Professor Máire O'Neill (née McLoone)

Principal Investigator, Centre for Secure Information Technologies (CSIT)
Director, UK Research Institute for Secure Hardware and Embedded Systems (RISE)

Institute of Electronics, Communications and Information Technologies (ECIT)
Queen's University Belfast (QUB), Queen's Island, Belfast, BT3 9DT, Northern Ireland.
E-mail:m.oneill@ecit.qub.ac.uk; Tel: +44 2890971785; Fax: +44 2890971702

Qualifications and Affiliations

- Postgraduate Certificate in Higher Education Teaching (PGCHET), Queen's University Belfast, 2006.
- Doctor of Philosophy in Data Security (Thesis title: Generic Silicon Architectures for Encryption Algorithms), Queen's University Belfast, December 2002.
- M.Eng. with Distinction (1st place) in Electrical & Electronic Engineering, Queen's University Belfast, 1999.
- Elected Member of the Royal Irish Academy, 2017 (its highest honour), Elected Fellow of the Irish Academy of Engineering (2015), SMIEEE, FHEA, MIET, Chartered engineer, member of International Association for Cryptologic Research (IACR).

Career History

- **Director of UK Research Institute in Secure Hardware and Embedded Systems (RISE),** a UK wide multi-University initiative, funded by EPSRC and the National Cyber Security Centre (NCSC), 2017 – 2022.
- Principal Investigator & Research Director, Centre for Secure Information Technologies (CSIT), Queen's University Belfast.
- Professor of Information Security (Oct 2010 – present)**,** Reader (Oct 2008 – Oct 2010), Lecturer (Oct 2004 – Oct 2008), School of Electronics, Electrical Engineering & Computer Science, QUB.
- Course Director, MSc in Cyber Security, Queens University Belfast, 2013 – 2015.
- **UK EPSRC Leadership Fellowship** on 'Next Generation Data Security Architectures', QUB, 2008-2015.
- **UK Royal Academy of Engineering (RAEng) Research Fellowship**, QUB, 2003 –2008.
- Postdoctoral Research Fellow, School of Electrical and Electronic Engineering, Queen's University Belfast, January 2003 – March 2003.
- Consultation work on Advanced Encryption Standard IP Core Development, Amphion Semiconductor Ltd, July 2001 – August 2001.

Research

To date, I have secured **external research funding of £30M (£7.1M as Principal Investigator –PI)** that includes funding from the EU, EPSRC, ESA, InnovateUK, GCHQ, DSTL and the Royal Academy of Engineering. (*Overall funding for CSIT Phase I & II leveraged a further £45M*).

- InnovateUK, **Agile Quantum Safe Communications (AQuaSec)**, involves 17 industry and academic partners, led by Toshiba Research Europe, QUB PI (2018-2020, £311k)
- European Space Agency (ESA), Techniques For Authentic Position/Velocity/Time (PVT), International Research Collaboration, with Qascom, Italy, Cillian O'Driscoll Consulting Ltd., and Bundeswehr University Munich, Germany, QUB PI (2018-19, £26k)
- **EPSRC/NCSC, Research Institute in Hardware Security** – Hosting UK wide collaborative activity and involved in a core programme of research activity on 'DeepSecurity; The Application of Deep Learning to Hardware Security', Principal Investigator (**2017-2022, £1.2M)**
- GCHQ PhD studentships:
  - 'Applying Deep Learning to Enhance Physical Unclonable Functions', PI (2017, £112k)
  - 'Multi-PUF Designs and Architectures', PI (2016, £112k)
  - 'Post Quantum Lattice Based cryptography', PI (2014, £109.5k)
  - 'Novel Application of Advanced Machine Learning Techniques for use in SCA Attacks', PI (2012, £108k)
- InvestNI Proof-of-Concept Funding, 'Crypto Agility: A Quantum Safe Protocol Engine, Co-I, (2013, £108K)

- Ministry of Science, ICT and Future Planning, South Korea, 'Secure key hiding technology for IoT Devices'**, £1.6M International Research Project**, Partners: ETRI (Project Lead, S.Korea), SecureIC (France), ICTK (S.Korea), Korea University, Purdue University (US); QUB PI (2016-18, £105k QUB)
- DSTL, 'Security for the Internet of Things – Software PUFs as a Trust Anchor', PI (2015, £49.7k)
- UK EPSRC/Innovate UK Innovation and Knowledge Centre, *Phase II* (EP/N508664/1), *Centre for Secure Information Technologies (CSIT)*, Co-Investigator (2015-2020, £5M)
- **Project co-ordinator of EU H2020 project 'SAFEcrypto**: Secure Architectures of Future Emerging Cryptography', involving 4 university partners and 3 industry partners from UK, Germany, France, Switzerland and Ireland, Principal Investigator (2015, €3.8M)
- EU H2020 project 'UniServer: A Universal Micro-Server Ecosystem by Exceeding the Energy and Performance Scaling Boundaries', Co-Investigator (2015, £677k)
- InvestNI Proof-of-Concept Funding, 'PUF-PKI: Authentication Platform for Electric Vehicle Charging Systems', Principal Investigator, (2013, £106K)
- UK EPSRC 'New Directions for EPSRC's Research Leaders' funding, PI, (2012-2014, £312.6K)
- UK EPSRC 'Bridging the Gap' Impact funding, (2012, £53k.)
- UK EPSRC/TSB Innovation and Knowledge Centre (EP/H049606/1, EP/G034303/1, EP/J006238**/**1), *Centre for Secure Information Technologies (CSIT)*, Funders also include industry, QUB & InvestNI, Co-I (2009-2014, £30.5M)
- UK EPSRC Leadership Fellowship (EP/G007586/1), *Next-Generation Data Security Architectures**,*** Principal Investigator, (2008-2013, £1.2M)
- UK Royal Academy of Engineering research fellowship on *'*Cryptographic Algorithms and Architectures for System-on-Chip', Principal Investigator, (2003-2008, £250k)
- UK EPSRC (EP/C006976/1), *Security Protocols & Architectures for Ad Hoc Networks,* Principal Investigator, (2005 - 2008, £126k)

Research Outputs

I have published two research monographs, 6 book chapters, 5 special issue journal editorials, 32 international peer-reviewed journal papers and 113 international peer-reviewed conference papers to date. (Top citation: 225, H-index = 29, i10-index=60, Google Scholar – see attached list of publications)

Invited Papers/Best Paper Awards

- Paper on 'Optimised Multiplication Architectures for Accelerating Fully Homomorphic Encryption', published in IEEE Transactions on Computers, was selected as feature paper of the month in September 2016, and was one of four papers chosen as **IEEE Trans. on Computers** '**Editor's pick of the year 2016'.**
- In 2015, to celebrate 25 years of the International Conference on Field-programmable Logic & Applications (FPL) my co-authored paper "FPGA Implementations of the Round Two SHA-3 Candidates" was awarded as one of 27 papers ***deemed to have most strongly influenced theory and practice in the field***.
- Five of the book chapters were invited contributions.
- Invited to submit journal papers to two Special Issues of Journal of VLSI Signal Processing, 2003 & 2007.
- Awarded Best Paper at IEEE Intl. Symposium on Hardware-Oriented Security and Trust (HOST), US, 2013
- Awarded Best Paper at the 22nd IET Irish Signals and Systems Conference, Dublin, 2011.
- Best Paper Finalist at the IEEE International Symposium on Circuits and Systems (ISCAS), 2011.
- Invited paper at 16th Asilomar Conference on Signal Processing, Systems and Computers, US, 2012.

