid, Ayesha *et al.* "Compact, Scalable, and Reconfigurable Gaussian Samplers for Lattice-Based Cryptography." *IEEE ISCAS*, 2018.
(7) Khalid, Ayesha *et al.* "Error Samplers for Lattice-Based Cryptography: Challenges, Vulnerabilities, and Solutions." *IEEE APCCAS*, 2018.
(8) Sailong, Fan *et al.* "Lightweight Hardware Implementation of R-LWE Lattice-Based Cryptography." *IEEE APCCAS*, 2018.
(9) Ravi, Prasanna *et al.* "Exploiting Determinism in Lattice-based Signatures: Practical Fault Attacks on pqm4 Implementations of NIST Candidates." *Asia CCS*, 2019.
(10) Howe, James *et al.* "Fault Attack Countermeasures for Error Samplers in Lattice-Based Cryptography." *IEEE ISCAS*, 2019.
(11) Howe, James *et al.* "Optimised Lattice-based Key Encapsulation in Hardware." *NIST's Second PQC Standardization Conference*, 2019.
(12) Apon, Daniel and Howe, James "Attacks on NIST PQC 3rd Round Candidates." *IACR Real World Crypto*, 2021.
(13) Howe, James *et al.* "SoK: How (not) to Design and Implement Post-Quantum Cryptography." *CT-RSA*, 2021.

Journal 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.* "On Practical Discrete Gaussian Samplers For Lattice-Based Cryptography." *IEEE Transactions on Computers*, 2016.
(3) Howe, James *et al.* "Standard Lattice-Based Key Encapsulation on Embedded Devices." *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018.
(4) Howe, James *et al.* "Exploring Parallelism to Improve the Performance of FrodoKEM in Hardware." *Journal of Cryptographic Engineering*, 2021.

Program Committees and Reviews.

Program committee for T-CHES 2021 (Artifacts), Indocrypt 2020, COSADE 2020, and MAL-IoT 2019. Reviewed papers for ACM TECS, IEEE Transactions on Computers, IMACC 2019, CRYPTO 2019, PQCrypto 2019, ASIACRYPT 2018, Designs Codes and Cryptography, CT-RSA 2018, CARDIS 2018, SAC 2016, WAHC 2015, and Security and Communication Networks.

Talks.

Invited to present at Lattice Coding & Crypto Meeting in September 2018 and NIST Post-Quantum Cryptography Hardware Day 2019. Presented at CT-RSA 2021, IACR RWC 2021, NIST's Second PQC Standardization Conference 2019, ISCAS 2019, T-CHES 2018, ISCAS 2018, ISCAS 2017, DAC 2016, FPT 2016, and on Modern Cryptography at Tomorrow's Mathematicians Today conference in 2009.

Awards.

Received IUK grant, 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 and Vivado), Python, C/C++, with some Java and HTML (see `www.pqczoo.com`) experience.

Research Statement

My research aims to bring principles and techniques from post-quantum cryptography, specifically 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 during my first year of PhD studies, the survey of which resulted in a journal paper. Using this knowledge as a basis significantly helped in understanding the motivations and design rationales of these lattice-based cryptographic scheme. Most of the remaining research during my thesis then followed from this which focused on designing architectures using optimisations which target specific devices such as FPGAs. My education up to this point focussed on applied mathematics (during my bachelor's degree) and cryptography and pure mathematics (during my master's degree), so I am very familiar with the mathematical side of cryptography.

I completed a research visit in 2015 at Ruhr-Universität, Bochum, with Thomas Pöppelmann and Tim Güneysu, funded by COST. For this research we investigated new techniques for the (essential) 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 cryptographic scheme: 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 bettered 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.

In 2017, I joined the side-channel and cryptography group at the University of Bristol, supervised by Elisabeth Oswald. Here I learnt a lot about side-channel analysis, a new field I am very interested in researching, particularly with respect to lattice-based cryptography. We have collaborated on many side-channel related projects, mainly focussed on novel countermeasures, plus I continue to collaborate with other research centres in the Hardware Security Group, Bochum, ALaRI Institute, Switzerland, and Temasek Laboratories, Singapore. During my research at Bristol I also continued to research hardware and software designs. A recent publication investigated a potential NIST key encapsulation post-quantum standard, named FrodoKEM, which I presented at T-CHES in collaboration with researchers at Ruhr-Universität, Bochum.

In early 2019, I began working at PQShield, a company specialising in post-quantum cryptography, as a Cryptography Engineer. My responsibilities here included research, profiling schemes on bare-metal targets, investigating side-channels, and designing countermeasures. I also contributed to InnovateUK funding submissions and doing the research and writing reports for this.

If you require a reference, please contact Professor Elisabeth Oswald (`elisabeth.oswald@bristol.ac.uk`), Professor Máire O'Neill (`m.oneill@ecit.qub.ac.uk`), and/or Dr. Francesco Regazzoni (`regazzoni@alari.ch`).