ETSI
The Standards People

Security Conference

Simple and Effective Methods to Achieve Quantum Security Today

Presented by: Daniel Shiu

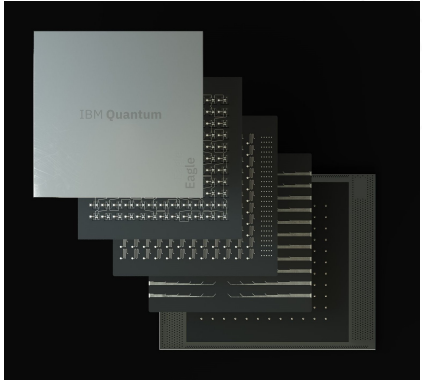
ARQIT

17/10/2023

Stronger, simpler encryption

ARQIT

My Latest Qualification

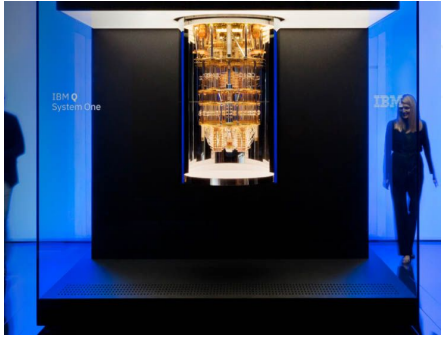


Stronger, simpler encryption

ARQIT

IBM Roadmap

Year	Name	# Qubits
2019	Falcon	27
2020	Hummingbird	65
2021	Eagle	127
2022	Osprey	433
2023	Condor	1121 (?)
2024	Flamingo	1386 (+?)
2025	Kookaburra	4158 (+?)
2026+	?	10K-100K (?)



Stronger, simpler encryption

AROIT

Some Headlines

Microsoft achieves first milestone towards a quantum supercomputer

June 21, 2023 • 8 min read

A Hole New World: RIKEN's Breakthrough in Silicon Quantum Dot Lifespan

TOPICS: Quantum Computing RIKEN Semiconductors

By RIKEN MAY 14, 2023

Quantum Breakthrough: A New Method for On-Chip Generation of Single Photon

TOPICS: Chips Electrical Engineering Photon Popular Quantum Technology UC Santa Barbara

By UNIVERSITY OF CALIFORNIA - SANTA BARBARA FEBRUARY 13, 2023

FORBES > INNOVATION > ENTERPRISE TECH

IBM Achieves Breakthrough In Quantum Computing

Karl Freund Contributor ⊙

Founder and Principal Analyst, Cambrian-AI Research LLC

Follow

0 Jun 14, 2023, 11:00am EDT

Quantinuum Launches H2, Reports Breakthrough in Work on Topological Qubits

By John Russell

May 9, 2023

Breakthrough Experiment Translates Quantum Information Across Technologies, Improving Quantum Communication

Margaret Davis Mar 25, 2023 02:58 AM EDT

Stronger, simpler encryption

ARQIT

Meanwhile: PQC and Migration

Keeping it Simple

- The quantum technologies are showing early signs of exponential growth
- Transition to PQC has many issues

Keeping it Simple

- The quantum technologies are showing early signs of exponential growth
- Transition to PQC has many issues
- Minimise dependence on PKC

A Simple Alternative

Symmetric key agreement

- Decades of experience at the enterprise level
- Diverse, agile, established, quantum resistant primitives
- Active trust management
- Efficient in bandwidth and computation

Standards Compatibility

- ISO/IEC 11770-2 IT Security techniques - Key management - Part 2: Mechanisms using symmetric techniques
- RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security
- RFC 9258 Importing External Pre-Shared Keys (PSKs) for TLS 1.3

Don’t take my word for it

NIST SP800-71

The protection of symmetric keys using symmetric key-wrapping schemes and replacing asymmetric digital signature schemes with symmetric-key message authentication schemes is one approach to replacing public key cryptographic key management in the relatively near term.

CNSA2.0 FAQ

NSA considers using pre-shared keys in a standards-compliant fashion a better near-term post-quantum solution than implementing experimental post-quantum asymmetric algorithms.

Migration Time?

- Days/hours
- Available today from multiple partners.

In Summary

Symmetric Key Agreement

- Simple, effective, quantum safe
- Compatible with existing standards
- Integration in days or hours
- It is available today

Thank you for listening

Questions?