ExpertInsights@IBV

Wielding a double-edged sword

Preparing cybersecurity now for a quantum world

IBM Institute for Business Value

A call to action

Large-scale quantum computers will significantly expand computing power, creating new opportunities for improving cybersecurity. Quantum-era cybersecurity will wield the power to detect and deflect quantum-era cyberattacks before they cause harm. But it could become a double-edged sword, as quantum computing may also create new exposures, such as the ability to quickly solve the difficult math problems that are the basis of some forms of encryption. While post-quantum cryptography standards are still being finalized, businesses and other organizations can start preparing today.

Here comes quantum computing

Quantum mechanics is a branch of physics that explores how the physical world works at a fundamental level. At the quantum level, particles can take on more than one state at the same time, and they can have their states correlated even when separated by a large distance. Quantum computing harnesses these quantum phenomena to process information in a profoundly new way.[1] The worldwide market for quantum computing is predicted to be more than USD 10 billion by 2024.[2]

Today's classical computers use two primary classes of algorithms for encryption: symmetric and asymmetric. In symmetric encryption, the same key is used to encrypt and decrypt a given piece of data. The Advanced Encryption Standard (AES) is an example of a symmetric algorithm. Adopted by the US government, the AES algorithm supports three key sizes: 128 bits, 192 bits, and 256 bits.[3] Symmetric algorithms typically are used for bulk encryption tasks, such as enciphering major databases, file systems and object storage.

In asymmetric encryption, data is encrypted using one key (usually referred to as the public key) and is decrypted using another key (usually referred to as the private key). Although the private key and public key are different, they are mathematically related. The widely employed Rivest, Shamir, Adleman (RSA) algorithm is an example of an asymmetric algorithm. Even though it is slower than symmetric encryption, asymmetric algorithms solve the problem of key distribution, which is an important issue in encryption.

How quantum computing computes

Instead of using binary bits of 0s and 1s, as classical computers do, quantum computers use quantum bits, or "qubits," as very complex switches. Due to their enhanced processing power, quantum computers are expected to solve problems that are "intractable" using today's machines.[4] Two qubits can represent 4 values simultaneously. Three qubits can represent 2^3 or 8 values simultaneously. Fifty qubits can represent more than one quadrillion values simultaneously, and 100 qubits can represent more than one quadrillion squared.[5]

Quantum risks to cybersecurity

A cryptographic future

The first interoperable data encryption standard, called DES, and the ubiquitous HMAC standard are the cornerstones of most of today's data authentication schemes. **For the quantum era**, new cryptographic algorithms that protect systems against current and future threats are under development by several companies, including IBM. One example: a new generation of lattice-based cryptography designed to provide security from attacks by both quantum and classical computers. Another example is called "fully homomorphic encryption," which may make it possible to perform unrestricted operations over encrypted data without surrendering confidentiality.

The advent of quantum computing will lead to changes to encryption methods. Currently, the most widely used asymmetric algorithms are based on difficult mathematical problems, such as factoring large numbers, which can take thousands of years on today's most powerful supercomputers. However, research conducted by Peter Shor at MIT more than 20 years ago demonstrated the same problem could theoretically be solved in days or hours on a large-scale quantum computer.[6] Future quantum computers may be able to break asymmetric encryption solutions that base their security on integer factorization or discrete logarithms.

Although symmetric algorithms are not affected by Shor's algorithm, the power of quantum computing necessitates a multiplication in key sizes. For example, large quantum computers running Grover's algorithm, which uses quantum concepts to search databases very quickly, could provide a quadratic improvement in brute-force attacks on symmetric encryption algorithms, such as AES.[7] To help withstand brute-force attacks, key sizes should be doubled to support the same level of protection. For AES, this means using 256-bit keys to maintain today's 128-bit security strength.[8]

Even though large-scale quantum computers are not yet commercially available, initiating quantum cybersecurity solutions now has significant advantages. For example, a malicious entity can capture secure communications of interest today. Then, when large-scale quantum computers are available, that vast computing power could be used to break the encryption and learn about those communications.

Wielding the power of quantum cybersecurity

Eclipsing its potential risks, quantum cybersecurity can provide more robust and compelling opportunities to safeguard critical and personal data than currently possible. It is particularly useful in quantum machine learning and quantum random number generation.

Machine learning already has numerous applications in cybersecurity, including:

- *Behavior anomaly detection:* recognizing anomalous activities, such as access from a new device, new location or at a new time.
- *Classification:* categorizing entities such as data, users, threat actors or malware.
- *Prediction:* anticipating events such as a network or database threat.

Quantum computing may speed up machine learning, enhancing its efficacy for cybersecurity. For example, quantum-enhanced machine learning could expedite the classification of massive amounts of data.