Postgraduate Student Supervision:

- I have supervised and supported the career development of 13 PDRAs and 11 PhD students as primary supervisor. Many now hold senior engineering positions in companies such as Imagine Technologies, Sensata, HP, Intel, two are Associate Professors and one graduate is CEO of his own company, Facta IOT, Shanghai, China.
- Successful Post-graduate students: James Howe (PhD, 2017), Chongyan Gu (PhD, 2016), Ciara Moore (PhD, 2015), Yongsheng Wang (PhD, 2013), Philip Hodgers (PhD, 2012), Xiaolin Cao (PhD, 2012), Weiqiang Liu (PhD, 2012), Kean Hong Boey (PhD, 2012), Yingxi Lu (PhD, 2009), Neil Smyth (PhD, 2008), Patrick Moore (PhD, 2008), Clare McGrath (MPhil, 2008)

Knowledge Transfer and Exploitation of Research

- Research into high-speed Advanced Encryption Standard (AES) architectures **successfully commercialised by Amphion Semiconductors** (acquired by Conexant, 2004, NXP, 2008, Trident Microsystems, 2010 and Entropic Communications, 2012), and utilized to provide security in their set-top box chip sets. In 2011, Trident reported that 100 million of their set-top boxes had been shipped worldwide.
- Novel security architecture for Electric Vehicle (EV) charging systems, developed in collaboration with ETRI, South Korea, **successfully licensed by LG-CNS,** a subsidiary of the LG electronics group, 2013.
- PUF technology licensed for evaluation by UK Defence company, 2015/16. Built into a demonstration model for electronic component counterfeiting, 2018.
- Co-founder of spin-out, Sirona Technologies Ltd (www.sirona.io) and winner of the **2015 INVENT Awards** (www.invent2015.co) – recognises inventions with the greatest commercial potential from Northern Ireland.
- Awarded **UK Royal Academy of Engineering 2014 Silver Medal**, which recognises outstanding personal contribution by an early or mid-career engineer that has resulted in successful market exploitation**.**

Professional Activity

Participation in Professional and Advisory Bodies

- Appointed to **UK Government's AI Council** to represent cyber security technology area, 2019.
- Appointed to serve as member of sub-panel 11 in the assessment phase (2020-21) of the UK **Research Excellence Framework (REF 2021)**, in the role of practising researcher. REF is the UK's system for assessing the excellence of research in higher education institutions.
- Member of the **UK Royal Academy of Engineering research committee** (2017-2020).
- Member of **Royal Irish Academy's Engineering and Computer Sciences Committee** (2018 -2022)
- Advisory Board member, FIRE (Facilitate Industry and Research in Europe) FP7 project, 2013-2014.
- Member of **Young Advisors Group to Commissioner Neelie Kroes,** Vice President of the European Commission and Commissioner for the European Digital Agenda, 2010 - 2011.
- **IEEE Circuits & Systems for Communications (CASCOM) Technical committee member**, 2007-present.
- Past **treasurer of the IEEE UKRI Executive Committee**, 2008/2009.

Associated Editor/Guest Editor

- Associate Editor, IEEE Transactions on Emerging Topics in Computing, 2016 -.
- Associate Editor, IEEE Transactions on Computers, 2016 -.
- Guest Editor, IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Technologies and Designs for Application-Specific Computing, with W. Liu and E. Swartzlander, 2017
- Guest Editor, Journal of Signal Processing Systems, Special Issue on New Frontiers in Signal Processing Applications and Embedded Processing Technologies, with J. McAllister and M. Pelcat, May 2016.
- Guest Editor, ACM Transactions on Embedded Computing Systems, Special Issue on Embedded Platforms for Cryptography in the Coming Decade, with P. Schaumont, T. Guneysu 2015
- Guest Editor, Special Issue on Next Generation Hardware Architectures for Secure Mobile Computing, Mobile Networks and Applications (MONET) Journal, Springer-Verlag, with N. Sklavos and X. Zhang, 2007.
- Guest Editor, Launch Issue of IET Information Security, Special Issue on Cryptographic Algorithms & Architectures for System-on-Chip, Vol. 152, Issue 1, with C. Paar and R. Woods, 2005.

Research Funding Evaluation

- Member of UK Royal Academy of Engineering Research Fellowship Sift Panel & Interview Panel, 2018 - .
- Chair, EPSRC Panel, Research Institute in Hardware Security - Call for Research Projects, September 2017.
- ERC Fellowship remote reviewer, 2013
- Member of the UK Engineering and Physical Sciences Research Council (EPSRC) Peer Review College
- Served on the EPSRC Challenging Engineering ICT Interview panel, 2010.
- Reviewer for Technology Foundation STW, the Dutch funding agency for university research, covering security in ICT, networks and information systems.
- Evaluator for EU Frame Work Programme 6 Marie Curie Individual Fellowship & Transfer of Knowledge schemes, 2005.

External Examiner Appointment

- External examiner of M.Sc. in Security and Forensic Computing, Dublin City University, 2010 – 2013.
- PhD external examiner: University of Bristol, UK (David McCann, 2017); University College Cork, Ireland (Maurice Keller, 2008); University of Waterloo, Canada (Edgar Santillan, 2012); Invited external examiner at University of Sheffield (2016)

International Conference/Workshop Activity

- Tutorial on 'Practical PUF Design for FPGA', DATE Conference, Florence, March 2019
- As Director of RISE, I organised a Spring School in Hardware Security, University of Cambridge, March 2018 & Queen's University Belfast, March 2019
- **Program Chair** of 16th IMA International Conference on Cryptography and Coding, 2017
- **Program Co-Chair**, Workshop on Signal Processing Systems (SiPS), Belfast, 2014.
- Invited to organise a Special Session on Post-quantum cryptography and Homomorphic Encryption at the Intel Workshop, held in conjunction with Eurocrypt 2014, Copenhagen, May 2014
- **Technical Co-Chair** of 7th Workshop on Embedded Systems Security (WESS 2012) at ESWEEK 2012, Tampere, Finland, October 2012.
- International Program committee membership:
  - Track Chair, IEEE International Symposium on Circuits & Systems (ISCAS), 2019
  - Conference on Selected Areas in Cryptography (SAC), 2019
  - IEEE International Workshop on Signal Processing Systems (SiPS), 2019
  - Invited to serve on the Embedded Security sub-committee of the ACM/IEEE Design Automation Conference (DAC), the premier event of the electronic circuits and systems community – only 4 academics sit on the sub-committee over a 4 year term, 2011-2014
  - Workshop on Cryptographic Hardware & Embedded Systems (CHES), 2008, 2010
  - Design, Automation and Test in Europe Conference (DATE) – 'Secure Embedded Implementations' track, 2009 - 2012
  - Workshop on RFID Security (RFIDSec), 2009
  - IEEE International SoC Conference (SoCC), 2009 -2011
  - International Conference on ReConFigurable Computing and FPGAs (ReConFig'08)- Track on Reconfigurable Computing for Security and Cryptography, 2008
  - IEEE International Symposium on Circuits & Systems (ISCAS), 2008 – present
  - 14th EUROMICRO Conference on Digital System Design, Special Session on Architectures and Hardware for Security Applications, 2011-2012
  - IET Irish Signals & Systems Conference (ISSC), 2004 – 2012
- Session Chair at several conferences including, IEEE SoCC 2009, DATE 2009, IEEE ISCAS 2007, 2011, 2012, 2014, 2015, 2018, 2019, CHES 2014, IEEE SiPS 2014.
- **Organiser of Special Sessions:**
  - 'Towards Practical Homomorphic and Post Quantum Cryptographic Architectures', IEEE ISCAS 2014
  - 'Quantum-Dot Cellular Automata (QCA) Circuit Design', IEEE ISCAS 2011
  - 'Novel Cryptographic Architectures for Low-Cost RFID' IEEE ISCAS 2007
- **Reviewer for the following international journals:** IEEE Transactions on Computers, IEEE Transactions on VLSI Systems, IEEE Transactions on Circuits & Systems, IEEE Communications Magazine, ACM Transactions on Reconfigurable Technology and Systems, IET Circuits, Devices & Systems, IET Computer & Digital Techniques, Eurasip Journal on Signal Processing, VLSI Journal – Integration, ETRI journal.
- Book proposal reviewer for Cambridge University Press.

Invited lectures/seminars

- Invited talk, IET eFutures Annual Community Event, 'Electronics in Infrastructure', London, 2018.
- Invited talk, Automotive Security Conference (AESIN), UK, July 2018.
- 16th Annual International Conference on Privacy, Security & Trust, Industry Day, Panel Session on The Future of Privacy and Trust, Belfast, 28 August 2018.
- **ENISA Summer School on Network and Information Security** – invited talk on Practical post-quantum cryptography, Greece, 24-28 September 2019

- **Royal Irish Academy Discourse**, Securing Connected Devices: An Arms Race, Dublin, October 2018.
- Invited talk, **Cure, Create, Innovate: 9 Young Scientists Transforming Our World**, Science Museum, London, March 2019
- Invited speaker at **Real World Crypto (RWC), Zurich, Jan 2018**, the premier conference in the field of practical cryptography, with over 600 attendees.
- Invited talk, Royal Academy of Engineering Research Forum, London, September 2017
- **Invited speaker on the Security and Resilience panel** at the **2015 Global Grand Challenges Summit** organised by the Chinese Academy of Engineering, UK Royal Academy of Engineering and US National Academy of Engineering, Beijing, September 2015.
- Invited Lecture on 'Security in a Post-Quantum World' at the JS Bell Festival, QUB, November 2014.
- Invited speaker on 'Practical Cryptography' at the UK Royal Academy of Engineering AGM, Sept. 2014.
- Keynote speaker on 'Security in a Post-Quantum World' at World Cyber Security Summit, Belfast, 2014.
- Participated in a UK Academic Cyber Security Research visit to Japan organised by the UK Engineering and Physical Sciences Research Council (EPSRC), February 2014.
- **Invited to be part of a UK delegation** at the **UK-Japan Symposium** on Privacy & Security in the Information Society, Tokyo, Japan, 2008 - organised by UK Royal Academy of Engineering and Engineering Academy of Japan.

