Making and Breaking Data Security With Quantum Machines

Disponible également en françaiss
www.isaca.org/currentissue

The characteristics of the quantum universe are not very intuitive when based on observations of everyday physics, which may explain why even theoretical physicist Albert Einstein found the phenomena "spooky."[1] Although the discipline is quite complex, it is important for IT professionals, particularly IT security experts, to familiarize themselves with the fundamental notions of quantum cryptography as an emerging means to enhance data privacy and security in today's world.

What Is Quantum Mechanics?

Richard Feynman, a Nobel Prize-winning physicist, once said, "If you think you understand quantum mechanics, you don't understand quantum mechanics."[2]

Quantum mechanics is a branch of physics based on how extremely small things, such as molecules, atoms, electrons and photons, behave in the universe. There are two main features of quantum particles that are useful to know: superposition and entanglement.

Superposition

Quantum particles can be in different positions (or states) at the same time and only collapse into one position when they are being observed. This phenomenon is known as superposition. Superposition is when a particle is in positions A and B at the same time, similar to a tossed coin while it is flipping in the air. The particle collapses into heads or tails only when measured (or in the case of the analogy, caught), and the result depends on random probabilities (often 50:50). For another example, elementary science lessons teach children how electrons revolve around the nucleus of atoms much like the planets revolve around the sun. Electrons also

DALIA KHADER | PH.D., CISSP, GSEC

Is the chief information security officer (CISO) for the international division of Swiss Life and a member of WomenCyberForce. She has more than 15 years of experience in the field of cybersecurity, including working in academia, during which she did extensive research in modern cryptography, working as a research associate at the University of Luxembourg (Kirchberg, Luxembourg) and working as a security architect for a telecom service provider. Khader won the 2021 CISO of the Year, Luxembourg award. Her work has been published by the World Economic Forum and Usenix and at RSA conferences. Her goal is to make complex cybersecurity concepts accessible to everyone. She can be reached at *https://lu.linkedin.com/in/dalia-khader-2b13b6a*.

HUSNA SIDDIQI

Is head of technology assurance management at a global organization. She has more than 16 years of experience in information security, data protection, IT risk and transformation program management across several sectors, including oil and gas, energy and utilities, consumer business, manufacturing, and professional services. Prior to becoming a consultant, Siddiqi was a computer science lecturer and a software engineer. She is chair of the independent advisory board for the UK Research and Innovation Centre for Accountable, Responsible and Transparent Artificial Intelligence (ART-AI) at the University of Bath (England). She is a World Economic Forum contributor with publications in several reputable forums. She aims to increase security and privacy awareness among diverse audiences using relatable examples and is actively involved in global initiatives to promote diversity and inclusion and address unconscious bias. She can be reached at *https://uk.linkedin.com/in/husna-siddiqi-5466158*.

spin (up or down depending on the spin orientation), much like the Earth rotates on its own axis. When applying the principle of superposition, the electrons can be spinning up and spinning down at the same time until measured. Once measured, an electron will collapse into a particle at either spin direction.

Entanglement

Quantum particles can be entangled in such a way that how one collapses impacts the other, even if they move extremely far from each other.

The particles can be imagined as two waves passing each other. As they move away, an invisible string ties them together forever, such that moving one will always impact the other. Entangled quantum particles could be many light years away from each other but still impact one another. If one electron is observed and collapses to spin upward, the other would immediately collapse to spin downward.

What Is Quantum Computing?

Before describing quantum computers, it is worth revisiting the basic elements of classical/modern-day computers.

They can enhance data security but can also be used to break security in classical computers unless protocols are quantum resistant.

Classical computers are built on electricity, and, in their simplest form, they store information based on two states: current flowing through (i.e., switch on) or current not flowing through (i.e., switch off). These states are mathematically represented in the form of binary digits (bits). A bit can be in one of two possible states: 1 or 0. If there are two bits, there are four possible bit combinations (i.e., 00, 01, 10, 11). A byte (8 bits) can have 256 combinations of 1s or 0s. The possible bit combinations rise exponentially with the number of bytes.

All mathematical problems, whether simple addition of two numbers or complex astronomy calculations, can eventually be broken down by classical computers into sequences of bits (0s and 1s). The memory capacity of computers, which is based on the number of bits, impacts the computational speed of solving problems.

Over time, memory sizes have grown exponentially due to advancements in technology. Gone are the days when bytes, kilobytes or megabytes would be brought up in conversation. Today, even when choosing a universal serial bus (USB), the discussion turns to gigabytes or terabytes. This extremely high volume of unstructured data can take a toll on classical computer processors, making it hard to keep up in terms of speed. Enter quantum computers.

