Institution: Royal Holloway, University of London		
Unit of Assessment: 10 Mathematical Sciences		
Title of case study: Formulating policy and practice for postquantum cryptosystems		
Period when the underpinning research was undertaken: 2000-2020		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Martin Albrecht,	Professor	2015 - date
Simon Blackburn,	Professor	1995 - date
Carlos Cid,	Professor	2005 - date
Rachel Player	Lecturer	2019 - date
Period when the claimed impact occurred: 2016- December 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Cryptographers at Royal Holloway, University of London (RHUL) have used their expertise to fundamentally influence the information security industry's policy on post-quantum cryptosystems: modern cryptographic schemes designed to be secure in a *post-quantum* world in which quantum computers are practical. Through a combination of the influence of their published papers and direct contributions, RHUL research has had a major impact on the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardisation Project, the highest-profile mechanism for industry-wide policy debate on best practice for post-quantum systems. Beneficiaries include a range of organisations with interests in cryptography for long-term secrets who need these cryptosystems now, including government organisations such as NIST itself, and companies such as Amazon Web Services, Philips, and Thales.

2. Underpinning research

The team of RHUL researchers in mathematical cryptology who contributed to this impact case study are all experts in post-quantum cryptography: the study of cryptographic mechanisms that can run on classical computers but are designed to remain secure if an adversary has access to a quantum computer.

The security of popular public-key cryptographic algorithms, which underpin the security of modern digital infrastructure, is based on the difficulty of mathematical problems such as integer factorisation and discrete logarithm problems. Though these problems seem to be hard for a classical computer, they can be efficiently solved by future quantum computers using Shor's algorithm. Post-quantum cryptography studies alternative mathematical problems, in (for example) coding theory, lattice theory, and group theory; algorithms for solving these problems are produced, the difficulty of solving these problems is estimated, and techniques for using these problems in cryptography are studied. Industrial interest in the area is now significant, as the estimated date for practical implementation of Shor's algorithm is now well-within the lifetime of current long-term secrets protected by cryptography.

The team's research referred to below (with RHUL authors in bold) represents a sample of a body of work in a long-running tradition of post-quantum cryptography at RHUL, giving an indication of the breadth of the team's theoretical research. Outputs include novel algorithms to solve mathematical problems in lattice theory [R1,R5] and in braid group representation theory [R3]; a new complexity-theoretic analysis [R2] of pre-existing lattice-based algorithms; a new theoretical clarity [R4] to statistical notions first proposed in the analysis of lattice-based post-

quantum cryptographic primitives; and a demonstration [R6] that a class of lattice reduction algorithms is competitive in practice and should therefore be considered in the security assessment of lattice-based schemes. All these outputs increase our understanding of the difficulty of problems on which post-quantum schemes are based, and so have a direct bearing on their design and security.

3. References to the research

R1. **Martin Albrecht**, Shi Bai, and Léo Ducas. "A subfield lattice attack on overstretched NTRU assumptions". In: CRYPTO 2016. Springer. 2016, pp. 153–178. url: https://link.springer.com/chapter/10.1007/978-3-662-53018-4_6.

R2. **Martin R. Albrecht**, **Carlos Cid**, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. "On the complexity of the BKW algorithm on LWE". in: Designs, Codes, and Cryptography 74.2 (Feb. 2015), pp. 325–354. issn: 0925-1022 (print), 1573-7586 (electronic). doi: http://dx.doi.org/10.1007/s10623-013-9864-x.

R3. Adi Ben-Zvi, **Simon R. Blackburn**, and Boaz Tsaban. "A Practical Cryptanalysis of the Algebraic Eraser". In: CRYPTO 2016, Part I. ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. LNCS. Springer, Heidelberg, Aug. 2016, pp. 179–189. doi: https://doi.org/10.1007/978-3-662-53018-4_7.

R4. **Sean Murphy** and **Rachel Player**. "δ-subgaussian Random Variables in Cryptography". In: Australasian Conference on Information Security and Privacy. Springer. 2019, pp. 251–268. url: https://link.springer.com/chapter/10.1007%2F978-3-030-21548-4_14.

R5. **Martin R. Albrecht**. "On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HElib and SEAL". in: Advances in Cryptology – EUROCRYPT 2017. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Cham: Springer International Publishing, 2017, pp. 103–129. url: https://link.springer.com/chapter/10.1007/978-3-319-56614-6_4.

R6. **Martin R Albrecht**, Léo Ducas, Gottfried Herold, Elena Kirshanova, **Eamonn W Postlethwaite**, and Marc Stevens. "The general sieve kernel and new records in lattice reduction". In: EUROCRYPT 2019. Springer. 2019, pp. 717–746. url: https://link.springer.com/chapter/10.1007/978-3-030-17656-3_25.

All the publications above have been subject to a rigorous peer-review process, and appear in well-thought-of venues; CRYPTO and EUROCRYPT are universally recognised as in the top rank of publication venues (ranking both conferences and journals) in the field of cryptography [E1], with an acceptance rate of below 25% over the last few years.

