



SAFEcrypto: Secure Architectures of Future Emerging cryptography

Gavin McWilliams
Queen's University Belfast

Organisation sponsors:



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:





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, January 2014

Organisation sponsors:





Rationale

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.

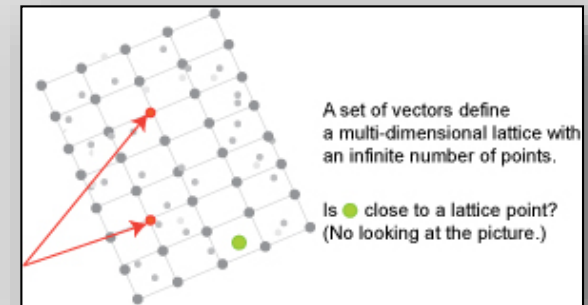
Organisation sponsors:



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.

Organisation sponsors:



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:

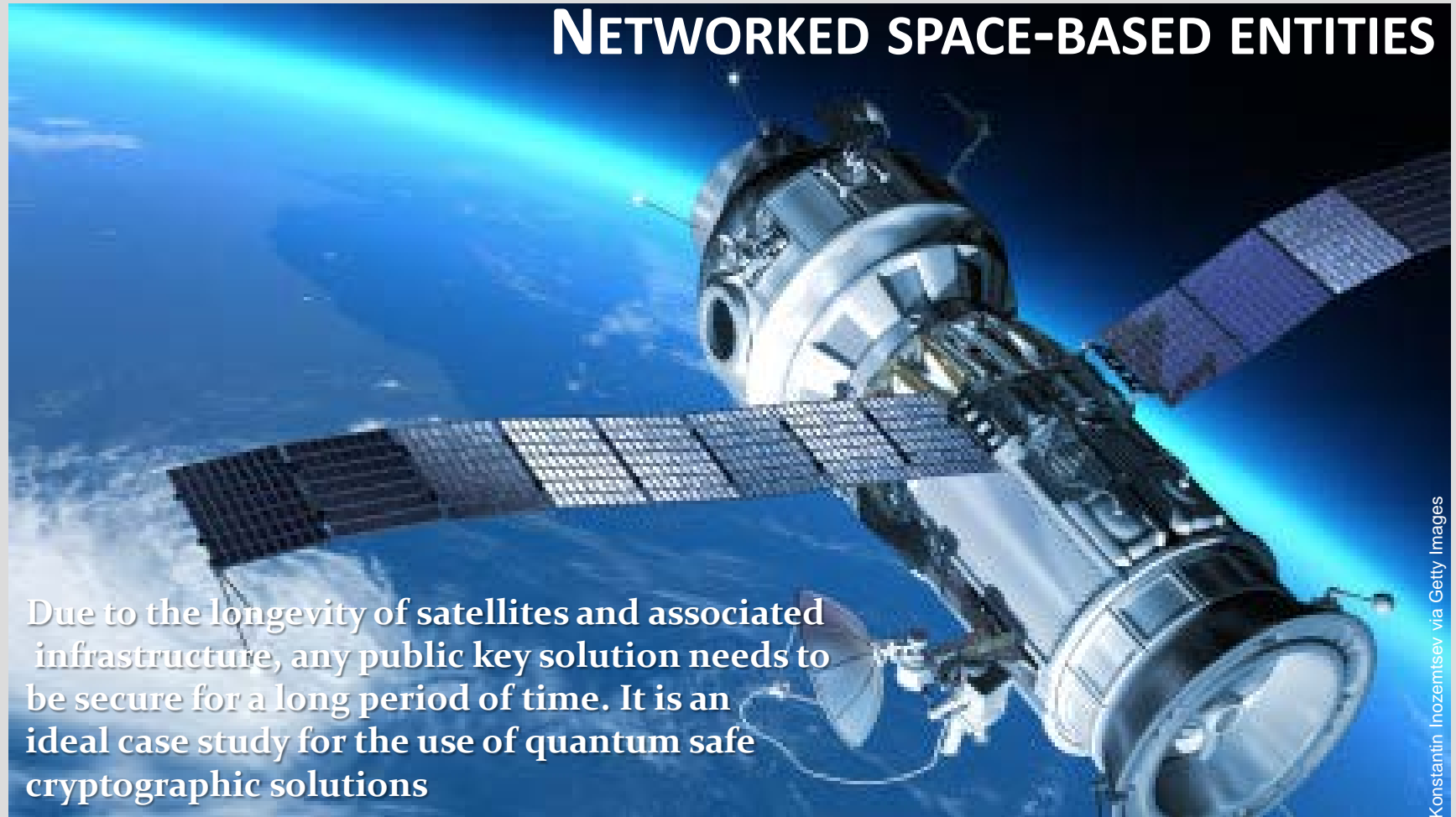
- Secure communications of networked space-based entities
- Trusted components for critical communication applications
- Privacy-preserving municipal data analytics