The equivalent of bits in quantum computers are called quantum bits (qubits). However, quantum computers are different than classical computers. Unlike classical bits, a quantum bit can be in both states of 1 and 0 at the same time due to superposition. Where electrons are used for quantum computing, each qubit can spin up and spin down at the same time.

The very ability to be in multiple states at the same time radically increases problem-solving speed. Imagine a group of friends trying to find a jewel in a complex maze in the shortest possible time. The most logical thing to do would be to split up and take different routes to increase the probability of finding it sooner. As mentioned, there can be 256 combinations of bits in a byte. However, a byte of qubits can be in all 256 positions at the same time. Imagine how much quicker such a computer can find the best route to the treasure, compared to even the fastest classical computer that tries each route at a time. If two of the friends are "entangled" such that when one finds the treasure the other immediately ceases to look for the treasure, that could help save time and energy. The fact that quantum particles such as electrons can be entangled in this way helps speed processing time and eliminate wrong results faster.

Quantum Computing and Its Relationship With Cybersecurity

Quantum computers can be used as tools and as weapons. They can enhance data security but can also be used to break security in classical computers unless protocols are quantum resistant.

Cryptography—the art and math of writing and solving codes—is the key underlying discipline behind the techniques that protect data. Encryption is similar to placing data in a box that is locked; locking the box is easy, but the aim is to make unlocking it extremely hard for anyone not in possession of the key.

More complex applications of quantum cryptography, including the use of quantum particles for generating the actual message, are still being created.

Modern cryptography relies on calculations that cannot be reversed in a feasible amount of time within the computational powers of a classical computer. One of today's most widely used algorithms to secure emails and Internet transactions—RSA (using 2048 bit)—would require 300 trillion years to break security using classical computers. However, using powerful, error-free quantum computers, it could be broken in 10 seconds.

In fact, the quantum threat impacts the entire digital world, from Internet browsing to email to remote access of systems to mobile communication. The infrastructure of systems such as public key infrastructure (PKI), transport layer security (TLS), virtual private networks (VPNs), basic crypto libraries and secure hardware modules is based on algorithms such as factoring, elliptic curves and discrete logs. Imagine the magnitude of work effort needed to roll out new algorithms across the entire ecosystem and supply chain of the Internet as it is known today.

In 2016, the US National Institute of Standards and Technology (NIST) began creating new cryptographic standards to withstand quantum computing. The new standards are expected to be released by 2024.[3]

Even though today's quantum computers have significant scaling up to do, information protection experts are trying to stay ahead to protect data by using methods such as:

- **Quantum cryptography**—Relies on quantum physics properties to build new cryptographic algorithms
- **Quantum-resistant cryptography**—Continues to rely on mathematics; however, the choice of the underlying mathematic is hard to solve even with high computational power and memory capacity and, therefore, the cryptography based on the mathematics is unbreakable with quantum computing.

Quantum Cryptography

Quantum computing can enhance the security and privacy of data in ways that a classical computer cannot. One modern-day quantum cryptography application is quantum key distribution.

In traditional cryptography, one party (Alice) sends another party (Bob) the key to the locked box separately in a secure channel and then puts the locked box on public display, knowing only Bob can open it with the key. But if a cunning eavesdropper (Jane) manages to intercept the communication and make a copy of the key, she can impersonate the communication between Alice and Bob.

Researchers designed a key exchange algorithm, BB84, that involved the transmission of qubits through quantum channels using photons.[4] The values of the photons and the filter through which they were polarized are generated at random by Alice, and upon receiving the photons, Bob uses his own randomly generated filters to determine the values. Because the filters are aligned either vertically/horizontally or diagonally (i.e., +/- a 45-degree rotation), a mismatched filter will randomly provide a 1 or 0, while a matched filter will provide the exact value sent by Alice. After the transmission is completed, Alice tells Bob which filters she used. They agree to discard the value where their filters did not match (Bob is not a mind reader, so there may be several of these) and keep the remaining values to form a strong, random key.

If Jane tries to intercept the communication, she will be caught because quantum information cannot be copied or cloned. Due to the characteristics of quantum physics, such as no-cloning theorem (unlike digital bits, a quantum state cannot be identically copied)[5] and Heisenburg Uncertainty principle (it is not possible to know both speed and position of a quantum material; the act of measuring one makes the other unknown),[6] her attempts to measure the values will disrupt the communication and create noise, prompting Alice and Bob to realize what happened, abort the key exchange and start the process over. Only when they can generate the key without any suspicion of interception will Alice send the actual encrypted message through a classical channel that only Bob can decrypt.

