

MathQuEST Day

Conference program

Monday 30 November 2026

E-Zone (Industry Hub), University of Western Australia

9:15 – 9:25

Arrival

9:25 – 9:30

Welcome

9:30 – 9:45

Prof Nalini Joshi, Centre Director

Opening remarks

9:45 – 10:30

Prof Jingbo Wang

Quantum Computing: Promises, Opportunities and Key Challenges

10:30 – 11:00

Prof Craig Costello

Bringing Q-Day forward: recent progress in quantum algorithms for the elliptic curve discrete logarithm problem

11:00 – 11:30

Morning tea

11:30 – 12:00

Prof Kate Smith-Miles

Instance Space Analysis: stress testing algorithms and strategically designing hard instances

12:00 – 12:30

Prof Murray Elder

Discussion about DEI with regards to hiring/student recruitment

12:30 – 1:30

Lunch

1:30 – 2:00

Prof Michael Small

Dynamical Systems to Machine Learning and Quantum Computing

2:00 – 2:30

Prof Youming Qiao

From a mathematical problem to a cryptographic implementation: a case study based on group isomorphism

2:30 – 3:00

Dr Lindon Roberts

Tutorial: An introduction to implementing quantum algorithms

3:00 – 3:30

Afternoon tea

3:30 – 5:00

MathQuEST meeting

Centre Members only

Followed by members' dinner

Talk abstracts

MORNING SESSION

9:45 – 10:30

Prof Jingbo Wang

Quantum Computing: Promises, Opportunities and Key Challenges

Quantum computing is advancing rapidly, with growing potential to address important computational challenges across science, technology, and industry. The Research Centre for Quantum Information, Simulation and Algorithms (QUISA) brings together researchers working across a broad range of areas, from fundamental theory to emerging applications. I will provide an overview of QUISA's current research in quantum algorithms for differential equations, quantum linear algebra, tensor networks, and complex-system modelling. I will also briefly highlight applications in optimisation, image and signal processing, bioinformatics, finance, and medicine, alongside QUISA's activities in quantum foundations and education. Together, these projects illustrate why quantum computing matters, why progress in the field is timely, and how foundational research may contribute to practical applications.

10:30 – 11:00

Prof Craig Costello

Bringing Q-Day forward: recent progress in quantum algorithms for the elliptic curve discrete logarithm problem

There has been a flurry of activity in recent months as quantum resource estimates for the elliptic curve discrete logarithm problem (ECDLP) continue to be lowered. I'll give a high-level overview of the ECDLP and its resolution via Shor's quantum algorithm, before discussing some of the recent works in the area.

11:30 – 12:00

Prof Kate Smith-Miles

Instance Space Analysis: stress testing algorithms and strategically designing hard instances

In this talk I will provide a brief overview of Instance Space Analysis - a methodology that provides visual representations of the entire space of possible instances of a problem. This representation enables two main insights: i) the conditions under which any algorithm has strengths and weaknesses, and ii) the degree to which empirical testing on a suite of instances is unbiased, comprehensive and sufficiently diverse to draw valid and reliable conclusions about algorithm performance and robustness. The methodology extends beyond "stress-testing" algorithm performance to generating synthetic test instances that occupy any target region of the instance space, enabling strategic design of exceptionally hard instances of a given problem. This approach may be useful for designing harder instances of hard problems underpinning post-quantum cryptography.

12:00 – 12:30

Prof Murray Elder

Discussion about DEI with regards to hiring/student recruitment

Murray Elder will facilitate an open discussion about Diversity, Equity and Inclusion (DEI) issues, with the following suggested topics:

1. Recruitment policy/procedures: have we missed anything? Will it work (in achieving its aims, with local institutional rules, etc.)?
2. "Start a tradition" of setting aside time at each major MathQuEST event for a discussion/focus on DEI. What would be the best ways to do it (to give different groups a voice)? An open panel or calling out from the floor may not be the best way to elicit diverse inputs.

If you would like anything included, feel free to email murray.elder@uts.edu.au prior to the timeslot.

Talk abstracts

AFTERNOON SESSION

1:30 – 2:00

Prof Michael Small

Dynamical Systems to Machine Learning and Quantum Computing

The central question of my talk is what can the mathematics of dynamical systems theory and complex systems theory tell us about machine learning and future quantum computing? The primary tool I will use to study this exchange is the reservoir computer (RC). RCs provide a useful paradigm for studying both dynamical systems and recurrent neural networks. They are random recurrent dynamical networks driven by an input time series, in which only the output layer is trained — typically via linear regression and regularization. This makes them lightweight and general-purpose, yet remarkably powerful for modelling nonlinear dynamical systems. I will explain why this is the case, showing that the internal state of the RC captures the same features as a time-delay embedding — that is, it faithfully (and generically) reconstructs the underlying high-dimensional dynamics from a scalar observable time series. Using what we call Reservoir Time Series Analysis I will show that this internal state encodes enough information to rival state-of-the-art tools in nonlinear time-series analysis, including recurrence quantification methods. Next, I will introduce new work constructing a reservoir substrate from the ordinal encoding of a time series, demonstrating that even this simple representation suffices for reservoir-based information processing — opening the door to new applications of reservoir computing. Finally, I will briefly outline some future directions in the application of this toolkit for quantum computation.

2:00 – 2:30

Prof Youming Qiao

From a mathematical problem to a cryptographic implementation: a case study based on group isomorphism

I started my PhD working on group isomorphism. After about 15 years, this theory idea was turned to a submission of a digital signature scheme to NIST's call for post-quantum signature schemes. I will share the mathematical ideas, cryptographic techniques, and lessons from practical implementations, from this experience.

2:30 – 3:00

Dr Lindon Roberts

Tutorial: An introduction to implementing quantum algorithms

The goal of this talk is to give a gentle introduction to implementing and running quantum algorithms, using Python's Qiskit framework. I plan to cover topics like: defining quantum registers and circuits, making measurements, and running quantum algorithms on classical and quantum hardware, drawing on simple examples such as Grover search.