
BROADCOM
WHITE PAPER
The Impact of Quantum Computing on Encryption

WHITE PAPER

The Impact of Quantum Computing on Encryption

TABLE OF CONTENTS

Overview

The future arrival of quantum computing should be concerning for any company using the Internet or encryption for data at rest. Quantum computing promises improvements to many sectors, but also threatens today's "unbreakable" encryption cipher suites and algorithms. While many are diligently working to make this kind of computing a reality, others are working just as diligently to develop quantum-resistant cryptography: ciphers and algorithms to ensure that privacy and trust will persevere.

The Background of Quantum Computing

Fundamentally, quantum computing provides significant advances in many areas of advanced computation. Sectors including finance (Axa, Citigroup, HSBC), pharmaceuticals (Pfizer, McKinsey, Roche), manufacturing (Volkswagen, BASF, Airbus), logistics (DHL, Ceva), and technology (6G networks, Intel, Cisco) can benefit from the promise held by quantum computing. In each of these areas, multiple and complex calculations lasting days or months could benefit from a faster time-to-solution that quantum computing may be able to provide.

Current Activity within Quantum Computing

In broad terms, quantum computing is moving beyond technology proofs and into an era now called noisy intermediate-scale quantum (NISQ), where quantum computers are demonstrating that they can solve problems more efficiently than classical computers can. While there is debate about whether some quantum computers are faster than classical computing, a general-purpose quantum computer that can perform *any* task faster than current supercomputers is still, at this time, in the future. Focus has shifted from just increasing the number of qubits and now also includes the following:

- Reducing noise, which ruins the results of computation
- Isolating which components of big data problems are good for quantum computers to operate on
- Developing tooling so programmers can work effectively with emerging hardware

Multiple quantum processor technology approaches are being developed by corporate, academic, and foundation-based groups. Groups working in one technology area are not necessarily competitive with others in that technology area; the field is new enough and broad enough to allow simultaneous, non-competitive progress. These advances vary in approach and range, and focus on several areas:

- Superconducting circuits
- Atomic-based approaches
  - Individual neutral atoms
  - Ions trapped by magnetic fields
- Photon-based approaches

See the Appendix for additional information regarding each approach.

Moving beyond hardware, the next level of the stack to tackle will include compilers, libraries, and SDKs making the hardware accessible to those attempting to solve real-world problems, quantumly.

The Quantum Computing Threat

Algorithms such as RSA, Diffie-Hellman (DH), and elliptic-curve cryptography (ECC) are all potentially solvable by quantum computers. One prominent attack is the store-now, decrypt-later attack, where encrypted traffic or files are stolen now and saved until a time when a quantum computer is available to decrypt them.

In 1994, Peter Shor, PhD, discovered a method that would quickly allow a quantum computer to calculate the private key from the public key, ruining the security guarantee of these algorithms. The date of development of the quantum computer that can do this has been called Q-Day, the day it will be *too late*. The approach of Q-Day is closely monitored by industries and researchers.

Quantum Computation Advancement

While the current technology still has a long way to go to fully achieve quantum computing, novel approaches by different organizations are demonstrating significant gains, bringing Q-Day closer.

Table 1: Progress to Q-Day. Target Algorithm to Crack: RSA 2048

Year	Qubits and Quantum Gates	Solve Time	References
1994	Peter Shor proposed Quantum		
2015	1 billion qubits	26.7 hours	*Surface codes: Towards practical large-scale quantum computation* University of Melbourne, UC Santa Barbara
2019	20 million qubits	8 hours	*How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits* Google, KTH Royal Institute of Technology, Swedish NCSA
2022	6.2 million qubits	7.1 hours	*Assessing requirements to scale to practical quantum advantage* MSFT research, ETH Zurich
2023	10,000 qubits and 2 trillion gates	104 days	*Fujitsu quantum simulator assesses vulnerability of RSA cryptosystem to potential quantum computer cryptography threat*
2024	1700 qubits and 69 billion gates	Not provided	*Reducing the Number of Qubits in Quantum Factoring* University of Rennes

WHILE TECHNOLOGY STILL HAS A LONG WAY TO GO TO ACHIEVE QUANTUM COMPUTING, NOVEL APPROACHES DEMONSTRATE SIGNIFICANT GAINS.