A sample of other invited seminars on my research in Data Security include:

- ICT Knowledge Transfer Network (KTN) Cyber Security Summit, Brussels, March 2012.
- Seoul National University, S. Korea, March 2009;
- University College Dublin, December 2007;
- British Computer Society (BCS) Equalitec E-Security Workshop, London, July 2007;
- Cylab, Carnegie Mellon University, Pittsburgh, PA, US, April 2006;
- Royal Academy of Engineering Research Forum 2005, London, September 2005;
- Workshop on Hash Functions, Krakow, Poland, organised by EU funded ECRYPT project, June 2005.
- Workshop on Coding and Cryptography, University College Cork, Ireland, May 2005

Teaching Experience

(Since Jan 2013 my teaching duties have been limited due to my EPSRC Engineering Leadership Research Fellowship, maternity leave (Jan – Jul 2010; Dec 2012 – Jul 2013; Aug 2016 - Mar 2017) and my role as Director of RISE).

- In 2013/14 I took on the role of **Course Director of a new MSc in Cyber Security**. This involved extensive market research to identify best practice, unique selling points, and the skills requirements of cyber security companies. I introduced internship opportunities into the new programme structure as part of the dissertation study (*commended by the programme's external examiner*).
- In 2015/16 I played an integral role in the **development of a revised MSc in Applied Cyber Security**, with modules delivered in block mode to target industry demand for professional training. The new MSc also offers applicants unique access to a full range of applied skills development and networking opportunities, including entrepreneurship and innovation training.
- I co-ordinated the successful application for provisional **GCHQ certification of the MSc in Cyber Security** in 2016 and assisted with the full certification application, which was successful in early 2017.
- In 2014/15 I developed a new Masters level module on Applied Cryptography for the MSc programme that included practical, hands-on laboratory exercises and a research-informed coursework exercise. I achieved Teaching Evaluation scores of 4.8 and 4.5 out of 5 in 2014/15 and 2015/16 respectively. In 2016/17, I updated and improved the module for **block-mode delivery** to incorporate best-practice for intensive-style learning, achieving a Teaching Evaluation score of 4.6.
- In 2015, I was awarded $25k funding under **Intel's University Program for Curricula design**, which I used to develop a new lab for the Applied Cryptography module.
- In 2017 I adapted the module material for online delivery as part of a pilot scheme with Kainos. I recorded and adapted the material for Queens' online platform. It will be possible to integrate this material into the block-mode delivery of the module to offer blended learning in the future.
- Successfully applied for three NCSC-sponsored undergraduate 8-week internships (offering students £300 per week) to be hosted in CSIT, 2018.
- Level 2 Circuits & Systems (2004 – 2012) with an average teaching evaluation score of 4.3/5.
- Module development and teaching: Level 3 MEng Design Exercise in Telecommunications (2006).

- MSc and Final year project supervision (2004 – present).
- Assessment of Technical Reports for Level 4 MEng Industrial Projects.
- Setting, correcting and second-marking examinations and projects (2004-present).

Academic Leadership

- Appointed **Director of the UK Research Institute in Secure Hardware and Embedded Systems (RISE),** a UK wide collaborative initiative, funded by EPSRC and the National Cyber Security Centre (NCSC). My vision for the research institute is to create a global centre for research and innovation in hardware security, in close collaboration with leading industry and stakeholder partners. A further focus is the translation of RISE research outcomes into products, services and business opportunities for the benefit of the UK economy. My aim is to establish a strong network of national and international collaborators and research partnerships
  - Responsible for the overall budget and the review process for the selection of Research Projects to form part of the research institute. Core project partners include the University of Cambridge, Bristol and Birmingham.
  - I organised a RISE launch event at CSIT, QUB, in November 2017, where the research institute was officially launched by Ciaran Martin, Director of the UK's National Cyber Security Centre.
  - To bring together the UK community in hardware security, I also organised a 2-day RISE Spring School in hardware security at the University of Cambridge, March 2018 and QUB, March 2019.
- Initiated a Memorandum of Understanding (MoU) between RISE/CSIT and the National Research Foundation (NRF), Singapore, concerning co-operation in 'Cybersecurity Research and Development', March 2018.
- **Principal Investigator** of Centre for Secure Information Technologies (CSIT), comprising 10 academics, 15 post-doc researchers and 22 PhD students. Responsible for developing the CSIT research strategy, holding monthly academic meetings, and quarterly all-CSIT networking and review events.
- Technical Director of the Data Security Systems group within CSIT – involved in the direct mentoring, management and appraisal of 4 Lecturers, 1 post-doctoral researcher and 5 PhD students, with 1 further post-doctoral research posts currently advertised.
- I have played a **key leadership role within CSIT** since its establishment and sit on its Senior Management Committee. I led the development of future research directions and played an integral role in the proposal writing for the successful CSIT Phase 2 EPSRC/TSB funding bid of £5M, which will support the centre from 2015-2020. I have also co-ordinated the funders' annual progress reviews.
- I co-ordinated CSIT's successful application to be recognised as an **EPSRC/GCHQ Academic Centre of Excellence in Cyber Security** Research in 2012. I was highlighted in the Award letter as being '*particularly important to the work of the academic centre of excellence'.* This recognition was successfully renewed in 2017.
- As the School of EEECS **SWAN (Scientific Women's Academic Network) Champion** from 2008 to 2015, I co-ordinated the School's successful application for an **Athena SWAN Silver award** in November 2011 and assisted with its renewal in April 2015. These awards recognise and celebrate good practice on recruiting, retaining and promoting women in SET.

Awards

Queen's Anniversary Prize: In 2015, CSIT was awarded a Queen's Anniversary Prize for Higher and Further Education. This is a biennial award scheme within the UK's national honours system and is UK's most prestigious form of national recognition open to a UK academic or vocational institution. CSIT was honoured for its work in strengthening global cyber security.

Fellowship Awards

- **EPSRC Leadership Fellowship** (£1.2M), 2008-2015
  Awarded across the whole of the EPSRC remit and provided up to five year's funding to talented researchers with the most potential to develop into the international research leaders of tomorrow. My award was extended due to maternity leave.
- **Royal Academy of Engineering Research Fellowship**, 2003-2008
  1 of only 8 in the UK to be awarded this prestigious fellowship in 2003

Academic Awards

- **Blavatnik Award for Young Scientists 2019 UK Awards Finalist** – Physical Sciences & Engineering
- Awarded a **UK Royal Academy of Engineering 2014 Silver Medal** which recognises outstanding personal contribution by an early or mid-career engineer that has resulted in successful market exploitation.
- **British Female Inventor of the Year**: British Female Inventors & Innovators (BFIIN) Awards, 2007.
- BFIIN ITEC Platinum Award Winner - Top prize in the Information Technology, Electronics, Communications (ITEC) category at the BFIIN Awards, London, 2007.
- Special recognition award for research on high-speed data security: European **Union Women Inventors & Innovators (EUWIIN) Awards**, Berlin, 2007.
- Short listed in the Young Researcher of the Year category of the **Times Higher Awards** 2007.
- Vodafone award for a research poster on 'Providing High-Speed Data Security': Britain's Younger Engineers Event, House of Commons, London, 2004.

Other Prizes

- Personal Tutor of the Year 2019, QUB Student Union Education Awards, 2019.
- Named as one of 50 people to watch in 2019 (one of 5 in Tech) by the Irish Times, January 2019.
- Named in 'Belfast Top 40 under 40' – one of six to receive a special achievement award, April 2008.
- Named in the 2007 Lá Nua Barr 50 which recognises individuals for their contribution to the Irish language, June 2007.
- Women's Engineering Society prize: **IET Young Woman Engineer of the Year awards**, 2006.
- IEE Leslie H Paddle Scholarship, 1999-2002: Awarded by the IEE for postgraduate research.
- BIT International Outstanding Student of the Year, 2000: Awarded by the Beijing Institute of Technology to ten students worldwide.
- UK Science, Engineering & Technology (SET) Student of the Year for Best Electronic Engineering Student in the UK, 1999.

