AUSQRC 2025

MATHEMATICAL PROBLEMS

FOUNDATIONS

ALGORITHMS & PROTOCOLS

AUTHENTICATE

BLOCKCHAIN

CRYPTOGRAPHY

PRIVACY

CLOUD SECURITY

END to END ENCRYPTION

APPLICATIONS

DATABASE SECURITY

Collaboration!

ACADEMIA

INDUSTRY

GOVERNMENT

NIKAI JAGGANATH

DR MUHAMMED ESGIN

PROF RON STEINFELD

IMPLEMENTATION & DEPLOYMENT

SECURE!

INTEGRATION

STANDARDISATION

MONASH University

MONASH INFORMATION TECHNOLOGY

Graphic Recording by **www.debbiewood.com.au** Captured on Wurundjeri Land

Post Quantum Cryptography: Successes & Remaining Challenges

Prof Jonathan Katz

AUSQRC 2025

Welcome

WHY:

SHOR'S ALGORITHM... ~~RSA ECC~~

CURRENT CRYPTOSYSTEMS CAN BE INSECURE

GROVER'S ALGORITHM... $\sqrt{n}$

WHAT:

ASYMMETRIC ENCRYPTION

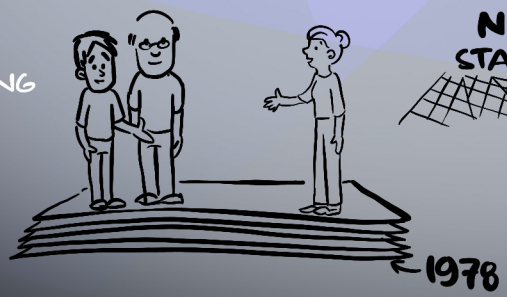
↳ HARVEST NOW, DECRYPT LATER

DIGITAL SIGNATURES

↳ THESE ARE EVERYWHERE.

How:

WE'RE BUILDING ON CRYPTO RESEARCH



NIST STANDARDS

HOW SOON?

YOU'D NEED 1 MILLION QUBITS...

IT'S NOT TOMORROW. DON'T PANIC!

BUT WE NEED TO BE READY

PQC

- FOUNDATIONS
- APPLICATIONS
- DEPLOYMENT

security

- COST TO IMPLEMENT
- HYBRID
- SCALE

COMPLEXITY VS. AGILITY

MONASH University

MONASH INFORMATION TECHNOLOGY

Graphic Recording by **www.debbiewood.com.au** Captured on Wurundjeri Land

Post Quantum Cryptography in Europe

Dr Thomas Prest

AUSQRC 2025

STEP 1 NIST PQC STANDARDS 2024

STEP 2 DEPLOY!

