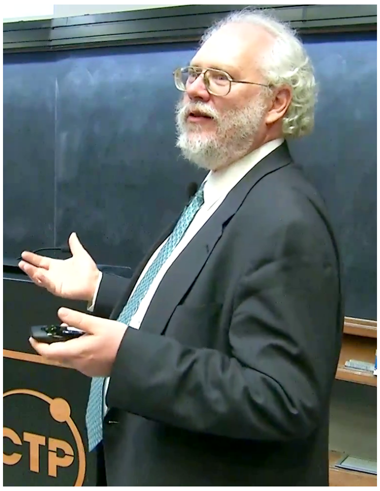
Industry PhD Projects in Post-quantum Cryptography with Monash University, CSIRO’s Data61 and Penten

Introduction

Quantum computing is expected to provide new computational capabilities that significantly exceed those of classical computers in some cases, including the computationally intractable problems that form the basis of modern cryptography. In 1994, Peter Shor proposed quantum algorithms that can factorise integers and solve discrete logarithms in polynomial time. Consequently, well-known and widely deployed public-key cryptosystems such as RSA, ECDH, ECDSA, El Gamal and their numerous variants (whose security rests on the assumption that factorisation and discrete logarithms are intractable) have become insecure against a quantum adversary. Similarly, the security level of private-key cryptosystems (such as AES) may be affected by Grover’s quantum search algorithm.


Peter Shor
(from www.youtube.com/live/J7HeDX_7Heg?si=GymMaJeBRwVcCxT3, International Centre for Theoretical Physics)

Although fully developed large scale quantum computers are yet to be demonstrated, there is significant and continuing progress towards construction of the components of a quantum computer. This means that the security level of cryptographic algorithms developed for classical computers tend to deteriorate with time. In this context, the US National Institute of Standards and Technology (NIST) has been leading a public process of evaluating and standardising *post-quantum cryptographic algorithms* that are resistant to quantum attack. This process has progressed to the standardisation of digital signature algorithms and a key encapsulation mechanism.

The new standards must now be implemented and integrated into the widely used cryptographic systems that maintain the security of our digital world. CSIRO’s Data61, Monash University and Penten are seeking PhD students to join us in addressing these challenges. We are recruiting students for two projects under the auspices of CSIRO’s Industry PhD program, to commence in 2025.

The Industy PhD Program is designed to bring Australian researchers and practitioners together to solve real-world problems. Penten, the industry partner, is a Canberra-based cyber technology business that delivers security products to Australian government and Defence clients. Its flagship Secure Mobility products provide secure access to classified and sensitive information from mobile devices. Penten’s partnership with CSIRO’s Data61 and Monash University on the iPhD program is an important part of protecting these and other systems against quantum attack. Students on the project will be able to spend significant time in Penten’s offices, working side by side with security professionals to develop a deep understanding of the deployment environment and translate research into real world outcomes. Academic supervisors from all three organisations will be engaged in the projects. We propose two topics of research: an investigation into techniques and frameworks to transition existing crypographic systems to post-quantum alternatives, and development of practical, resilient quantum-safe threshold schemes. These are outlined below. Interested candidates may also find the following resources useful as background and to provide a taste of what it might mean to conduct research in cryptography:

- Introduction to Modern Cryptography[1]
- Lecture Notes on Cryptography[2]
- The Quantum Threat to Cybersecurity: Looking Through the Prism of Post-Quantum Cryptography[3]

[1] J. Katz and Y. Lindell. *Introduction to Modern Cryptography, Second Edition*. CRC Press. See https://www.cs.umd.edu/~jkatz/imc.html

[2] S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. Technical report, 2008a. See https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

[3] S. Galbraith, D. Liu, S. Nepal, S. Ruj, J. Pieprzyk, J. Liu, R. Steinfeld, A. Sakzad, M. Esgin, V. Kuchta, et al. The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography, 2021. See https://www.math.auckland.ac.nz/~sgal018/CSIRO-PQC-whitepaper.pdf

Project collaborators include:

Monash	Data61	Penten
A. Prof. Ron Steinfeld	Dr Dongxi Liu	Phil Yialeloglou
Dr Amin Sakzad	Dr Raymond Zhao	
Dr Muhammed Esgin	Dr Nazatul Sultan	

Please see below for eligibility criteria:
`www.csiro.au/en/careers/Scholarships-student-opportunities/Postgraduate-programs-and-Scholarships/Industry-PhD`

and register an expression of interest at:
`https://forms.gle/XJjTZtL8vCDFSs617`

Techniques and Frameworks for Enabling Post-Quantum Cryptography Migration

NIST's ongoing efforts[4] have led to recent standardization of several post-quantum algorithms: ML-DSA and SLH-DSA for digital signatures and ML-KEM for key establishment[5]. As soon as these algorithms are standardised, there will be an urgent need to migrate security protocols and systems to the new standards. Governments in US and EU have already established timelines for such migration because of harvest-now-decrypt-later concerns.

Post-quantum and pre-quantum cryptography have different characteristics in terms of the sizes of keys, ciphertexts, and signatures[6,7]. Current research into migration is focused on the challenges of implementing post-quantum algorithms by addressing the size and protocol misalignment problem. There are also concerns about the security of the new methods, which have not had the benefit of as much scrutiny by the cryptography community as their predecessors.

However, there is very little work that comprehensively considers high-trust, high-speed, and high-agility migration. This project will address these challenges by developing techniques and frameworks that accelerate and de-risk migration to diverse devices and network environments.