Quantum random number generation. Random number generation is essential in cryptography. The two main categories of classical random number generation are pseudo random number generators (PRNGs) and true random number generators (TRNGs).

Quantum Random Number Generators (QRNGs) can be thought of as a special case of TRNGs in which the data is the result of quantum events. But unlike traditional TRNGs, QRNGs promise truly random numbers by exploiting the inherent randomness in quantum physics. A true random number generator provides the highest level of security because the number generated is impossible to guess.

Generating random numbers

One way to look at the difference between PRNGs and TRNGs is thinking about spinning a roulette wheel. PRNGs generate random numbers by spinning the wheel many times and keeping a list of the outcomes. When a random number is required, it provides the next answer on the list. The random number is already predetermined. TRNGs work by spinning the wheel each time a random number is required without a pre-determined list.[9]

Getting started

A recipe for a smooth transition

In the cybersecurity world, much has been conjectured about quantum computers' eventual ability to breach current cryptography. Before that day arrives, forward-thinking enterprises are implementing cybersecurity solutions that protect against both classical and quantum-based computing attacks ensuring their transition to the quantum era to be a smooth one.

To prepare for the coming post-quantum cryptography era, enterprise leaders can take four steps now:

1. Identify, retrain or recruit for the necessary quantum cybersecurity skills, either directly or through your organization's ecosystem. These experts should become your organization's cybersecurity champions. They can collaborate with standards bodies, deduce the implications of various potential quantum cybersecurity approaches and create your organization's quantum security transition plan.
2. Begin identifying where post-quantum security methods should be adopted throughout your organization by assessing your potential quantum-era security exposure:
   - *Symmetric encryption algorithms:* Where symmetric algorithms remain appropriate in your organization in the quantum era, at least double the key sizes currently being used to help ensure an appropriate future level of security strength. [10]
   - *Asymmetric encryption algorithms:* Identify where asymmetric algorithms are in use today and plan to switch to post-quantum alternatives.
   - *Hashing algorithms:* Assess the output sizes currently being used and plan to use larger output sizes.
3. Keep up-to-date with advances in post-quantum cybersecurity standards and emerging post-quantum security solutions, such as lattice-based approaches, code-based cryptography, multivariate cryptography and hash-based cryptography, among others.
4. Work with encryption solution providers to deploy quantum-safe alternatives as they become available.

Notes and sources

1 "What is quantum computing?" IBM. https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/

2 "Quantum Computing Technologies & Global Market, 2017-2024 Volume 1." Homeland Security Research Corp. 2017.

3 "Cryptographic algorithm and key length." IBM. https://www.ibm.com/support/knowledgecenter/en/SSWPVP_3.0.0/com.ibm.sklm.doc/overview/cpt/cpt_ic_oview_tech_cryptographic_algorithm.html

4 How do quantum computers work? https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/

5 Pednault, Edwin. "Quantum Computing: Breaking Through the 49 Qubit Simulation Barrier." IBM. October 17, 2017. https://www.ibm.com/blogs/research/2017/10/quantum-computing-barrier/

6 Nordstrom, Amy. "Quantum Computer Comes Closer to Cracking RSA Encryption." IEEE Spectrum. March 3, 2016. https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

7 "Quantum Computing Now Has a Powerful Search Tool." MIT Technology Review. April 5, 2017. https://www.technologyreview.com/s/604068/quantum-computing-now-has-a-powerful-search-tool/

8 Chang, Linus. "How secure is today's encryption against quantum computers?" betanews. October 13, 2017. https://betanews.com/2017/10/13/current-encryption-vs-quantum-computers/

9 Haahr, Mads, Dr. "Introduction to Randomness and Random Numbers." Random.org. https://www.random.org/randomness/

10 "IBM Multi-Cloud Data Encryption." IBM. https://www.ibm.com/us-en/marketplace/cloud-data-encryption

About ExpertInsights@IBV reports

ExpertInsights@IBV represents the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

Experts on this topic

Walid Rjaibi

IBM Distinguished Engineer and
Chief Technical Officer for Data Security
IBM Security
https://www.linkedin.com/in/walid-rjaibi-cissp-8325077/
wrjaibi@ca.ibm.com

Sridhar Muppidi

IBM Fellow, Vice President and
Chief Technical Officer
IBM Security
https://www.linkedin.com/in/smuppidi/
muppidi@us.ibm.com

Mary O'Brien

Vice President, Development
IBM Security
https://www.linkedin.com/in/mary-o-brien-4946a590/
obrienma@ie.ibm.com

New Orchard Road
Armonk, NY 10504
Produced in the United States of America
July 2018

39017839USEN-00