2035 COMPLETE MIGRATION to PQC

DEPLOYMENT is TOUGH! → SIDE CHANNEL ATTACKS

→ IMPLEMENTATION BUGS

KEMTLS/AuthTLS

REPLACE HANDSHAKE SIGNATURE with KEM

PROBLEM: EUROPE is FRAGMENTED

ANSSI

BSI

NCSC

CCB

TLS

VPNS

DNSSEC

PROTOCOLS

SECURITY

FUNCTIONALITY

TRANSPARENCY

AUDITABILITY & VISIBILITY

CT

MTC

BATCH

root

a

b

c

#

PQC

IT'S FAST, BUT NEEDS MEMORY

IT'S BIG

30x THE SIZE of CLASSICAL

MONASH University

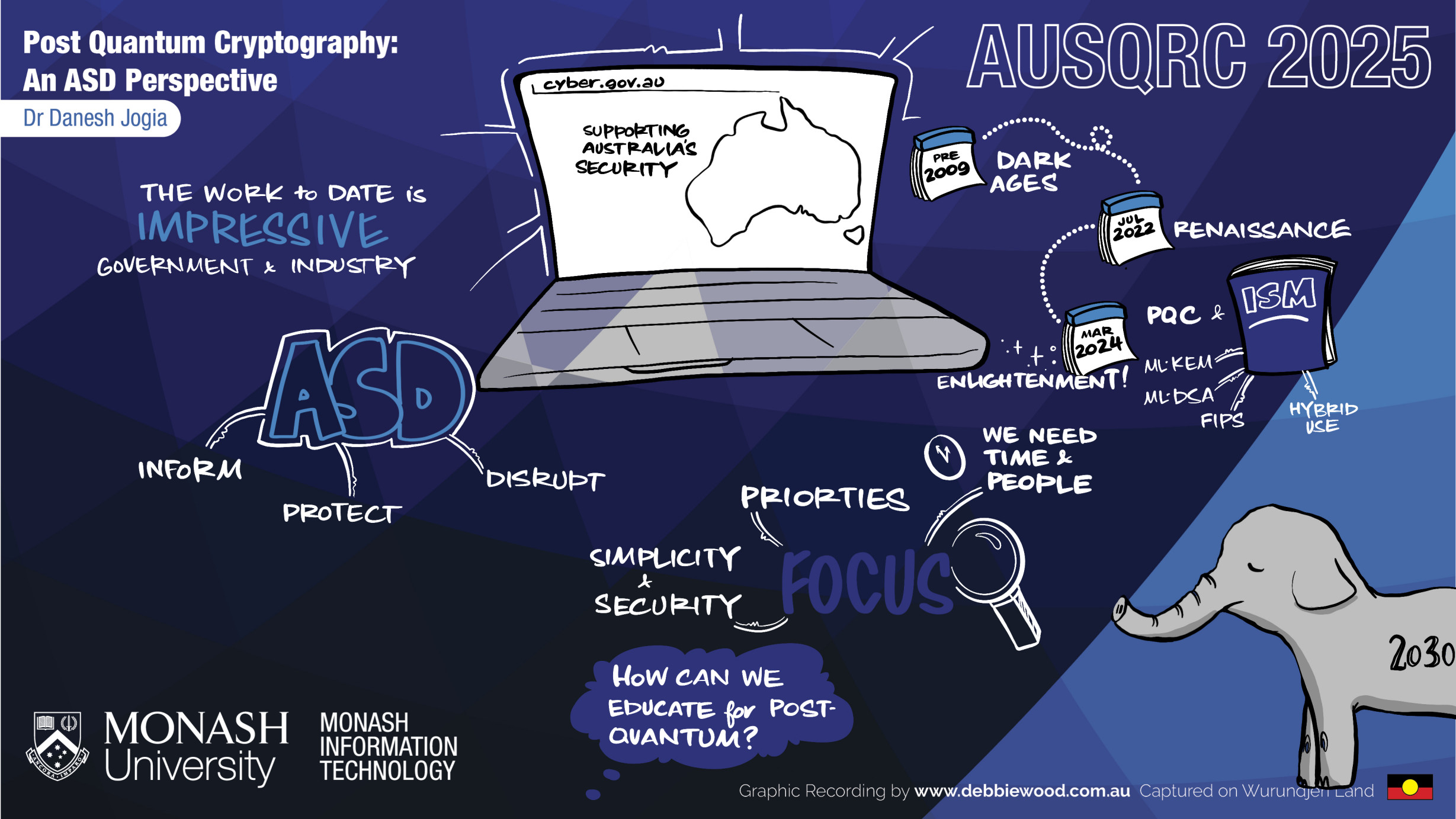
MONASH INFORMATION TECHNOLOGY

Graphic Recording by **www.debbiewood.com.au** Captured on Wurundjeri Land

Post Quantum Cryptography: An ASD Perspective

Dr Danesh Jogia

AUSQRC 2025



MONASH University
MONASH INFORMATION TECHNOLOGY

Graphic Recording by **www.debbiewood.com.au** Captured on Wurundjeri Land

AUSQRC 2025

Panel with Julian Fay

Prof Jonathan Katz
Dr Thomas Prest
Dr Danesh Jogia
Joshua Lickiss

1 STANDARDS
2 AMPLIFY

AUDITS? NO.
TOOLS YES.
ADVICE
GUIDELINES

WHERE WILL THE WORKFORCE COME FROM?
2030
(NOT AGES AWAY!)
ONLY 10 PEOPLE GLOBALLY HAVE CAPABILITY...

HOW MUCH PROTECTION DO YOU NEED?

