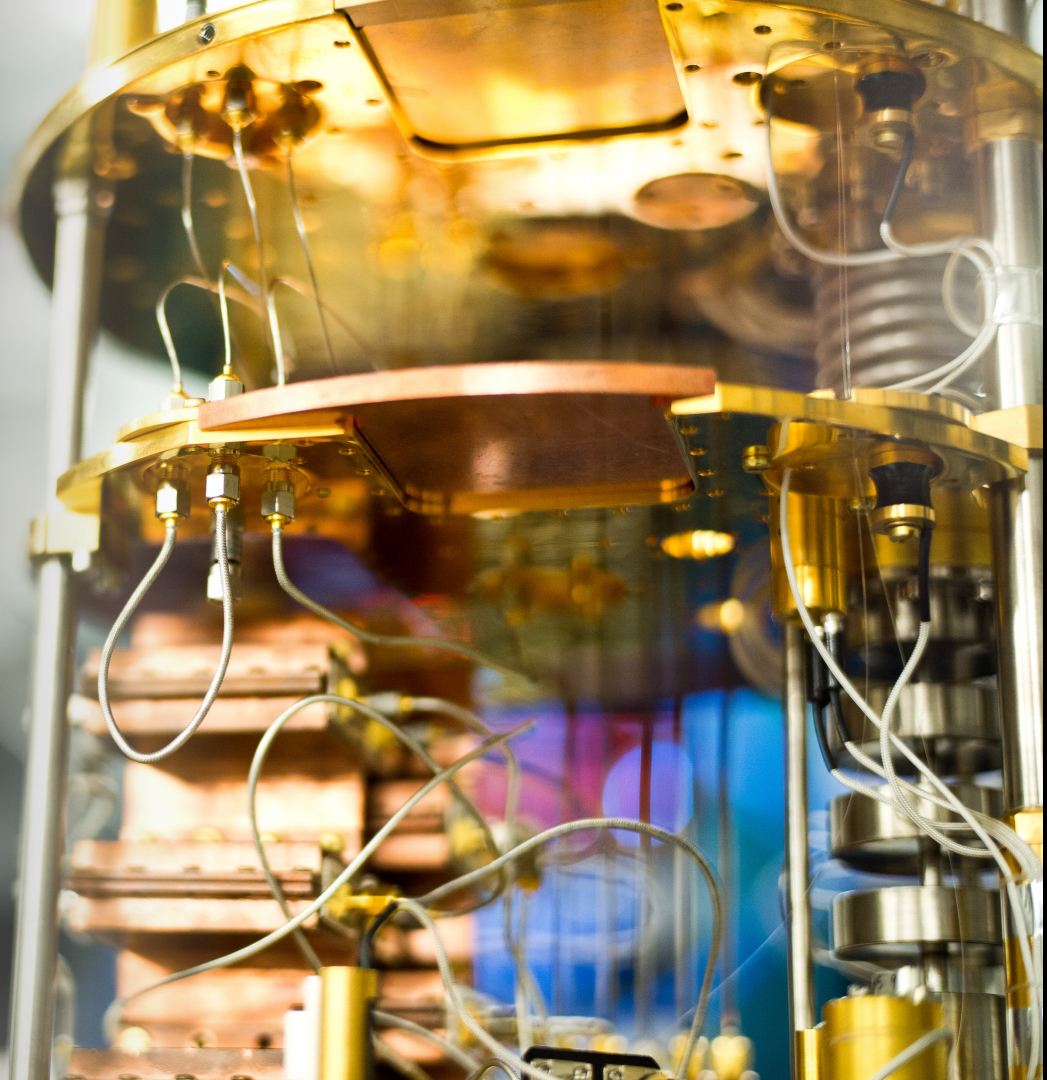
IBM **Research**

Quantum Safe Cryptography

Introducing the IBM Research Security Reviews subscription

Stay current with the world's leading security research



IBM Research offers clients in-depth reviews of cutting-edge cryptography research

Why keep up-to-date with crypto research?

