Contribution ID: **4** Type: **Roundtable Member**

Quantum Computers and Preparing Future-Proof Encryption

Monday, 5 November 2018 16:10 (5 minutes)

After making computer chips with the smallest possible transistors, researchers and technologists are pursuing new technologies including qubits - the beginnings of practical quantum computers. In this talk I'll do an introduction to what advantages that quantum computers have over today's classical computing, how internet and email security would be impacted, and how we could start securing our systems and servers with post-quantum encryption (PQE).

From following and meeting with a few startups in this space, I plan to present an overview of expected developments in the next few years (mainly in chemistry and other research problems), and why Google and Akamai are already evaluating present-day solutions to the future post-quantum encryption problem. NIST is currently evaluating multiple proposals for a PQE standard, especially lattice-based encryption.

As a software engineer I have previously worked on two related open source libraries: jsQuil (for JavaScript programming of remote quantum computers) and CodeCrypt (a drop-in replacement for GPG).

Topics

CHA2

Primary author: Mr DOIRON, Nicholas (McKinsey & Company)

Presenter: Mr DOIRON, Nicholas (McKinsey & Company)

Session Classification: [CHA] Keeping Pace with IT Security - Threat Intelligence for the IAEA/Nuclear Regulatory World

Track Classification: Addressing Growing Safeguards Challenges (CHA)