GOOGLE HAS A PROCESS & a PQC DEDICATED TEAM

SMART-CARDS
VISA
PAYMENT
RISK
INVESTMENT

LATTICE BASED IS WHAT WE'RE INVESTING 25+ YEARS of STUDY

MIGRATION CAUSED by MARKET FORCES

IT'S DIFFICULT to explain...

JUST BELIEVE US, IT'S A THREAT.

PUBLIC trust

BAD ACTORS
NATION-STATES
SPYWARE
CYBER
PHISHING
RANSOMWARE
ATTACKS
HACKERS
WILL THEY HAVE THE MONEY?

THREATS TO TECH FROM THROUGH

AUTHENTICATION is CRITICAL

YOUR SECURITY is ONLY AS GOOD AS THE LOWEST PART OF YOUR FENCE

UNCERTAINTY is NO EXCUSE for INACTION!

Q. WILL AI-ASSISTED CRYPTANALYSIS BREAK PQC?

A. UNLIKELY.

MONASH University
MONASH INFORMATION TECHNOLOGY

Graphic Recording by **www.debbiewood.com.au** Captured on Wurundjeri Land

Overcoming challenges with PQC deployment on a global scale

Sandra Roggeveen
& Rob Gillan

AUSQRC 2025

FAST FOOD NETWORKS

IOT

CRITICAL INFRUSTRUCTURE

AUTOMATION

DATA SIZE IS EXPLODING

HOW DO WE TAKE INDUSTRY ON THE JOURNEY?

FUTURE PROOF

QUANTUM

TEST & RELEASE

in AUSTRALIA

WE DONT KNOW WHAT WE DONT KNOW??

WHAT'LL IT COST?

HOW LONG WILL IT TAKE?

WE NEED TO WORK TOGETHER!

CORE LIBRARIES (openSSL, wolfSSL) are NO LONGER SIMPLE DROP-INS for PQC.

CODE

P.S. HERE'S the SECRET CODE!

QKD

QUANTUM KEY DISTRIBUTION SHOULD BE EXPLORED

MONASH University
MONASH INFORMATION TECHNOLOGY

Graphic Recording by **www.debbiewood.com.au** Captured on Wurundjeri Land

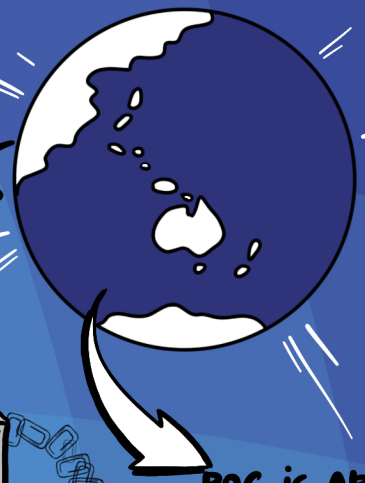
Securing everyone's future: Post Quantum Cryptography in telecommunications

Dan Robinson
& Christian Danci

AUSQRC 2025

CYBER

CONTROL SOPHISTICATED NATION-STATES



THE NEXT 20 YEARS WILL BE MORE DYNAMIC THAN the LAST 20.

EXTERNAL

INTERNAL

SUPPLY

ENCRYPTION NEEDS LOCKING DOWN

FOLLOWING ASD STANDARDS!

PREVENT STORE!

POC is ABOUT AN ECOSYSTEM

QKD

POC

PLS

GG

PART of a HOLISTIC PLAN!

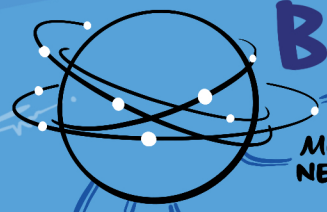
DISCOVER

ASSESS

PLAN

REMEDIATE

BUSINESS



DIGITAL

MOBILE NETWORK

IoT

OPTICAL FIBRE

SERVICES

trust

NEW CUSTOMER NEEDS

CHANGING BIZ MODELS

customer engagement

TECHNOLOGY and CONNECTIVITY for AUSTRALIANS

sCALE

MILLIONS of CUSTOMERS & MOBILE PHONES

MONASH University
MONASH INFORMATION TECHNOLOGY

Graphic Recording by www.debbiewood.com.au Captured on Wurundjeri Land