# Key Management for Quantum-safe Cryptography

NIST Workshop
Cybersecurity in a Post-Quantum World
April 2-3, 2015

# Participants

- **Goal:** explore the issues and opportunities in key management for quantum-safe cryptography
  - **Bob Griffin (moderator),** Chief Security Architect at RSA, the Security Division of EMC
  - **Liz O'Sullivan (panellist)**, Lecturer at the Centre for Secure Information Technology (CSIT) , Queen's University Belfast
  - **Sean Parkinson (panelist)**, Consultant Software Engineer at RSA, the Security Division of EMC
  - **Gregoire Ribordy (panelist),** CEO of IDQuantique
  - **William Whyte (panelist)**, Chief Scientist at Security Innovation

# SAFECrypto Project

(Secure Architectures of Future Emerging Cryptography)

- **4-year project funded under the European Union Horizon 2020 program**
  - 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
  - Project kick-off in January 2015
  - Focus on lattice-based crypto
  - Includes key management work package
  - Use cases include satellite communication, embedded systems, and municipal data analytics

- **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
  - HWCommunications Ltd
  - Thales

# Questions

- What are the **use cases** that key management must address in the post-quantum world? Where do those use cases diverge from ones currently understood and implemented in key management solutions? (William, Gregoire)

- What are the **critical technical issues** that need to be addressed in order to achieve effective key management for post-quantum crypto? (Liz, Sean)

- How well do **existing key management** approaches address these use cases and the particular requirements of quantum-safe cryptography? What do existing key management capabilities reveal about the requirements for architecture and design of key management for post-quantum crypto? (Gregoire, Sean)

SAFE crypto

# Questions - 2

- How best can a **transition** to quantum-safe cryptography in general, and quantum-safe cryptographic key management in particular, be managed? When do we know that algorithms are ready to be trusted and what do we do before then? (William, Gregoire)

- What **research efforts, standards efforts or implementations** are currently working on key management for quantum-safe cryptography? What do these efforts indicate about the issues and concerns unique to post-quantum crypto key management? (Liz, Sean)

- How important is **interoperability in key management** for post-quantum crypto? What processes and programs should be considered to improve interoperability across post-quantum crypto key management implementations? (Gregoire, William)