Contribution to the Community

- **TEDx talk**, Queen's University Belfast, 'Spies and Dolls – The Future of IoT Security', May 2019.
- Registered STEMNET Science and Engineering Ambassador.
- Invited talk to over 50 female students promoting engineering at the Randox STEM Challenge day, Randox Science Park, June 2017.
- Invited talk on Practical Data Security, BelTech conference, Belfast, to >400 post-primary students, 2016.
- Profiled in Marie Claire magazine, Jan 2016.
- I was invited to participate in the **BBC World Service Forum Programme on Codes and Ciphers**, Feb 2015,which has over 210M listeners worldwide (http://www.bbc.co.uk/mediacentre/latestnews/2015/combined-globalaudience). The Forum is a weekly discussion programme, in which '*3 prominent international figures debate their big ideas to each other*' - the panel also included Paul Vigna, Journalist for the Wall Street Journal, and Luciano Floridi, Professor of Philosophy and Ethics of Information, Oxford University.
- Guest of Honour and Invited Speaker at Strathearn School Prize night, Belfast, October 2014 and Bloomfield Collegiate, October 2018.
- Invited to serve on the judging panel for the Undergraduate Awards of Ireland & Northern Ireland, 2011.
- Provided two interactive presentations at the 'Creating the Technology of Tomorrow' events organised to encourage school pupils to study science subjects at QUB, held in W5, , Belfast, SeptDec 2008.
- Judging panel member for the Young Engineers for Britain competition at the Sentinus Young Innovators event, Odyssey Arena, Belfast, 2007, 2011, 2012.
- Invited presentation on to > 400 students at the Belfast Telegraph Lectures for Schools, Feb 2006.
- Participated as a role model in WISE (Women in Science, Engineering and Construction) promotional video aimed at secondary school students in Northern Ireland, 2005.
- Contributed to articles in the Daily Telegraph, the Times, the THES and the Independent promoting women in engineering.

List of Publications

I am either principal supervisor or main author on almost all of the publications listed. Almost all published journal papers are in the top decile journals in my main fields of research, Hardware Security and QCA Circuit Design. More generally, all of the journal papers fall within the top two quartiles of journals in the broader area of Electrical and Electronic Engineering, and all papers published in the last five years fall within the top quartile of such journals - based on SCImago Journal & Country Rank.

Books

- Liu, W, Swartzlander, E.E., O'Neill, M, *Design of Semiconductor QCA Systems*, Artech House, ISBN: 978-1-60807-687-1, 2013.
- McLoone, M., McCanny, J.V.; *System-on-Chip Architectures and Implementations for Private-Key Data Encryption*; Research Monograph, Kluwer Academic/Plenum Publishers, ISBN 0-306-47882-X, 2003.

Book Chapters

- Liu, Q, Gu, C, Qu, G, O'Neill, M, *Approximate Computing and Its Application to Hardware Security: A Tutorial,* Springer book – Cyber-physical Systems Security. Editor, Cetin Koc, December 2018.
- Gu, C, Hanley, N, O'Neill, M, *Lightweight Cryptographic Identity Solutions for the Internet of Things*. In Benjamin Aziz, editor, Engineering Secure IoT Systems, chapter 11. IET, 2016.
- Liu, W, Srivastava, S, O'Neill, M, Swartzlander, E.E, *Security Issues in QCA Circuit Design – Power Analysis Attacks*, Book chapter in Field-Coupled Nanocomputing, Springer LNCS 8280, pp 194-222, September 2013.
- Cao, X., O'Neill, M; "*F-HB+: A Scalable Authentication Protocol for Low-Cost RFID Systems*", Book chapter in 'Current Trends and Challenges in RFID' ISBN 978-953-307-356-9, Chapter 13, Intech Open Access Publisher, *invited submission*, March 2011.
- Smyth, N., McLoone, M., McCanny, J.V.; *WLAN Security Processing Architectures*, Chapter in 'Wireless Security and Cryptography: Specifications and Implementations', editors, N. Sklavos, X. Zhang, CRC-Press, ISBN: 084938771X, March 2007.
- McLoone, M., McCanny, J.V.; *Performance Analysis of SHACAL-1 Encryption Hardware Architectures*; Chapter in 'New Algorithms, Architectures and Applications for Reconfigurable Computing', editors, W. Rosenstiel, P. Lysaght, Kluwer Academic, pp 251-264, ISBN 1-4020-3127-0, 2004.

Special Issue Journal Editorials

- IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Technologies and Designs for Application-Specific Computing, Guest Editors, W. Liu, M. O'Neill, E. Swartzlander, to be published 2017.
- Guest Editor, Journal of Signal Processing Systems, Special Issue on New Frontiers in Signal Processing Applications and Embedded Processing Technologies, Guest Editors, J. McAllister, M. O'Neill and M. Pelcat, Vol. 84, pp 293-294, September 2016.
- ACM Transactions on Embedded Computing Systems, Special Issue on Embedded Computing Platforms for Cryptography in the Coming Decade, Guest Editors, Patrick Schaumont, Maire O'Neill, Tim Guneysu, Vol. 14, No. 3. 41, April 2015.
- IET Information Security Special Issue on Cryptographic Algorithms & Architectures for System-on-Chip, Guest Editors, McLoone, M, Paar, C, Woods, R, Vol.152, Issue 1, October 2005.
- Mobile Networks and Applications (MONET) Journal; Special Issue on Next Generation Hardware Architectures for Secure Mobile Computing', Guest Editors, Sklavos, N, McLoone, M, Zhang, X; Springer-Verlag Publishers, Vol. 12(4), August 2007.

Journal Papers

1. Gu, C, Liu, W, Hanley, N, Hesselbarth, R, O'Neill, M, *A Theoretical Model to Link Uniqueness and Min-Entropy for PUF Evaluations*, IEEE Transactions on Computers, accepted August 2018.

2. Liu, W, Zhang, L, Zhang, Z, Gu, C, Wang, C, O'Neill, M, Lombardi, F, *XOR-Based Low-Cost Reconfigurable PUFs for IoT Security*" ACM Transactions on Embedded Computing Systems, accepted August 2018.

3. Cui, Y, Gu, C, Wang, C, O'Neill, M, Liu, W, *Ultra-lightweight and Reconfigurable Tristate Inverter Based Physical Unclonable Function Design,* IEEE Access, Vol. 6, pp. 28478-28487, May 2018.

4. Liu, W. Mei, F., Wang, C., O'Neill, M, Swartzlander, E.E., *Data Compression Device based on Modified LZ4 Algorithm,* IEEE Transactions on Consumer Electronics, Vol. 64, Issue 1, pp 110-117, February 2018.

5. Rafferty, C, O'Neill, M, Hanley, N Evaluation of Large Integer Multiplication Methods on Hardware, IEEE Transactions on Computers, pp. 1369-1382, Vol. 66, Issue 8, August 2017.

6. Howe, J, Khalid, A, Rafferty, C, Regazzoni, F, O'Neill, M, On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography, IEEE Transactions on Computers, pp. 322-334, Vol. 67, Issue 3, March 2018.

7. Gu, C, Hanley, N, O'Neill, M; *Improved Reliability of FPGA-based PUF Identification Generator Design*, ACM Transactions on Reconfigurable Technology and Systems (TRETS), Article no. 20, Vol. 10, Issue 3, July 2017.

8. O'Neill, M, *Insecurity by Design: Today's IoT Device Security Problem*, Engineering, Vol. 2(1), pp 48-49, Special Section: The Grand Challenges, March 2016.
(*Invited paper based on invited presentation at the 2015 Global Grand Challenges Summit organised by the Chinese, UK and US National Academies of Engineering, Sept 2015*)

9. Cao, X, Moore, C, O'Neill, M, O'Sullivan, E, Hanley, N, *Optimised Multiplication Architectures for Accelerating Fully Homomorphic Encryption*, IEEE Transactions on Computers, pp. 2794 – 2806, Vol. 65, Issue 9, Sept 2016.
One of four papers chosen as IEEE Trans. on Computers 'Editor's pick of the year 2016'.