- With the advent of quantum computers, cryptography today is facing a revolution
- There is an explosion of hundreds of new crypto algorithms that are quantum-safe, with the field evolving at a very rapid pace
- These changes will significantly impact many applications
- Corporations need trusted advice on managing the transitions, understanding new standards, and identifying associated risks

IBM is a long-standing leader in cryptography research, with an eye for real-world issues

- IBM has decades of experience in cryptography research and is a world leader on many fronts, for example, in setting new quantum-safe crypto standards in collaboration with NIST and ETSI
- IBM is blazing the trail for quantum computing, while in parallel developing the next generation security solutions. This combined insight gives us a balanced perspective on the risk and impact for our clients
- IBM has a solid understanding of real-world issues that our clients are facing, starting with financial services and crossing most every industry

IBM Research Security Reviews subscription

- A new subscription model offering from IBM research
- Our focus in the first year is on **quantum-safe crypto research**
- Also, related topics such as crypto agility will be featured
- Learn what IBM Research is thinking on this fast paced topic

IBM

The first year of the IBM Research Security Reviews will focus on quantum-safe cryptography

Subscribers can expect:

- Commentary on global standardization efforts of quantum-safe crypto. Various standards organizations are defining standards for quantum-safe cryptography. IBM is deeply involved in this process and will provide clients with a first-hand account of the latest developments

- New algorithms research overview and status, such as for:
  - Multivariate crypto
  - Code-based crypto
  - Lattice-based crypto
  - Hash-based signatures / symmetric crypto
  - Super-singular isogenies-based crypto

- A practical perspective on implementing cryptographic agility

Quantum computers are moving out of the lab and may some day be able to break widely-used cryptography methods

Quantum-safe cryptography includes new algorithms that may run on classical compute platforms but are robust against the anticipated capabilities of future quantum computers.

Example: Lattice cryptography hides data inside complex algebraic structures called lattices

IBM

Quantum-Safe Cryptography:
IBM **Research** Security Reviews Subscription

Topics:

a) Quantum risk to cryptography
b) Quantum safe cryptography standards
c) Quantum safe cryptography performance and optimization
d) Implication of quantum algorithms to networks, infrastructure, services and applications
e) Quantum safe migration strategies
f) Cryptographic and cyber-security agility

Delivery:

a) Initial background report available now *(see the sample)*
b) Reports published quarterly including updates on cryptography research
   → Next report to be published on September 23, 2019
c) Seminars aligned with an IBM Q Network quarterly meeting or event
   → Next seminar on October 2, 2019 at IBM Research in Zurich
d) Subscription ends on June 30, 2020

Enrollment:

a) Corporate subscription price starts at $15K/seat (enterprise license also available)
b) Request a *sample contract* from your IBM Representative

2nd PQC Standardization Conference

August 22-24, 2019
University of California, Santa Barbara

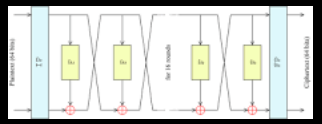
The NIST Post-Quantum Cryptography Standardization Process has entered the next phase, in which 26 second-round candidates are being considered for standardization. NIST plans to hold a second NIST PQC Standardization Conference in August 2019 to discuss various aspects of these candidates, and to obtain valuable feedback for the selection of the finalists. NIST will invite each submission team of the 26 second-round candidates to give a short update on their algorithm.

Published on the NIST website

Perspectives from IBM Research can help you understand what to expect and how to plan

IBM

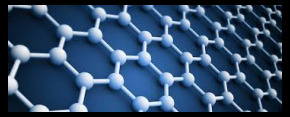
IBM Research offers unique expertise with decades of deep research in cryptography and quantum computing



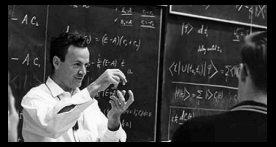
On 17 March 1975, the IBM developed DES system was published in the Federal Register.

In 1995, the IBM designed HMAC system was published in RFC 2104 and later standardized as FIPS 198

In 2009 Craig Gentry's breakthrough on Fully Homomorphic Encryption based on lattice constructs



2018: CRYSTALS – Dilithium: Digital Signatures from Module Lattices, CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM submitted to NIST PQC Process



In May 1981, IBM and MIT hosted a conference where Richard Feynman came up with the idea of quantum computers

*In May 2016, IBM was the first company to make quantum computers available for free online with the **IBM Q Experience**. In 2017, IBM followed up with the **IBM Q Network** for business and academia*

IBM Researchers now regularly publish ground-breaking work on real quantum computers

*Designed by IBM scientists, systems engineers and industrial designers, **IBM Q System One** is optimized for stability, reliability, and continuous commercial use*

IBM Research, Thomas J. Watson Research Center
1101 Kitchawan Rd. Yorktown Heights, NY 10598, USA

IBM Research Security Reviews subscription

All information contained in this document is for informational purposes only and subject to change without notice. The terms and conditions of the subscription agreement with IBM will govern the IBM Research Security Reviews, and nothing in this presentation shall be considered a legally binding obligation.

To subscribe, contact IBM Research at securityreport@zurich.ibm.com