Funding:

- Albrecht (PI), EPSRC first grant (EP/P009417/1) "Bit Security of Learning with Errors for Post-Quantum Cryptography and Fully Homomorphic Encryption", 2017-2019, GBP80,000.
- Albrecht (local PI), EU H2020 project on lattice-based cryptography "Prometheus", 2017-2021, EUR465,000.
- Albrecht (PI), EPSRC standard research grant (EP/S020330/1) "Lattice-Based Cryptography", 2019-2022, GBP482,000 (project partner: Cloudflare).
- Albrecht (PI), EPSRC standard research grant (EP/S02087X/1) "Bridging the Gap Between Lattice Coding and Lattice Cryptography - Post-Quantum Cryptography", 2019-2022, GBP380,000.

4. Details of the impact

Our research has influenced understanding, policies and practices of the information security industry, when constructing and assessing postquantum cryptosystems. This impact is evidenced by the NIST postquantum standardisation process. We describe: (4a) the NIST process itself; (4b) the ways in which our research was used to inform and influence the process; (4c) quotes from a sample of beneficiaries to document the reach and significance of the process.

4a Influencing the NIST Postquantum Standardisation Process:

Secure encryption is of critical importance to the economy and society: *The Economic Impacts of the Advanced Encryption Standard, 1996-2017* [Chen et al, E2] commissioned by NIST (part of the U.S. Department of Commerce, responsible for standardisation across many areas in order to promote U.S. industrial competitiveness) estimated that the economic benefits of the NIST AES standardisation alone were over USD250,000,000,000 (2017).

All public key algorithms commonly standardised, such as RSA, Diffie-Hellman, ElGamal and Elliptic Curve variants, are based on problems that become tractable (using Shor's algorithm) if an adversary has access to a quantum computer: "*a sufficiently powerful quantum computer will put many forms of modern communication – from key exchange to encryption to digital authentication – in peril*" [Chen et al, E2]. Many applications, such as the digital signing of long-term contracts or encryption of sensitive medical information, require underlying cryptographic algorithms to remain secure for 15-25 years or more. And yet "*researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars. This is a serious long-term threat to the cryptosystems currently standardized by NIST*" [Chen et al, E2]. This situation resulted in a global demand for post-quantum cryptosystems: designed to operate on today's hardware but remaining secure if an adversary has access to a quantum computer.

In 2016 the NIST Post-Quantum Cryptography standardisation process [E2] was initiated with the aim to define best practice for practical cryptographic algorithms that the international community would regard as secure for wide deployment in the post-quantum world. The process is a policy debate, taking the form of an international public competition split into rounds. Teams of cryptographic experts submit algorithms; these are scrutinised by the community; unsuitable submissions are removed, and others are merged; the scrutiny repeated until a trusted portfolio of ciphers emerges. There have been three rounds in total, with the most highly recommended submissions forming a group of finalists, identified on 22 July 2020. This process has influence beyond NIST to other arenas: For example, the Head of International Standards at the UK National Cyber Security Centre chairs the ETSI TC CYBER QSC Working Group, which was established in 2015 with the aim to assess and recommend quantum-safe cryptographic primitives and protocols for the European standardisation organisation ETSI, writes that the Group has been following the NIST post-quantum standardisation process closely [E3]. Royal Holloway research has been integral to this policy debate.

4b How our work was used in the NIST process:

The work of RHUL researchers has been a major influence on the NIST Post-quantum standardisation process, ensuring that the final portfolio of algorithms is accepted by the international community and giving companies the confidence to deploy products with a clear expectation of what the future post-quantum standard will be. **39% of all submissions and 73% of the finalists used the RHUL team's research**, either citing their research in their specification document in support of their design decisions, or making use of the researchers' expertise directly as a contributor to the proposal. (Cipher specifications and submission documents are available via the NIST Postquantum website [E2].) **A total of 19 outputs** written by team members have been cited by algorithm designers as part of the NIST process [E4]. These publications are a mix of theoretical outputs such as those above, and applied outputs written specifically to address issues relevant to the process. Moreover:

RHUL support for successful *Round 3* finalists: Albrecht and Cid are part of the submission team of *Classic McEliece,* one of the four finalists for Key Encapsulation Mechanisms (KEMs). The submission is the result of the merger with the 2nd round submission *NTS-KEM*, of which they were also part of the design team. NTS-KEM was joint work with industry partner PQ Solutions, who "*invited RHUL to be part of the submission team because of the contribution*

made by RHUL in the evolution and refinement of NTS-KEM from the original NTS scheme […and] *because of their very high reputation both internationally as well as nationally and the quality of their recent outstanding publications*" [E5].

Research in establishing concrete costs for solving the Learning with Errors (LWE) problem [E3], which underlies post-quantum cryptosystem security, served as foundation for the parameter choices of round 3 finalists *CRYSTALS-KYBER*, *Frodo*, *NTRU*, *NTRU Prime*, *qTESLA*, and *SABER.* RHUL research concerned with the asymptotic difficulty of solving hard problems on general and algebraic lattices [E4] is cited by both *Falcon* and *NTRU Prime.*

The U.S. National Security Agency (NSA) states that they "*are confident in those lattice-based schemes with strong dependence on well-studied mathematical problems*" [E9]. This public statement illustrates the importance of the underpinning role of the study of these underlying problems; four of the five lattice-based finalists cite the RHUL team's work.

RHUL influence on the selection process: Critical for confidence in the NIST process is the efficient scrutiny of submissions. Both optimising the choices and rejecting weak submissions are essential in the process. RHUL research showing that two post-quantum underpinning problems (Ring-LWE and Module-LWE) are equivalent in difficulty [E3] led NIST to advance Module-LWE-based schemes *Kyber*, *Saber* and *Dilithium* into the 3rd round over Ring-LWE counterparts [E2, Apon]. Research by Blackburn [E3] was instrumental in the elimination of *WalnutDSA*, which depends on a problem in the representation theory of braid groups.

The Chief Scientist Thales UK writes: "*We recognise the significant contribution of the researchers at Royal Holloway to the NIST PQC process: their work has had a widespread and positive influence. Martin Albrecht and Rachel Player's parameter selection tool and related underpinning theoretical work has informed many of the lattice-based algorithm designs in the NIST process, and we have made direct use of this work in our evaluations. We also very much appreciate Simon Blackburn's role in removing weak candidates (in particular WalnutDSA) from consideration... All this work is fundamental to our confidence in the process.*" [E6]

4c Defining best practice, developing understanding, implementation and deployment:

The NIST Post-Quantum Standardization Process is the first major initiative in this area and is highly influential in defining best practice. Beneficiaries of the process include agencies and companies needing to understand, develop or implement public-key cryptosystems, and the wider information security industry aiming to advise clients on quantum-safe options. Amazon Web Services, Philips, PQ Solutions Ltd, Thales UK are exemplars of interested parties [E5-8]. Round 3 finalists are already recommended by agencies in areas where long term security is critical. For example, both the NSA [E9] and its German counterpart BSI have already expressed opinions on candidates and primitives. BSI writes "*From the BSI's point of view, security is our top priority. The lattice-based algorithm FrodoKEM and the classic McEliece code-based method are the most conservative choices. […These] two algorithms mentioned are recommended if a manufacturer or user* ***already wants to use a quantum computer-resistant procedure for key update***" (translated from [E10]).

Matt Ball, Chief Scientist of Thales UK, writes: "*The NIST PQC standardisation process is the most significant international development over the last few years,* ***performing a vital role in establishing best-practice****, deepening our understanding of PQC, and in suggesting candidate PQC algorithms whose security and performance have been rigorously tested*" [E6].

The Senior Standardisation Officer at Philips states "[W]*e felt it was essential to invest in developing secure and performant quantum-safe alternatives. We saw the NIST process as* ***the most important worldwide initiative towards this goal***" [E7].

RHUL independent security analysis has supported PQ Solutions deployment of novel post-quantum products. CSO and Chairman of PQ Solutions Ltd writes *"[W]e are already developing*

PQ products based on the emerging NIST PQ standards including Classic McEliece. Being part of the NIST process gives the company a commercial advantage in assuring potential customers of rigorous and secure implementations. For example, ***we already sell a popular hybrid PQ VPN****, a VPN using a combination of existing encryption standards plus expected PQ standards*" [E5].

Leading cloud computing provider Amazon Web Services (AWS), Senior Principal Engineer writes "*The NIST post-quantum standardization process is extremely important to us at AWS. […] The NIST process has extremely high visibility in industry and* ***is defining the best practice for postquantum systems****. […]* ***We are implementing hybrid-post-quantum solutions today*** *based on NIST submissions to understand their impact to cloud computing*" [E8].

5. Sources to corroborate the impact

E1. Letter of support: Michel Abdalla, President of the International Association of Cryptologic Research (IACR).
E2. NIST links relevant to this case study.
E3. Letter of support: Colin Whorlow, Head of International Standards, UK National Cyber Security Centre.
E4. RHUL publications referenced in the NIST Postquantum Standardisation Process.
E5. Letter of support: Professor Martin Tomlinson, CSO and Chairman, PQ Solutions Ltd
E6. Letter of support: Matt Ball, Chief Scientist Thales UK.
E7. Letter of support: Oscar Garcia-Morchon, Senior Standardization Officer Intellectual Property & Standards, Philips.
E8. Letter of support: Matthew Campagna, Senior Principal Engineer, Amazon Web Services (AWS).
E9. NSA's Cybersecurity Perspective on Post-Quantum Cryptography Algorithms. (2020) url: https://www.nsa.gov/What-We-Do/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/
E10. Bundesamt für Sicherheit in der Informationstechnik, Migration zu Post-Quanten Kryptografi, Report (2020)
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=2.