10. Liu, W, Chen, L, Wang, C., O'Neill, M and Lombardi, F "*Design and Analysis of Inexact Floating-Point Adders*", IEEE Transactions on Computers, Vol.65 (1), Jan 2016.

11. Yu, Y, Wang, C, Liu, W, Cui Y and O'Neill M, "*Improving RO PUF Design Using Frequency Distribution Characteristics*", IEICE Electronics Express, vol. 12, no. 3, pp. 1043-1048, 2015 [Co-supervisor]

12. Wang, Y, O'Neill, M, Kurugollu, F, O'Sullivan, E, *Privacy Region Protection for H.264/AVC with Enhanced Scrambling Effect and a Low Bitrate Overhead*, Vol. 35, pp 71-84, Signal Processing: Image Communication, July 2015.

13. Howe, J, Pöppelmann, T, O'Neill, M, Güneysu, T, O'Sullivan, E, *Practical Lattice-Based Digital Signature Schemes*, ACM Transactions on Embedded Computing Systems, Special Issue on Embedded Computing Platforms for Cryptography in the Coming Decade, Vol. 14, No. 3. Article No. 41, May 2015.

14. Liu, W, O'Neill, M, Swartzlander, E.E , *A First Step Towards Cost Functions for Quantum-dot Cellular Automata Designs*, IEEE Trans on Nanotechnology, Vol. 13 (3), pp 476 – 487, February 2014.

15. Wang, Y, O'Neill, M, Kurugollu, F, *A Tunable Encryption Scheme and Analysis of Fast Selective Encryption for CAVLC and CABAC in H.264/AVC*, IEEE Transactions on Circuits and Systems for Video Technology, Vol 23 (9), pp 1476-1490, Sept 2013.

16. Lu, L, Liu, W, O'Neill, M, Swartzlander, E.E, *QCA Systolic Array Design*, IEEE Transactions on Computers, vol. 62, no. 3, pp.548-560, March 2013.

The IEEE Computing Society invited the authors to submit a presentation of this research for upload to their website and YouTube (https://www.youtube.com/watch?v=z7rtCfsvZSA), which has now received >1300 views.

17. Liu, W, Srivastava, S, Lu, L, O'Neill, M, Swartzlander, E.E, *Are QCA Cryptographic Circuits Resistant to Power Analysis Attack?,* IEEE Transactions on Nanotechnology, vol. 11, no. 6, November 2012.

18. Liu, W, Lu, L, O'Neill, M, Swartzlander, E.E, Woods, R., *Design of Quantum-dot Cellular Automata Circuits Using Cut-Set Retiming,* IEEE Transactions on Nanotechnology, vol. 10, no.5, September 2011.

19. Lu, Y, O'Neill (nee McLoone), M, McCanny, JV, *Evaluation of Random Delay Insertion against DPA on FPGAs*, ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 4, issue 1, December 2010.

20. Wu, J, O'Neill, M, *Ultra-Lightweight True Random Number Generators*, IET Electronics Letters, Vol. 46, Issue 14, pp 988-990, July 2010.

21. O'Neill (nee McLoone), M, Robshaw, M, *Low-Cost Digital Signature Architecture Suitable for RFID Tags,* IET Computers and Digital Techniques, Volume 4, Issue 1, January 2010.

22. Safdar, G.A., O'Neill, M., *A Novel Common Control Channel security framework for Cognitive Radio network*s, International Journal of Autonomous and Adaptive Communications Systems (IJAACS), Special Issue on Cognitive Radio Systems, Inderscience Publishers, Vol. 5, No. 2, pp 125-145, 2012.

23. Safdar, G.A., O'Neill, M., *Performance Analysis of Novel Randomly Shifted Certification Authority Authentication Protocol for MANETs*, EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 243956, 11 pages, January 2009.

24. McLoone, M., McIvor, C; *High-Speed & Low Area Hardware Architectures of the Whirlpool Hash Function*, Invited submission to Journal of VLSI Signal Processing - Special Issue on Field Programmable Technology, Eds. G. Brebner, S. Chakraborty, W-F. Wong, Vol.47(1), pp. 47-57, April 2007.

25. McIvor, C., McLoone, M., McCanny, J.V.; *Hardware Elliptic Curve Cryptographic Processor Over GF(p)*; IEEE Transactions on Circuits & Systems Part I, Volume 53, Issue 9, pp. 1946 – 1957, September 2006.

26. Smyth, N., McLoone M., McCanny, J.V; *WLAN Security Processor;* IEEE Transactions on Circuits & Systems Part I, Volume 53, Issue 7, pp. 1506-1520, July 2006.

27. McLoone, M; *Hardware Performance Analysis of the SHACAL-2 Encryption Algorithm;* IEE Proceedings – Circuits, Devices and Systems, Vol. 152, No. 5, pp. 478-484, October 2005.

28. McIvor, C., McLoone, M., McCanny, J.V.; *Modified Montgomery Modular Multiplication and RSA Processing Techniques*; IEE Proceedings – Computers & Digital Techniques, Vol. 151, No. 6, pp 402-408, November 2004.

29. McIvor, C., McLoone, M., McCanny, J.V.; *Improved Montgomery Modular Inverse Algorithm*; IEE Electronics Letters, Vol. 40, No. 18, September 2004, pp 1110-1111, ISSN 0013-5194.

30. McLoone, M., McCanny, J.V.; *A High Performance FPGA Implementation of DES Using a Novel Method for Implementing the Key Schedule*; IEE Proceedings – Circuits, Devices and Systems, Vol. 150, No. 5, pp. 373-378, October 2003.

31. McLoone, M., McCanny, J.V.; *Rijndael FPGA Implementations Utilizing Look-Up Tables*; Invited submission to Journal of VLSI Signal Processing Systems - Special Issue on Signal Processing Systems, Eds. F. Catthoor, M. Moonen, Kluwer Academic Publishers, vol. 34-3, pp 261-275, 2003

32. McLoone, M., McCanny, J.V.; *Generic Architecture and Semiconductor IP cores for AES Cryptography*; IEE Proceedings – Computers & Digital Techniques, Vol. 150, No. 4, pp. 239-244, July 2003.

Conference Papers

1. Z. Zhang, C. Gu, W. Liu, C. Zhang, Y. Cui, C. Wang, M. O'Neill, Multi-Incentive Delay-Based (Mid) PUF , IEEE International Symposium on Circuits and Systems (ISCAS), Japan, May 2019.
2. Y. Wang, C. Wang, C. Gu, Y. Cui, M. O'Neill, W. Liu, Theoretical Analysis of Delay-Based PUF and Design Strategies for its Improvement, IEEE International Symposium on Circuits and Systems (ISCAS), Japan, May 2019.
3. S. Brannigan, C. Rafferty, A.Khalid, M. O'Neill, Addressing Side-Channel Vulnerabilities in the Discrete Ziggurat Sampler, 8th IACR International Conference on Security, Privacy, and Applied Cryptography Engineering, IIT Kanpur, India, Dec 2018
4. J. Miskelly, C. Gu, Q. Mai, Y. Cui, W. Liu, M. O'Neill, Modelling Attack Analysis of Configurable Ring Oscillator (CRO) PUF Designs, 23rd IEEE International Conference on Digital Signal Processing (IEEE DSP 2018), Shanghai, China, November 2018
5. A. Khalid, C. Rafferty, J. Howe, S. Brannigan, W. Liu, M. O'Neill, Error Samplers for Lattice-Based Cryptography - Challenges, Vulnerabilities and Solutions" IEEE Asia Pacific Conference on Circuits and Systems (APCCAS 2018), October 26-30, 2018, Chengdu, China
6. S. Fan, W. Liu, J. Howe, A. Khalid, M.O'Neill, Lightweight Hardware Implementation of R-LWE Lattice-Based Cryptography, IEEE Asia Pacific Conference on Circuits and Systems (APCCAS 2018), October 26-30, 2018, Chengdu, China.

7. Y. Fang, Q. Ma, C.Gu, C. Wang, M. O'Neill, W. Liu, A Comparative Study of Modeling Attacks On Arbiter PUF, IEEE Asia Pacific Conference on Circuits and Systems (APCCAS 2018), October 26-30, 2018, Chengdu, China.

8. T. Zhang, E. McLarnon, W.Liu, M. O'Neill, F. Lombardi. Design of Majority Logic (ML) Based Approximate Full Adders, IEEE International Symposium on Circuits and Systems (ISCAS), Florence, May 2018.

9. C. Liu, Jian Ni, W.Liu, Z. Liu, M. O'Neill, Design and Optimization of Modular Multiplication for SIDH. IEEE International Symposium on Circuits and Systems (ISCAS), Florence, May 2018.

10. A.Khalid, J. Howe, C.Rafferty, F. Regazonni, M. ONeill, Compact, Scalable, and Efficient Gaussian Samplers for Lattice-Based Cryptography, IEEE International Symposium on Circuits and Systems (ISCAS), Florence, May 2018.

11. Q. Ma, C. Gu, N. Hanley, C. Wang, W. Liu, M. O'Neill, A New Lightweight Machine Learning Attack Resistant Multi Physical Unclonable Function Design, 23rd Asia and South Pacific Design Automation Conference (ASP-DAC 2018), Jan 2018.

12. Howe, J, O'Neill, M, GLITCH: A Discrete Gaussian Testing Suite For Lattice-Based Cryptography, Proceedings of the International Conference on Security and Cryptography (SECRYPT 2017), Spain, July 2017.

13. Howe, J., Khalid, A, Rafferty, C., O'Neill, M, '*Compact and Provably Secure Lattice-Based Signatures in Hardware*, IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, US, 28-31 May 2017

14. Gu, C, Hanley, N, O'Neill, M, '*FPGA-Based Strong PUF with Increased Uniqueness and Entropy Properties'* , IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, US, 28-31 May 2017

15. Y. Cui, C. Wang, W. Liu, M. O'Neill, '*XOR Gates Based Low-Cost Configurable RO PUF'*, IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, US, 28-31 May 2017

16. Regazzoni, F., Khalid, A., O'Neill, M. *Lattice-Based Cryptography: from Reconfigurable Hardware to ASIC*, 15th International Symposium on Integrated Circuits 12-14 Dec 2016.

17. Khalid, A., Howe, J., Rafferty, C., O'Neill, M., *Time-Independent Discrete Gaussian Sampling For Post-Quantum Cryptography*, IEEE International Conference on Field-Programmable Technology (ICFPT 2016), 7-9 December 2016

18. Y. Cui, C. Wang, W. Liu, M. O'Neill, '*A Reconfigurable Memory PUF based on Tristate Inverter Arrays'*, IEEE International Workshop on Signal Processing Systems (SiPS 2016) Dallas, US, October 2016

19. Gu, C, Cui, Y, Hanley, N, O'Neill, M, *'Novel Lightweight FF-APUF Design for FPGA*' IEEE International System-on-Chip Conference (SOCC), Seattle, US, September 2016.

20. Howe, J., Moore, C., O'Neill, M., Regazzoni, R., Guynesu, T., Beeden, K., *Shelter from the Storm: Lattice-Based Encryption over Standard Lattices in Hardware*, Article No. 162, ACM Design Automation Conference (DAC), Austin, June 2016.

21. O'Neill, M, O'Sullivan, E., McWilliams, G., Saarinen, M-J, Moore, C., Khalid, A., Howe, J., delPino, R., Abdalla, M., Regazzoni, F. Valencia, F., Guneysu, T. Oder, T., Waller, A., Jones, G., Barnett, A., Griffin, R., Byrne, A., Ammar, B., Lund, D., Secure Architectures of Future Emerging Technology – SAFEcrypto (Invited Paper), ACM Intl Conference on Computing Frontiers (CF 2016), pp 315-322, Italy, May 2016.

22. Cui, Y., Wang, C, Liu, W., O'Neill, M., Lombardi, F. *Low-Cost Configurable Ring Oscillator PUF with Improved Uniqueness*, 2016 IEEE Int'l Symposium on Circuits & Systems, Montreal, May 2016.

23. Won, Y-S, Hodgers, P, O'Neill, M, and Han, D-G, *On the Security of Balanced Encoding Countermeasures*, 14th Smart Card Research and Advanced Application Conference (CARDIS), LNCS vol 9514, p. 242-256, Nov 2015, Germany.

24. Kang, Y.S, O'Sullivan, E., Choi, D., O'Neill, M, *Security Analysis on RFID Mutual Authentication Protocol*, 16th International Workshop on Information Security Applications (WISA 2015), LNCS vol. 9503, pp. 65-74, Jeju Island, Korea, August 20-22, 2015.

25. Ahn, H-J, Hanley, N, O'Neill, M, Han, D-G, *An Improved Second-Order Power Analysis Attack Based on a New Refined Expecter - Case study on protected AES*, 16th International Workshop on Information Security Applications (WISA 2015), LNCS vol. 9503, pp. 174-186, Jeju Island, Korea, August 20-22, 2015.

26. Gilmore, R, Hanley, N, O'Neill, M, *Neural Network Based Attack on a Masked Implementation of AES*, IEEE Intl. Symposium on Hardware-Oriented Security and Trust (HOST), US, May 2015.

27. Liu, W, Yu, Q, Wang, C, Cui, Y, O'Neill, M, *RO PUF Design in FPGAs Using Frequency Distribution Characteristics*, 2015 IEEE Int'l Symposium on Circuits & Systems, Lisbon, May 24-27, 2015.

28. Gu, C, Hanley, N, O'Neill, M, *Ultra-Compact and Robust FPGA-Based PUF Identification Generator*, 2015 IEEE Int'l Symposium on Circuits & Systems, Lisbon, May 24-27, 2015

29. Hodgers, P, Hanley, N, O'Neill, M, *Pre-Processing Power Traces to Defeat Random Clocking Countermeasures,* 2015 IEEE Int'l Symposium on Circuits & Systems, Lisbon, May 24-27, 2015.

30. Tian, Q, O'Neill, M, Hanley, N *Can Leakage Models Be More Efficient? Non-Linear Models in Side Channel Attacks,* IEEE Intl. Workshop on Information Forensics and Security (WIFS'14), Atlanta, US, December 2014.

31. Wang, Y, O'Neill, M, Kurugollu, F, *New FMO Type to Flag ROI in H.264/AVC*, 5th European Workshop on Visual Information Processing (EUVIP), December 10-12, 2014, Paris, France, 2014

32. N. Hanley, M. O'Neill, M. Tunstall, L. Marnane, *Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks,* IEEE Workshop on Signal Processing Systems (SiPS), Belfast, October 2014.

33. Moore, C, O'Neill, M. Hanley, N, O'Sullivan, E, *Accelerating Integer-based Fully Homomorphic Encryption using Comba Multiplication*, IEEE Workshop on Signal Processing Systems (SiPS), Belfast, October 2014.

34. Liu, W, Chen, L, Wang, C, O'Neill, M, Lombardi, F, *Inexact Floating-Point Adder for Dynamic Image Processing,* 14th IEEE International Conference on Nanotechnology (IEEE Nano 2014), Toronto, August 2014.

35. McLarnon, E, O'Neill, M, Liu, W, Hanninen, I, *Bit Erasure Analysis of Binary Adders in Quantum-dot Cellular Automata*, 14th IEEE International Conference on Nanotechnology (IEEE Nano 2014), Toronto, August 2014.

36. Moore, C, O'Neill, M. O'Sullivan, E, Y, Doroz, B. Sunar, *Towards Practical Homomorphic Encryption*, IEEE International Symposium on Circuits and Systems (ISCAS), Melbourne, June 2014.

37. C. Gu, J. Murphy, M. O'Neill, *A Unique and Robust Single Slice FPGA Identification Generator*, IEEE International Symposium on Circuits and Systems (ISCAS), Melbourne, June 2014.

38. Cao, X, Moore, C, Hanley, N, O'Neill, M. O'Sullivan, E, *High-Speed Fully Homomorphic Encryption over the Integers*, 2nd Workshop on Applied Homomorphic Cryptography and Encrypted Computing- associated with Financial Cryptography and Data Security 2014, Barbados, March 2014.

39. Wang, Y, O'Neill, M, Kurugollu, F, "*A Tunable Selective Encryption Scheme for H.264/AVC*"4th European Workshop on Visual Information Processing (EUVIP), June 10-12, 2013, Paris, France

40. Hodgers, P, Hanley, N, O'Neill, M, *Pre-Processing Power Traces with a Phase-Sensitive Detector*, IEEE Intl. Symposium on Hardware-Oriented Security and Trust (HOST), Austin, Texas, June 2013. **BEST PAPER**

41. L Liu, W, Srivastava, S, Lu, L, O'Neill, M, Swartzlander, E.E, *Power Analysis Attack of QCA Circuits: a Case Study of the Serpent Cipher*, IEEE International Symposium on Circuits and Systems (ISCAS), Beijing, May 2013.

42. Wang, Y, O'Neill, M, Kurugollu, F, *Partial Encryption by Randomized Zig-Zag Scanning for Video Encoding*, IEEE International Symposium on Circuits and Systems (ISCAS), Beijing, May 2013.

43. Wang, Y, O'Neill, M, Kurugollu, F, '*Privacy Region Protection for H.264/AVC by Encrypting the Intra Prediction Modes without Drift Error in I Frames,* 38th International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Vancouver, Canada, May 2013.

44. Moore, C, Hanley, N, McAllister, J, O'Neill, M. O'Sullivan, E, Cao, X, *Targeting FPGA DSP Slices for a Large Integer Multiplier for Integer Based FHE, 2013 Workshop on Applied Homomorphic Cryptography*, Japan, April 2013.

45. Wang, Y, O'Neill, M, Kurugollu, F, *The Improved Sign Bit Encryption Of Motion Vectors For H.264/AVC*, 20th European Signal Processing Conference (EUSIPCO), Bucharest, August 2012.

46. Hanley, N, O'Neill, M, *Hardware Comparison of the ISO/IEC 29192-2 Block Ciphers with Side-Channel Experiments*, IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2012), pp. 57-62, Amherst, US, 2012.

47. Liu, W, O'Neill, M, Swartzlander, E.E , *A Review of QCA Adders and Metrics*, 46th Asilomar Conference, Monterey, September 2012.

48. Cao, X, O'Neill, M, *Scaling Modular Multiplication to the Minimum*, 23nd IET Irish Signals and Systems Conference – (ISSC 2011), Maynooth, June 2012.

49. Murphy, J, O'Neill, M, Burns, F, Bystrov, A., Yakovlev, A, Self-timed Physically Unclonable Functions, IFIP International Conference on New Technologies, Mobility and Security (NTMS 2012), Turkey, May 2012.

50. Cao, X, O'Neill, M, *Application-Oriented SHA-256 Hardware Design for Low-Cost RFID*, IEEE International Symposium on Circuits and Systems (ISCAS), Seoul, South Korea, May 2012.

51. Liu, W, Lu, L, O'Neill, M, Swartzlander, E.E; *Cost-Efficient Decimal Adder Design in Quantum-Dot Cellular Automata*, IEEE International Symposium on Circuits and Systems (ISCAS), Seoul, South Korea, May 2012.

52. Wang, Y, O'Neill, M, Kurugollu, F, *Adaptive Binary Mask for Privacy Region Protection*, IEEE International Symposium on Circuits and Systems (ISCAS), Seoul, South Korea, May 2012.

53. Cao, X, O'Neill, M, *A Private and Scalable Authentication for RFID Systems Using Reasonable Storage*, 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11), Changsha, China, Nov, 2011.

54. Hodgers, P, Boey, K.H, O'Neill, M, *Variable Window Power Spectral Density Attack,* IEEE Intl. Workshop on Information Forensics and Security (WIFS'11), Brazil, November 2011.

55. Hodgers, P, Boey, K.H, O'Neill, M, *Power Spectral Density Side-Channel Attack Overlapping Window Method*, 14th EUROMICRO Conference on Digital System Design (DSD 2011), September 2011, Finland.

56. Cao, X, O'Neill, M, *A Forward Private Protocol Based on PRNG and LPN For Low-Cost RFID*, Proceedings of the International Conference on Security and Cryptography (SECRYPT 2011), Spain, July 2011, INSTICC Press, 2011.

57. Cao, X, Lu, L, O'Neill, M, *A Compact SHA-256 Architecture for RFID Tags,* 22nd IET Irish Signals and Systems Conference – (ISSC 2011), Dublin, June 2011.

58. Liu, W, Lu, L, O'Neill, M, Swartzlander, E.E; *Design Rules for Quantum-dot Cellular Automata*, IEEE International Symposium on Circuits and Systems (ISCAS), pp. xxx, Brazil, May 2011.

59. Cao, X, O'Neill, M, F-HB: *An Efficient Forward Private Protocol,* Workshop on Lightweight Security & Privacy Devices, Protocols, and Applications (LightSec 2011), March 2011.

60. Boey, K.H, Lu, Y, O'Neill, M, Woods, R, *How resistant are SBoxes to Power Analysis Attacks?,* IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011), Paris, Feb. 2011.

61. Boey, K.H, Lu, Y, O'Neill, M, Woods, R, *'Security of AES Sbox Designs to Power Analysis*' 17th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Greece, December 2010.

62. Boey, K.H, Lu, Y, O'Neill, M, Woods, R, *'Random Clock against Differential Power Analysis'*, IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Kuala Lumpur, December 2010.

63. Lu, Y, Boey, K.H, O'Neill, M; *'SEED Masking Implementations against Power Analysis Attacks'*, IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Kuala Lumpur, December 2010.

64. Lu, Y, Boey, K.H, O'Neill, M; 'Li*ghtweight DPA Resistant Solution on FPGA to Counteract Power Models'*; IEEE International Conference on Field-Programmable Technology (ICFPT), Beijing, December 2010.

65. Moore, P, O'Neill, M, McLaughlin, K, Sezer, S, *A High-Speed Key Exchange Multi-Core SoC Architecture for IPSec Real-Time Internet Traffic*, IEEE Globecom 2010 Workshop on Multimedia Communications and Services (MCS 2010), Miami, December 2010.

66. Liu, W, Lu, L, O'Neill, M, Swartzlander, E.E, *Montgomery Modular Multiplier Design in Quantum-dot Cellular Automata Using Cut-Set Retiming,* 10th IEEE International Conference on Nanotechnology (IEEE Nano 2010), Soeul, Korea, August 2010.

67. Boey, K.H, Lu, Y, O'Neill, M, Woods, R, *Differential Power Analysis of CAST-128*, IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2010), pp. 143-148, Greece, July 2010.

68. Lu, L, Liu, W, O'Neill, M, Swartzlander, E.E, *QCA Systolic Matrix Multiplier*, IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2010), pp. 149-154, Greece, July 2010.

69. Baldwin, B, Hanley, N, Hamilton, M, Lu, L, Byrne, A, O'Neill, M, Marnane, W.P., *FPGA Implementations of the Round Two SHA-3 Candidates*, Second SHA-3 Candidate Conference, Santa Barbara, August 2010.

70. Baldwin, B, Byrne, A, Lu, L, Hamilton, M, Hanley, N, O'Neill, M, Marnane, W.P*, FPGA Implementations of the Round Two SHA-3 Candidates*, 20th International Conference on Field Programmable Logic and Applications, (FPL 2010), Italy, August 2010. At the 25th FPL conference, held in London, 2015, this publication was selected as one of the **top 27 papers over the 25 year history of the conference '*deemed to have most strongly influenced theory and practice in the field*.'**

71. Baldwin, B, Byrne, A, Lu, L, Hamilton, M, Hanley, N, O'Neill, M, Marnane, W.P, *A Hardware Wrapper for the SHA-3 Hash Algorithms*, IET Irish Signals and Systems Conference (ISSC), June 2010.

72. Lu, Y, Boey, K.H, O'Neill, M, McCanny, JV; *Differential Power Analysis Resistance of Camellia and Countermeasure Strategy*; IEEE International Conference on Field-Programmable Technology (FPT), pp. 183 - 189, Australia, December 2009.

73. Lu, Y, Boey, K.H, O'Neill, M, McCanny, JV, Satoh, A; *Is the Differential Frequency-Based Attack Effective Against Random Delay Insertion?*, IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, pp. 51-56, Finland, October 2009.

74. Lu, L, O'Neill, M, Swartzlander, E. Jnr, *ASIC Evaluation of ECHO Hash Function*, 22nd IEEE International System-on-Chip Conference (SOCC), pp.387-390, Belfast, September 2009.

75. Lu, Y, Boey, K.H, O'Neill, M, McCanny, JV; *Practical Comparison of Differential Power Analysis Techniques on an ASIC Implementation of the AES Algorithm*; IET Irish Signals and Systems Conference – (ISSC 2009), pp.1-6, June 2009.

76. Safdar, G.A., O'Neill, M; *Common Control Channel Security Framework for Cognitive Radio Networks*, IEEE 69th Vehicular Technology Conference: VTC2009-Spring, pp. 1-5,Barcelona, Spain, April 2009.

