MONASH UNIVERSITY AND OCSC

POST-QUANTUM CRYPTOGRAPHY IN THE INDO-PACIFIC PROGRAM

Proactively building regional quantum computing resilience

MONASH University

OCSC
Oceania Cyber Security Centre

DEPARTMENT OF STATE
UNITED STATES OF AMERICA

PROJECT OVERVIEW

The Post-Quantum Cryptography in the Indo-Pacific Program (PQCIP) is an educational capacity-building initiative that will train cybersecurity and information technology professionals from organizations in the Indo-Pacific to understand and develop the capability to deploy NIST Post-Quantum Cryptography standards and help them protect against emerging quantum computing threats.

Engaging with both industry and government representatives, PQCIP will help stakeholders identify their existing post-quantum computing vulnerabilities and equip them with the necessary skills to secure their digital systems and information into the future. The program will build regional resilience against the threats posed by quantum computing technology by delivering tailored educational material developed and implemented by post-quantum specialists at Monash University and the Oceania Cyber Security Centre (OCSC).

Through the course of the program, participants will learn to identify their knowledge gaps and what quantum computing vulnerabilities already exist in their systems. PQCIP will assist participants to develop post-quantum cryptography transition plans that adhere to NISTPQC standards and will allow organizations to proactively manage emerging quantum computing threats.

Fully funded by the United States Department of State (DOS) and implemented by Monash University and the OCSC, all components of the program will be available to identified participants free of charge.

THE POST-QUANTUM COMPUTING TRANSITION

Post-quantum cryptography involves mathematical techniques for ensuring that information stays private, or is authentic, and resists attacks by both quantum and non-quantum (i.e. classical) computers. The leading application for post-quantum cryptography is securing online communications against attacks using quantum computers.

Data breaches are unfortunately inevitable. Encryption is the key control to preserve the confidentiality of information even when it falls into the wrong hands. However, current cryptography is under threat from emerging quantum computing which will rapidly break encryption and reveal previously protected confidential and highly sensitive information.

Threat actors continue to stockpile stolen or eavesdropped encrypted information, saving it for the near future when quantum computing will reveal its secrets.

- Do you know what systems and information are vulnerable in your organisation?
- What is your plan to protect them from the emerging quantum threat?
- Where will you start?

HOW PQCIP CAN HELP

PQCIP provides a unique opportunity to proactively manage quantum-computing cybersecurity challenges while developing the skills of the region's digital workforce. The team from Monash University and OCSC have more than 20 collective years of experience working in cybersecurity across a broad range of industries and regions. This includes working with post-quantum cryptography and cybersecurity standardisation and consulting in the public and private sectors and providing advice on cyber strategy and policy to governments in the Indo-Pacific to strengthen their national cybersecurity resilience.

With support from the US Department of State, our capacity-building project is free to selected participants from Pacific Island Countries, Indonesia and Malaysia.

PQCIP articipants will learn and develop the skills to:

- Explain to senior management the problem,
- Conduct their own assessments of their organisations systems and information, and
- Develop their own plan for migration of their organisation's systems and information to quantum secure cryptography

It has historically taken decades to establish cryptography infrastructure, therefore we must prepare now to meet the challenges of the quantum computing era. We value equity, diversity and inclusion, and particularly encourage women participants to join the programme.

PROGRAM STRUCTURE

PQCIP is a self-paced training program that is available on the Monash Education Academy platform to eligible participants from April 2023 until June 2025. The training will be primarily asynchronous, with online presentation videos and reading materials available from the training website for participants to access at any time and their own pace.

The estimated time commitment for this program is 32 hours, plus an additional 8 optional hours. A summary of the training modules, their estimated participant time commitments and planned start date is provided in Table 1.

TABLE 1

Module	Time	Available Date
Knowledge Gap Assessment Survey	0.5	From April 2023
Quantum Vulnerability Assessment	11.5 hrs	From May 2023
NIST PQ Cryptography Standards	8 hrs	From February 2024
Transitioning Systems to PQ Cryptography	7.5 hrs	From September 2024
Nation Specific Module	4.5 hrs	From September 2024

PROGRAM STRUCTURE

PROGRAM TIMELINE

The dates stated in Table 1 are estimated dates when students can start the module but may be subject to change. Participants can start taking the Module at any time after this starting date, subject to the following constraints:

- A module should be completed within 6 months from when a participant commences the module.
- The latest date for commencing a module is 31 Dec 2024.
- The latest date for completing a module is 30 June 2025.
- Participants should plan their timeline for completing the modules, taking into account the expected completion time of 2-3 months per module, based on a time commitment of ~1-1.5hr/week, and the expected start dates of offering for the modules indicated in Table 1.

There are a total of 8 optional hours including workshops, consultations, and additional topics as listed in Table 2.

PROGRAM DELIVERY AND REQUIREMENTS

The four-part program is designed for people with a background in information technology services; however, it does not require any prior knowledge of post-quantum cryptography. Enrolled participants will receive login credentials to access the training website. Participants will need their own devices with Internet access and web browser to access the training website.