Organisation sponsors:



SAFEcrypto Case Studies

NETWORKED SPACE-BASED ENTITIES



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

Konstantin Inozemisev via Getty Images

Organisation sponsors:



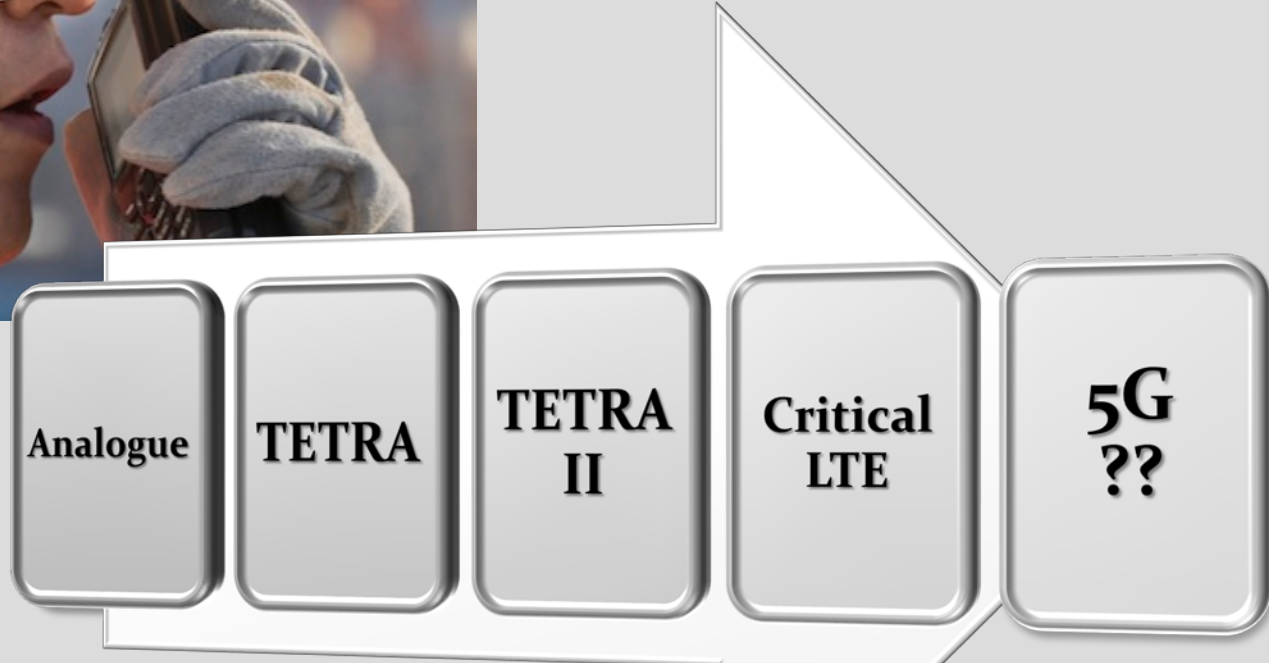
Public Safety Communications

http://www.delencaandsecurity-airbusds.com/pl_P/tetra-communication-system12

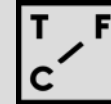


In Future, use of COTS devices and legacy equipment will underpin the operation of public safety communications.

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



Organisation sponsors:





Privacy-preserving municipal data analytics



Organisation sponsors:





Quantum-Safe Cryptography

Timeliness of SAFEcrypto project ...

The screenshot shows the NSA website's 'Information Assurance' section. At the top, it features the logos for the National Security Agency and the Central Security Service, with the tagline 'Defending Our Nation. Securing The Future.' Below this is a navigation menu with 'INFORMATION ASSURANCE' highlighted. The main content area is titled 'Cryptography Today' and contains the following text:

Home > Information Assurance > Programs > NSA Suite B Cryptography

Cryptography Today

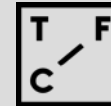
In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure,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

The left sidebar lists various information assurance topics, with 'IA Programs' expanded to show 'Commercial Solutions for Classified Program'.

August 2015

Organisation sponsors:





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)



Queen's University
Belfast



INVENTEURS DU MONDE NUMÉRIQUE

Università
della
Svizzera
italiana

RUHR
UNIVERSITÄT
BOCHUM

RUB

- Industry partners

EMC/RSA



HWCommunications Ltd



Thales UK

THALES

Organisation sponsors:





Questions & Answers



www.safecrypto.eu

Gavin McWilliams
g.mcwilliams@qub.ac.uk

Organisation sponsors:

