SAFEcrypto: Secure Architectures of Future Emerging cryptography

Gavin McWilliams
Queen’s University Belfast
Quantum Technology – recent breakthroughs

- **The World’s First Quantum Computer ??**
- D-Wave’s current model billed as a 512-qubit machine (2012).
- Bought by Lockheed Martin & Google/NASA
- Difficult to verify if performing quantum operations or not!
- Has shown significant speed-ups but only for certain calculations
- Has helped to advance the research in Quantum Computing

Organisation sponsors:
NSA funding a $79.7 million research program to build a ‘cryptologically useful quantum computer’

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 be vulnerable to Shor’s algorithm and 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
- Most promising as allows for other constructions beyond encryption/signatures, e.g. IBE, ABE, homomorphic encryption.
Horizon 2020 SAFEcrypto

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:

- Secure communications of networked space-based entities
- Trusted components for critical communication applications
- Privacy-preserving municipal data analytics

Organisation sponsors:
Due to the longevity of satellites and associated infrastructure, any public key solution needs to be secure for a long period of time. It is an ideal case study for the use of quantum safe cryptographic solutions.
In Future, use of COTS devices and legacy equipment will underpin the operation of public safety communications.

Long operational lifetimes are common with a European first responder network uplift planned for 2025-2028. Requires low-powered implementations of lattice based cryptography.
Privacy-preserving municipal data analytics

Municipal Data

Collect Data
Apps
Systems
Network

Store

Analytics

Academic
- Report
- Investigate & Analyze
- Visualize

Industry
- Report
- Investigate & Analyze
- Visualize

Municipal
- Report
- Investigate & Analyze
- Visualize

Organisation sponsors:
Quantum-Safe Cryptography

Timeliness of SAFECrypto project ...

Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

August 2015
SAFECrypto Summary

• 4-year project - commenced in January 2015
• Academic partners
  Queen’s University Belfast (UK)
  Institut National De Recherche en Informatique et en Automatique (France)
  Universita Della Svizzera Italiana (Switzerland)
  Ruhr-Universitaet Bochum (Germany)
• Industry partners
  EMC/RSA
  HWCommunications Ltd
  Thales UK

Organisation sponsors:
Questions & Answers

Gavin McWilliams

www.safecrypto.eu