All software required for exercises and assessments will be provided at no charge either via the training website or via linked freely available publicly accessible Internet resources. Only web browser access will be used, participants will not be required to install any special software programs on their own devices.

PROGRAM CONTENT

The training will be focused on the practical aspects of quantum vulnerability assessment and PQC transitioning. Background theoretical concepts will be presented to support the understanding of the practical aspects and as optional advanced training topics. The program will include regular live tutorial/consultation sessions via Zoom video conference, in which a teaching associate will be available to answer participant questions one-on-one. Attendance at the consultation sessions is also optional and it is estimated that participants will only attend one consultation session hour per training module, although more will be provided if necessary.

The self-conducted organisation transition plan in module (iii): Transitioning common systems to PQC, is an opportunity for students to apply knowledge gained and develop their own practical transition plan in their own context. A summary of the topics covered by the Modules is in Table 2.

TABLE 2

Module	Topic
Module (i): Quantum Vulnerability Assessment	Cryptography Foundation Background Concepts
	Quantum Vulnerable Problems/Cryptosystems
	Identifying Quantum Vulnerable Applications
	Live online consultation/tutorial session by region (optional)
	Self-Conducted Organization App Inventory & Risk Assessment
Module (ii): NIST PQC standards	High-Level Introduction to PQC Approaches and Hard Problems

PROGRAM CONTENT

Module	Topic
Module (ii): NIST PQC standards	PQ Encryption (KEM): Kyber Algorithm
	PQ Encryption: Kyber – Advanced Aspects (optional)
	PQ Default Signature: Dilithium Algorithm
	PQ Specialised Signatures: Falcon (Compactness), SPHINCS+ (Lower Risk) Algorithm
	Live online consultation/tutorial session by region (optional)
	PQ Signature: Advanced Aspects (optional)
	Brief Overview of Alternative (NIST PQC Round 4) Code Based Schemes
	Brief Overview of the "Additional Digital Signatures PQC Process" in Progress by NIST
Module (iii): Transitioning Common systems to PQC	Introduction to Transitioning Common
	Transitioning TLS / web apps

PROGRAM CONTENT

Module	Topic
Module (iii): Transitioning Common systems to PQC	Transitioning other systems
	Self-conducted organisation transition plan
	(optional) Live online consultation/tutorial session by region
	Conclusion
Nation-Specific Supplementary Module	Introduction to Supplementary Module
	Nation-specific topics covered online
	Nation-specific physical workshop
	Live online consultation/tutorial session by country
	Conclusion

PROGRAM OUTCOMES

A deep understanding of postquantum cryptography, associated threats and solutions.

A list identifying participant-specific quantum-vulnerable systems and information.

An expertly evaluated transition plan that applies PCQ standards to protect vulnerable systems and information.

A library of open-access resources for additional training and troubleshooting reference.

A cohort of other skilled IT/cybersecurity professionals in the region for future collaboration.

COURSE QUALIFICATIONS

Upon satisfactory completion of the training module assessments, participants will be issued with a training module completion certificate and digital badge that can be accredited to each participant's CV and shared on LinkedIn.

APPLY NOW

Applications are open to people managing or working in IT or cyber in eligible organisations in either Malaysia, Indonesia, the Philippines or a Pacific Island Nation. We value equity, diversity and inclusion, and particularly encourage women participants to join the programme.

Fully funded by the U.S. Department of State and implemented by Monash University and the OCSC, all components of the program will be available to eligible participants **free** of charge.

ELIGIBILITY CRITERIA

- Participants must be part of a government or organisation from Malaysia, Indonesia, the Philippines or a Pacific Island Nation.
- Participants must be available to complete each stage of the program.
- Participants cannot be from military, intelligence, or law-enforcement organisations. Applicants can work with Monash University and US DOS to help determine their eligibility.
- People managing or working in IT or cyber in eligible organisation.

For any questions regarding the enrolment, content, or technical or other issues, email the team at: **pqcip@monash.edu**

PROJECT TEAM

A/Prof. Ron Steinfeld.
Project Director, Monash University.

Prof. Carsten Rudolph.
Deputy Dean of the Faculty of IT, Monash University.

Dr Amin Sakzad.
PQC consultant, Monash University.

Dr Muhammed Esgin.
PQC consultant, Monash University.

Prof. Raphael Phan.
Malaysia Lead, Monash University,

Nikai Jagganath.
Research Associate, Monash University.

Dr James Boorman.
Head of Research and Capacity Building, OCSC.

Joe Fulwood.
Researcher officer and marketing and communications lead, OCSC.

LIST OF ABBREVIATIONS

Abbreviation	Description
CV	Curriculum Vitae
KEM	Key Encapsulation Mechanism
NIST	National Institute of Standards and Technology
PQ	Post Quantum
PQC	Post Quantum Cryptography
PQCIP	Post Quantum Cryptography in the Indo-Pacific
SPHINCS+	A stateless hash-based signature scheme that has been selected for standardization as part of the NIST Post-Quantum cryptography (PQC) standardization process.
TLS	Transport Layer Security
VPN	Virtual Private Network