NIST IS DEVELOPING, TESTING, AND WILL DELIVER ALGORITHMS TO KEEP DATA AND COMMUNICATIONS SAFE AS QUANTUM COMPUTING PROGRESSES.

Defending against Quantum Computing

Foreseeing a need for protection after Q-Day, NIST began a process in 2016 to replace RSA, DH, and ECC with algorithms that will work after a capable quantum computer is developed. Generally, this has been called post-quantum cryptography (PQC).

Popular software libraries, such as BouncyCastle, wolfSSL, and the BoringSSL/openssl fork Open Quantum Safe, offer implementations of the NIST PQC finalist candidate algorithms: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+.

Broadcom Activity with Regards to Post-Quantum Cryptography

Broadcom is taking several courses of action with regards to post-quantum cryptography:

- Broadcom is closely monitoring the following:
  - Standards bodies such as NIST and the IETF for the latest developments on post-quantum cryptography
  - Hardware manufacturers for the latest developments in quantum computing
  - Developments in quantum cryptanalytic research by commercial and academic bodies
  - Various foundations and other interested organizations
- Broadcom is working with our cryptographic experts and software partners as new algorithms are verified and supported.
- Broadcom product teams are working towards crypto agility, preparing products to make it easier to swap both critical cryptographic modules and ciphers and algorithms for others if the need or customer's preference arises.

BROADCOM FOLLOWS THE GUIDANCE OF NIST AND OTHER LEADING ORGANIZATIONS, PREPARING PRODUCTS TO BE READY WHEN Q-DAY ARRIVES.

Summary

Quantum computing promises a revolution in advanced computing. Many verticals will benefit from these improvements, delivering solutions to their customers even faster. While the computing technology is still in the early stages, the estimated time needed to crack ciphers is showing rapid progress. NIST and other bodies are developing, testing, and will deliver algorithms to keep data and communications safe as quantum computing progresses. Broadcom is following the guidance of NIST and other leading organizations and preparing products to be ready before Q-Day arrives.

Appendix

Several main quantum technologies are currently being explored.

Superconducting Circuits

Technology – Superconducting circuits utilize the quantum effects of tiny electronic circuits that are cooled to near absolute zero.

Current status – IBM has an aggressive roadmap and has been producing a large number of quantum processors. IBM hit scale with 1121 qubits in December 2023 with its Condor release. The IBM Heron is modular and expected to hit 100 million operations in 2024 onboard the IBM Quantum System Two. The Rigetti Ankaa-2 system is using 84 superconducting qubits. University of Science and Technology of China (USTC) had a 66-qubit system in 2021. Google has also developed technology in this area with several processors such as the Sycamore with 54 qubits in 2018.

Atomic-Based Approach: Neutral Atoms

Technology – Individual, non-charged atoms (neutral atoms) are manipulated and operated on using laser pulses. Atomic-based systems must be cooled to prevent thermal noise from destroying the calculation.

Current status – A trio of organizations are evaluating neutral atom quantum technology. The QuEra rubidium-based Aquila appears to have the edge with 256 physical (10 logical) qubits. The Phoenix computer from Atom Computing currently has 100 qubits based on strontium. Pasqal is also using rubidium atoms and is producing results. Each atom is nudged into place using optical tweezers, which are very precise lasers. Different pulses of light help read from and write to these atoms.

Atomic-Based Approach: Trapped Ions

Technology – Individual charged atoms (ions) are controlled with magnets. The ions are manipulated with magnetic fields and operated on with laser pulses. Atomic-based systems must be cooled to prevent thermal noise from destroying the calculation.

Current status – Two organizations are looking at non-neutral atoms. Quantinuum is using ytterbium atoms ionized by a laser in a magnetic trap, where it is moved into position. Lasers are used to read and write. Quantinuum has pushed this to 32 qubits. IonQ is also using ytterbium ions and is also up to 32 qubits.

Photonic

Technology – Light-based systems (photons) have emerged that operate on photons instead of electrons. Currently this also needs to be supercooled, but this may be able to operate at room temperature soon.

Current status – Three organizations are working on quantum computers utilizing laser pulses instead of atoms. Mid-2022, the Borealis quantum computer from Xanadu used 216 squeezed states that are akin to qubits. In 2020, USTC created one named Jiuzhang that uses 50 indistinguishable single-mode squeezed states. Quandela is a startup offering up to 12 photonic qubits on their modular MosaiQ system.

IMS-QuantumCryptography-WP100 April 3, 2024