

FASTS “HEADS UP” BRIEFING

Quantum Cryptography: Security and Information Technology in the Quantum Age

Introduction

The security of financial, business, Government and defence communications and data storage is critical. Conventional methods of attack are already with us, and new methods based on scientific advances in Quantum Information pose a potential threat.

The field of Quantum Information is a hot topic in modern physics and the fundamental concepts of quantum mechanics are now being applied to the storage, transmission and processing of information. In particular, recent advances in *Quantum Cryptography* can make the transmission of information completely secure.

However, other future applications of quantum mechanics such as the Quantum Computer are potentially disruptive technologies, that may make the existing storage or transmission of information by conventional cryptography vulnerable to attack.

Why is this of immediate interest to Government?

- The roll out of Quantum cryptography may pose a challenge to regulatory, privacy and standards frameworks; and
- Governments have a critical interest in ensuring the integrity and security of their own information networks and data storage.

For whom might this be of interest?

This technology is of interest to Government in both its capacity as a regulator but also an end-user. It also concerns financial institutions, communications providers, database repositories, and national security organizations.

Which Ministerial portfolios does it involve?

The Department of Defence is already aware of advances in Quantum Information and has scientists working in these areas in partnership with publicly funded researchers. Other directly relevant Ministries include:

- The Treasury
- Department of Innovation, Industry, Science and Research
- Department of Broadband, Communication and the Digital Economy
- Department of Foreign Affairs and Trade
- Prime Minister and Cabinet

and all departments and agencies concerned with security and privacy of data including the Department of Health and Aging, Australian Taxation Office, Australian Federal Police and other security agencies. There is also relevance here for the Australian Law Reform Commission and the Privacy Commissioner.

FASTS is the peak representative body for 60,000 Australian scientists and technologists

Purpose of the briefing

This “*Heads Up*” Briefing is the first in a new series of briefings for Government Departments and agencies coordinated by the Federation of Australian Scientific and Technological societies (FASTS), which represents more than 60,000 Australian scientists.

The aim of “*Heads Up*” Briefings is to outline new developments in science that may prompt the need for policy and regulatory responses in the short to medium term.

This briefing will provide participants with an overview of *Quantum Cryptography* from Australia’s top scientists in the field, and highlight possible policy implications of the science.

Date and Time:

Thursday 7th May

11.30 – 12.30 Briefing

12.30 – 13.30 Lunch

Venue:

Old Parliament House, Members Dining Room 1

Briefing format

FASTS will host a one hour briefing on *Quantum Cryptography* with short presentations from the following experts:

- Professor Ken Baldwin (President, FASTS) - *Welcome and Introductions*
- Professor Tim Ralph (University of Queensland) - *Quantum cryptography – what is it and what can it do?*
- Professor Ping Koy Lam (ANU) - *Physical Realisations of Quantum Cryptography*
- Dr Vikram Sharma (QuintessenceLabs Pty. Ltd.) - *Commercial Applications of Laser-Based Quantum Cryptography*
- Professor Lloyd Hollenberg (Quantum Communications Victoria) - *Single-Photon Quantum Cryptography*

The presentations will be followed by a Q&A panel discussion on the broader future issues relating to *Quantum Cryptography*.

FASTS is the peak representative body for 60,000 Australian scientists and technologists

Presenter biographies:

Professor Ken Baldwin, *Research School of Physics and Engineering, Australian National University*

Professor Baldwin is President of FASTS, a researcher in quantum physics, and the winner of the 2004 Eureka Prize for Promoting Understanding of Science for his role in initiating *Science meets Parliament*. He is Deputy Director of the Australian Research Council Centre of Excellence for Quantum-Atom Optics.

Professor Tim Ralph, *Department of Physics, University of Queensland*

Professor Ralph has a wide range of research expertise in quantum information theory and co-invented the quantum key distribution scheme being developed by QuintessenceLabs Pty. Ltd. He heads the Queensland Node of the Australian Research Council Centre of Excellence for Quantum Computer Technology.

Professor Ping Koy Lam, *Research School of Physics and Engineering, Australian National University*

Professor Lam is the Quantum Optics group leader at ANU and a member of the Australian Research Council Centre of Excellence for Quantum-Atom Optics. He is a former winner of the Eureka Prize for Scientific Research for his work on faster methods of quantum encryption, and is a founder of QuintessenceLabsPty. Ltd. based in Canberra.

Dr Vikram Sharma, *QuintessenceLabs Pty. Ltd., Canberra*

Vikram Sharma is founding director and CEO of QuintessenceLabs Pty. Ltd. He is a Sloan Fellow from Stanford University, California, and also holds an MSc in computer science and a PhD in quantum physics from the ANU. Prior to QuintessenceLabs, Vikram founded three successful start-up ventures in information technology.

Professor Lloyd Hollenberg, *School of Physics, University of Melbourne*

Professor Hollenberg is a member of the Australian Research Council Centre of Excellence for Quantum Computer Technology, and is Manager of the Quantum Device Modelling and Algorithms Program. He is also Technical Director (Theory) of Quantum Communications Victoria (QCV), overseeing the single photon source prototype development for quantum communications applications.

FASTS is the peak representative body for 60,000 Australian scientists and technologists