The research will investigate several areas:

- We will focus on modular security designs that can take into account the features of a device environment when migrating. These designs should support devices with constrained computation and network resources, should scale to complex hybrids of post-quantum algorithms and be readily adapted to new standards.
- We will analyse and combine the security of such designs with advanced security notions like chosen-ciphertext security, forward secrecy, and post-compromise security in quantum random oracle model or standard model[8]. A universally-composable framework will be leveraged to securely combine multiple protocols. Cryptographic verification tools and stateful protocol fuzzing testing will be conducted to ensure security at both specification and implementation levels.
- We will aim develop prototype implementations of such designs and their combinations to evaluate and demonstrate both the functionality and security features of the migration techniques.

[4] Next steps in preparing for post-quantum cryptography. White paper, National Cyber Security Centre, 11 2023. URL `www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography`

[5] IR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. Technical report, NIST, 2022. `https://csrc.nist.gov/pubs/ir/8413/upd1/final`

[6] G. Tasopoulos, J. Li, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld. Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In *ISPEC*, volume 13620 of *Lecture Notes in Computer Science*, pages 432–451. Springer, 2022

[7] SP 1800-38: Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (Preliminary Draft). Technical report, NIST, 2023. `https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)`

[8] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011

Resilient & Practical Quantum-Safe Cryptographic Threshold Schemes

Security of cryptography for both confidentiality and integrity critically depends on the secrecy of the private cryptographic keys, whose exposure would lead to total breach of security. For high security assurance applications requiring a high resilience to and cost of attacks, a desirable requirement is defence in depth, where the attacker has to compromise multiple points in the system, avoiding single points of failure. This project will investigate two techniques used in the design of high-resilience quantum-safe encryption and authentication algorithms, at both the design and implementation levels.[9].

At the design level, we will focus on the design of practical quantum-safe threshold cryptosystems, in which the secret key is split into multiple shares distributed among multiple computation devices. Attackers need to compromise multiple devices (shares) to gain any information on the shared secret key, and the cryptographic (decryption or signature) computation is also distributed among devices so that the secret key is never explicitly recovered on any single device.

At the implementation level, we will focus on developing practical implementation masking techniques for resiliency against side-channel attacks, in particular, via radiated electromagnetic emissions from the computation device that reveal information on the values computed in the device to an attacker receiving such emissions. With the masking implementation techniques, even the computation inside each device is distributed on multiple internal secret shares, such that a side-channel attack would need to recover information on a large number of values computed inside the device, significantly increasing the cost of the attack. Such side-channel resistance techniques closely relate to the threshold cryptography techniques described above.

Preliminary research progress has been recently made on improved efficiency for such quantum-safe threshold decryption [10] and signature[11] algorithms and their masked implementation[12], but their communication/memory and computation cost overheads remain quite high. This project aims to build on and improve these results to develop a toolkit of practical design and implementation techniques for resilient quantum-safe cryptosystems.

References

IR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. Technical report, NIST, 2022. `https://csrc.nist.gov/pubs/ir/8413/upd1/final`.

Next steps in preparing for post-quantum cryptography. White paper, National Cyber Security Centre, 11 2023. URL `www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography`.

SP 1800-38: Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (Preliminary Draft). Technical report, NIST, 2023. `https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)`.

D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th Interna-*

[9] S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. Technical report, 2008b. See Sec. 10.6 of `https://cseweb.ucsd.edu/~mihir/papers/gb.pdf`

[10] K. Boudgoust and P. Scholl. Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 371–404. Springer, 2023

[11] R. del Pino, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, and M.-J. Saarinen. Threshold Raccoon: Practical threshold signatures from standard lattice assumptions. *Cryptology ePrint Archive*, 2024

[12] M. F. Esgin, T. Espitau, G. Niot, T. Prest, A. Sakzad, and R. Steinfeld. Plover: Masking-friendly hash-and-sign lattice signatures. In *EUROCRYPT (6)*, volume 14656 of *Lecture Notes in Computer Science*, pages 316–345. Springer, 2024. Full version at `https://eprint.iacr.org/2024/401.pdf`

tional Conference on the Theory and Application of Cryptology and Information Security, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

K. Boudgoust and P. Scholl. Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 371–404. Springer, 2023.

R. del Pino, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, and M.-J. Saarinen. Threshold Raccoon: Practical threshold signatures from standard lattice assumptions. *Cryptology ePrint Archive*, 2024.

M. F. Esgin, T. Espitau, G. Niot, T. Prest, A. Sakzad, and R. Steinfeld. Plover: Masking-friendly hash-and-sign lattice signatures. In *EUROCRYPT (6)*, volume 14656 of *Lecture Notes in Computer Science*, pages 316–345. Springer, 2024. Full version at `https://eprint.iacr.org/2024/401.pdf`.

S. Galbraith, D. Liu, S. Nepal, S. Ruj, J. Pieprzyk, J. Liu, R. Steinfeld, A. Sakzad, M. Esgin, V. Kuchta, et al. The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography, 2021. See `https://www.math.auckland.ac.nz/~sgal018/CSIRO-PQC-whitepaper.pdf`.

S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. Technical report, 2008a. See `https://cseweb.ucsd.edu/~mihir/papers/gb.pdf`.

S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. Technical report, 2008b. See Sec. 10.6 of `https://cseweb.ucsd.edu/~mihir/papers/gb.pdf`.

J. Katz and Y. Lindell. *Introduction to Modern Cryptography, Second Edition*. CRC Press. See `https://www.cs.umd.edu/~jkatz/imc.html`.

G. Tasopoulos, J. Li, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld. Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In *ISPEC*, volume 13620 of *Lecture Notes in Computer Science*, pages 432–451. Springer, 2022.