SAFEcrypto: Secure Architectures of Future Emerging cryptography

PSC Europe December 2015 - Elizabeth O'Sullivan,
Centre For Secure Information Technology, Queen's University Belfast

This project has received funding from the European Union H2020 research and innovation programme under grant agreement No 644729

SAFEcrypto Project

- **4-year project funded - commenced in January 2015**
- new generation of practical, robust and physically secure post quantum cryptographic solutions

- **Academic partners**
  - Institut National De Recherche en Informatique et en Automatique (France)
  - Queens University Belfast (UK)
  - Ruhr-Universitaet Bochum (Germany)
  - Universita Della Svizzera Italiana (Switzerland)

- **Industry partners**
  - EMC/RSA
  - HWCommunications Ltd
  - Thales

SAFEcrypto

Quantum Technology – NSA's Efforts

Excerpts from the "black budget," Volume 2, "Combined Cryptologic Program":

(U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

(U) Project Description

(S//SI//REL TO USA, FVEY) The Penetrating Hard Targets Project provides proof-of-concept technological solutions to {...} enable:

{...}

- (S//SI//REL TO USA, FVEY) Breaking strong encryption.

{...}

- (S//SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.

NSA funding a $79.7 million research program to build a 'cryptologically useful quantum computer'

S. Rich, B.Gellman, The Washington Post (Jan 2014)

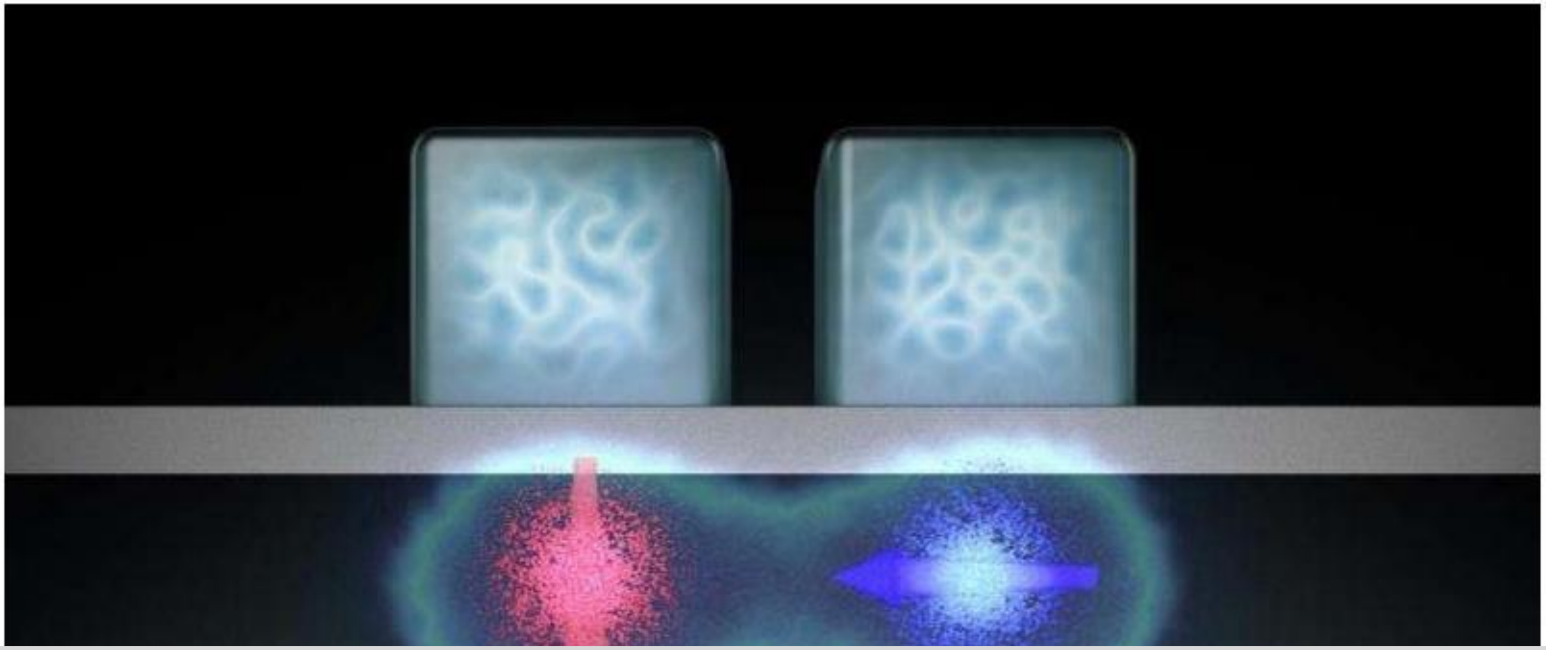
Quantum Technology – Recent Breakthroughs

PHYS.ORG Nanotechnology Physics Earth Astronomy & Space Technology Chemistry

Home » Physics » Quantum Physics » October 5, 2015

Crucial hurdle overcome in quantum computing

October 5, 2015



Letters to Nature – October 2015 - Researchers in University of New South Wales Australia have demonstrated two qubit logic gate in silicon

Quantum Technology – Commercial Progress

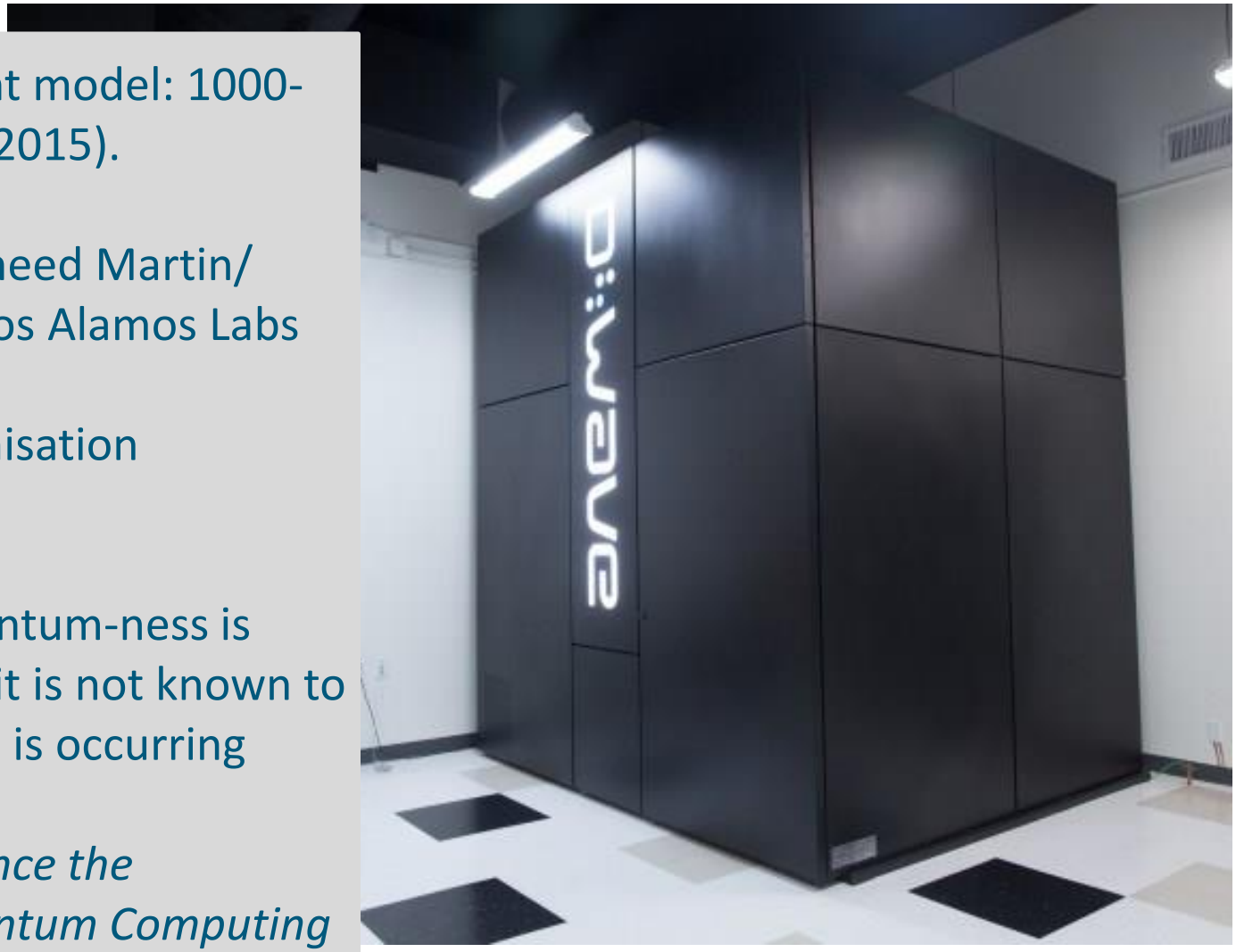
D-Wave's current model: 1000-qubit machine (2015).

Bought by Lockheed Martin/ Google/NASA/Los Alamos Labs

Quantum Optimisation Technology

Evidence of quantum-ness is emerging – but it is not known to what extent this is occurring

helping to advance the research in Quantum Computing



What happens if/when quantum computers become a reality ?

Commonly used Public-key encryption algorithms
(based on integer factorisation and discrete log problem) such as:

RSA, DSA, DHKE, EC, ECDSA

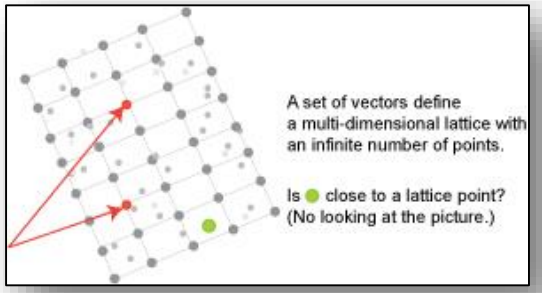
will no longer be secure…

Symmetric algorithms appear to be secure against quantum computers (and Grover's algorithm) by simply increasing the associated key sizes.

Quantum-Safe Cryptography

Post-Quantum or Quantum-Safe Cryptography: conventional *non-quantum* cryptographic algorithms that will remain secure even after practical quantum computing is a reality.

- Code-based
- Hash-based
- Multivariate-quadratic
- ***Lattice-based***



Advantages of Lattice-based Cryptography

- Underlying operations can be implemented efficiently
- Promising as allows for other constructions/applications beyond encryption/signatures , eg. IBE, ABE, homomorphic encryption, etc.

SAFE crypto

Quantum-Safe Cryptography

Transition to Quantum-Safe cryptography in the not so distant future…

August 2015

Overall Goal

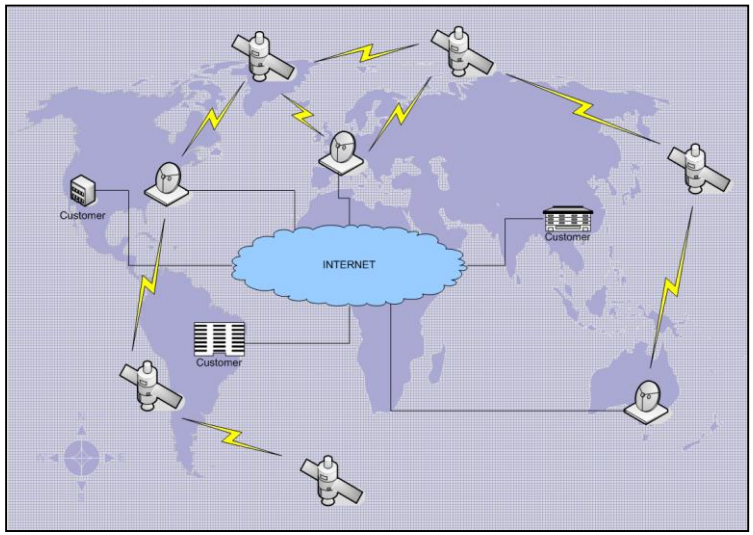
SAFEcrypto will provide a new generation of **practical, robust and physically secure post-quantum cryptographic solutions** that ensure **long-term security** for future ICT systems, services and applications.

SAFEcrypto will deliver *proof-of-concept demonstrators* of the lattice-based cryptographic primitives applied to 3 case-studies:

- Satellite Key Management
- Commercial Off-The-Shelf (COTS) in Public Safety Communication
- Privacy-preserving municipal data analytics

1. Secure communications of networked space-based entities

Current symmetric algorithm approaches not suitable for next-generation space-based entities



Future Deployments:

- Flexibility for
- Symmetric key compromise
- Protection of key loading
- Perfect forward secrecy

SAFEcrypto - Feasibility of a lattice-based key management solutions for applications with bandwidth, latency and unreliable channel issues

2. Trusted components for critical communication applications

Use of COTS devices and legacy equipment underpin the operation of critical services - need to secure the communication between these devices.

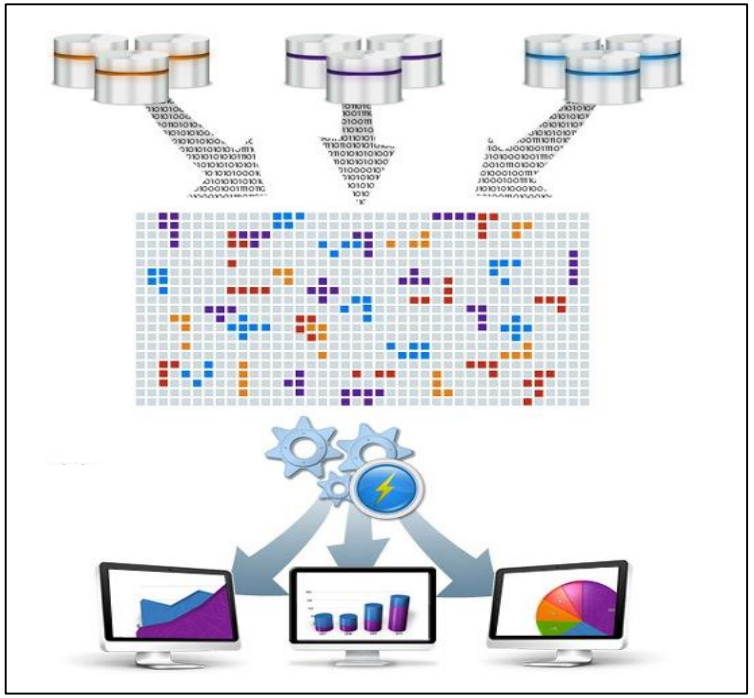
www.qinetiq.com

SAFEcrypto will provide:

- New add-on quantum-safe crypto capability to legacy equip & COTS devices
- High-speed crypto for bandwidth hungry applications
- New key-exchange techniques within disparate new & legacy systems/networks

3. Privacy-preserving municipal data analytics

Significant benefits possible through collaborative analytics of large government-owned data sets; however, this needs appropriate management of the accessibility and privacy of the information.



gigaom2.files.wordpress.com

SAFEcrypto will provide:

- A lattice-based ABE scheme and key management approaches to allow for effective and privacy-preserving collaborative analytics

SAFEcrypto Objectives

Project Objectives for Lattice-based Cryptography

- Conduct V**ulnerability and risk assessment** of the identified case studies.
- Derive P**ractical lattice-based cryptographic constructions** (digital signature, authentication, ABE and IBE.
- Design and implement **hardware architectures for each of the proposed primitives** (constrained devices as well as high performance).
- Design and implement **open-source software routines** for the primitives
- Investigate **physical attack-resistant design methodologies** for lattice-based hardware and software implementations.
- Develop **effective models for the management, storage and distribution of keys**
- Build hardware/software co-design **proof-of-concept demonstrators** to illustrate the feasibility of the lattice-based cryptographic hardware and software architectures in providing long-term security for the three case studies

Quantitative Objectives

- In comparison to existing RSA and ECC-based public-key cryptosystems:
  - 10-fold speed-up in throughput
    - Satellite use-case
    - Privacy-preserving data analytics use-case
  - 5-fold reduction in energy consumption
    - Critical communication use-case

SAFEcrypto Objectives

Dissemination of project results and activities

Academic conferences

Industry Events

Standardization initiatives

Contribution to open source

SAFE crypto

SAFEcrypto: Secure Architectures of Future Emerging cryptography

www.safecrypto.eu

This project has received funding from the European Union H2020 research and innovation programme under grant agreement No 644729