77. Lu, Y, O'Neill (nee McLoone), M, McCanny, JV; *FPGA Implementation and Analysis of Random Delay Insertion Countermeasure against DPA*, IEEE International Conference on Field-Programmable Technology (FPT), pp.201-208, Taiwan, December 2008.

78. O'Neill (nee McLoone), M; *Low-Cost SHA-1 Hash Function Architecture for RFID Tags*, Proceedings of the 4th Workshop on RFID Security (RFIDSec08), pp. 41 – 51, Budapest, July 2008.

79. Lu, Y, O'Neill (nee McLoone), M, McCanny, JV; *Differential Power Analysis Attack of a SHACAL-2 Hardware Implementation*; IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2933-2936, Seattle, May 2008.

80. McCanny, JV, Sezer, S, O'Neill (nee McLoone), M; *Exploring Technology Related Design-Space Limitations of High Performance Network Processing*; Invited Paper, IEEE European Solid State Circuits Conference (ESSCIRC), pp. 222-231, September 2007.

81. McGrath, C., Safdar, G.A., McLoone, M; *Identity Based Public Key Exchange (IDPKE) for Wireless Ad Hoc Networks*, in Proceedings of the International Conference on Security and Cryptography (SECRYPT 2007), pp. 167-170, Barcelona, Spain, July 2007, INSTICC Press, 2007.

82. Safdar, G.A., McLoone, M; *Randomly Shifted Certification Authority Authentication Protocol for MANETs*, 16th IST Mobile & Wireless Communications Summit, pp.1-5, Budapest, July 2007.

83. McLoone, M, Robshaw, M, *New Architectures for Low-Cost Public Key Cryptography on RFID Tags*, IEEE International Symposium on Circuits and Systems (ISCAS); pp. 1827-1830 New Orleans, May 2007.

84. Moore, P., McLoone M. Sezer, S.; *Investigation into Hardware/Software Partitioning within the IKE-V2 System*'; 15th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA), Monterey, California, February 2007.

85. McLoone, M, Robshaw, M, *Public Key Cryptography and RFID Tags*, RSA Conference 2007, Cryptographers' Track (CT-RSA 2007), LNCS 4377, pp. 372 – 384, San Francisco, February 2007.

86. Smyth, N., McLoone M., McCanny, *An Adaptable and Scalable Asymmetric Cryptographic Processor*, 17th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP 2006), Colorado, September 2006.

87. Safdar, G.A., McGrath, C, McLoone, M; *Existing Wireless Network Security Mechanisms and their Limitations for Ad Hoc Networks*; IET Irish Signals and Systems Conference – (ISSC 2006), pp. 197-202, June 2006.

88. McGrath, C, Safdar, G.A., McLoone, M; *Novel Authenticated Key Management Framework for Ad Hoc Network Security*; IET Irish Signals and Systems Conference – (ISSC 2006), pp. 185-190, June 2006.

89. Safdar, G.A., McGrath, C, McLoone, M; *Limitations of Existing Wireless Network Authentication and Key Management Techniques for MANETs*; IEEE International Symposium on Computer Networks (ISCN'06), pp. 101-105, Istanbul, June 2006.

90. McLoone, M., Mc Ivor, C., Savage, A.; *High-Speed Hardware Architectures of the Whirlpool Hash Function*; IEEE International Conference on Field-Programmable Technology (FPT), pp.147-154, Singapore, December 2005.

91. Mc Ivor, C., McLoone M., McCanny, J.V; *High-Radix Systolic Modular Multiplication on Reconfigurable Hardware*; IEEE International Conference on Field-Programmable Technology (FPT), pp. 13-18, Singapore, December 2005.

92. Smyth, N., McLoone M., McCanny, J.V; *Reconfigurable Processor for Public Key Cryptography*; IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, Athens, November 2005.

93. McCanny, JV, Sezer, S, McLoone, M; *Reconfigurable SoC Architectures for High Bandwidth Network Processing Systems*; Invited Paper, IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, Athens, November 2005.

94. Moore, P., McLoone M. Sezer, S.; *Reconfigurable Instruction Interface Architecture for Private-Key Cryptography on the Altera NIOS-II Processor*, Advanced Industrial Conference on Telecommunications (AICT 2005), Lisbon, Portugal, July 2005.

95. Sezer, S, McLoone M., McCanny, J.V; *Reconfigurable Architectures for Network Processing*, Invited Paper, IEEE VLSI-TSA International Symposium on VLSI Design, Automation, and Test (VLSI-TSA-DAT), Taiwan, April 2005.

96. Smyth, N., McLoone M., McCanny, J.V; *Reconfigurable Cryptographic RISC Microprocessor*; IEEE VLSI-TSA International Symposium on VLSI Design, Automation, & Test (VLSI-TSA-DAT), Taiwan, April 2005.

97. McLoone, M., Mc Ivor, C., McCanny, J.V.; *Coarsely Integrated Operand Scanning (CIOS) Architecture for High-Speed Montgomery Modular Multiplication*; IEEE International Conference on Field-Programmable Technology (FPT), pp 185-192, Brisbane, December 2004.

98. McLoone, M., Mc Ivor, C., McCanny, J.V.; *Montgomery Modular Multiplication Architecture for Public Key Cryptosystems*; IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, pp. 349-354, Texas, October 2004.

99. Smyth, N., McLoone M., McCanny, J.V.; *Reconfigurable Hardware Acceleration of WLAN Security*; IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, pp 194-199, Texas, October 2004.

100. Smyth, N., McLoone M., McCanny, J.V; *Microprocessor Architecture for Private-Key Cryptography*; IEE Irish Signals and Systems Conference – (ISSC 2004), June 2004.

101. Mc Ivor, C., McLoone M., McCanny, J.V; *An Elliptic Curve Cryptographic Accelerator Over GF(p)* ; IEE Irish Signals and Systems Conference – (ISSC 2004), June 2004.

102. Mc Ivor, C., McLoone M., McCanny, J.V; *Fast Montgomery Multiplier Architectures Suitable for ECCs Over GF(p)*; IEEE International Symposium on Circuits and Systems (ISCAS); May 2004.

103. Mc Ivor, C., McLoone M., McCanny, J.V; *FPGA Montgomery Multiplier Architectures – A Comparison*; IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM); California, April 2004.

104. Mc Ivor, C., McLoone M., McCanny, J.V., Daly, A., Marnane, W.; *Fast Montgomery Modular Multiplication and RSA Cryptographic Processor Architectures*; 37th Annual Asilomar Conference on Signals, Systems and Computers, November 2003.

105. McLoone, M, McCanny, J.V.; *Very High Speed 17 Gbps SHACAL Encryption Architecture*; International Conference on Field Programmable Logic and Applications (FPL); pp. 111-120, Lisbon, Portugal, September 2003.

106. McIvor C., McLoone, M., McCanny, J.V.; *A High-Speed, Low Latency RSA Decryption Silicon Core*; IEEE International Symposium on Circuits and Systems (ISCAS); Thailand, May 2003.

107. McLoone, M., McCanny, J.V.; *Efficient Single-Chip Implementation of SHA-384 & SHA-512*; IEEE International Conference on Field-Programmable Technology (FPT), pp311-314, Hong Kong, December 2002.

108. McLoone, M., McCanny, J.V.; *A Single-Chip IPSec Cryptographic Processor*; IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, pp133-138; USA, Oct 2002.

109. McLoone, M., McCanny, J.V.; *Rijndael FPGA Implementation Utilising Look-Up Tables*; IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, pp349-359, Antwerp, Belgium, September 2001.

110. McLoone, M., McCanny, J.V.; *Single-Chip FPGA Implementation of Advanced Encryption Standard Algorithm*; International Conference on Field Programmable Logic and Applications (FPL); Springer-Verlag, pp152-161, August 2001.

111. McLoone, M., McCanny, J.V.; *High Performance FPGA Implementation of Rijndael;* Irish Signals and Systems Conference - ISSC 2001, Eds. R. Shorten, T. Ward, T. Lysaght, ISBN 0-9015-1963-4, pp415-420, NUI Maynooth, Ireland, June, 2001.

112. McLoone, M., McCanny, J.V.; *High Performance Single-Chip FPGA Rijndael Algorithm Implementations*; Workshop on Cryptographic Hardware and Embedded Systems (CHES'01); Springer-Verlag, pp65-77, Paris, May 2001.

113. McLoone, M., McCanny, J.V.*A High Performance Implementation of DES*; IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation, pp374-383, Louisiana, October 2000.