A quantum key distribution protocol relying on the entanglement properties of photons has been designed.[7] More complex applications of quantum cryptography, including the use of quantum particles for generating the actual message, are still being created.

Challenges in Quantum Cryptography

The novel idea to design cryptographic schemes based on quantum computing poses plenty of

challenges, one being that the current network communication infrastructure is not compatible for quantum communication. How to effectively transfer quantum states remains in question. Another problem is that quantum cryptography still has room for growth in terms of sophisticated cryptographic schemes. In the meantime, traditional (mathematics-based) cryptography has improved, and the relative maturity has increased rapidly, making quantum-resistance cryptography a more feasible solution to resist quantum attacks.

Quantum-Resistant Cryptography

Modern cryptography relies on mathematical problems (e.g., integer factorization, discrete log, elliptic-curve discrete log problems) that can be solved but require a massive amount of computational power when using classical computers, taking up to trillions of years. These can still be broken in a feasible amount of time with a perfect quantum computer.

However, there are still some mathematical problems for which a solution has not yet been discovered or that can be reduced to worst-case scenarios instead of specific computational power. For example, factorization is used in today's cryptography because solving it requires better computational power and memory capacity in classical computers; while a good one-time password is breakable by trying to guess every single permutation of that password, the worst-case scenario is independent of the technology. More concrete examples of quantum-resistant cryptography include lattice,[8] multivariate[9] and hash-based[10] cryptography.

Challenges in Quantum-Resistant Cryptography

One of the challenges of algorithms that have undergone standardization efforts by NIST is reduced efficiencies due to factors such as the size of keys, ciphertext and signatures.

Another challenge with using post-quantum cryptography is that modern security is predominantly reliant on prequantum algorithms and making the switch would involve large-scale transformation and a high cost of adaptation.

For example, take the Open Systems Interconnection (OSI) model.[11] Most protocols and every single layer of the model would need to be redesigned to address data in transit, such as Transport Layer Security (TLS), Internet Protocol Security (IPsec), Wi-Fi Protected Access 2 (WPA2), Secure/Multipurpose Internet Mail Extensions (SMIME) and Secure Shell Protocol (SSH). Change would also be required in the hardware security modules and all the systems that provide security to data at rest.

Quantum Today

Today's quantum computers can only hold a small number of qubits, and scaling up is difficult because very precise environmental conditions are needed for particles to stay in the desired superposition or entangled states (e.g., extremely low temperature). Moreover, the fact that quantum information cannot be copied in the same way as digital information causes additional barriers to scalability.

Nonetheless, the qubit capacity of quantum computers has seen a remarkable increase in this millennium, from the experimental 2-qubit Yale processor in 2009[12] to the 127 qubit IBM processor in 2021.[13] In terms of transmitting photons for quantum key distribution, fiber optic links have seen a tenfold increase in length in the past decade (from 200 km spools to 1200 km satellite-based entangled distribution).[14, 15]

The fact that quantum information cannot be copied in the same way as digital information causes additional barriers to scalability.

There are numerous players in the quantum computing market today (e.g., IonQ, PsiQuantum, D-wave), in addition to pioneer tech giants such as Google,[16] IBM[17] and Intel,[18] that are in the race to build useful (million qubit) quantum computers someday.

In terms of security, quantum-resistant cryptography being mathematically oriented gives the world a stronger chance of success in preparing for the day quantum computing becomes a practical reality. The design of such algorithms is independent of the advancement in the quantum computing field. On the other hand, the building blocks of quantum computing and quantum-based cryptography rely on the same physics fundamentals, making the pace of progress of both comparable and the challenges in making and breaking security interlaced. Furthermore, every algorithm that was featured in round three of standardization efforts by NIST in 2021 was mathematics oriented using quantum-resistant techniques.[19]

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Conclusion

The developments in the field of quantum over the past century have been phenomenal—from discovering the spooky nature of quantum particles to visualizing a computer that can simulate the quantum environment to the emergence of very powerful (albeit small-scale) quantum computers that have immense potential to make or break cybersecurity. The next decade promises even more exciting developments from this marriage of physics and computer science, with 2022 expected to be the year of quantum breakthroughs.[20]

Authors' Note

The views expressed in this article do not reflect those of the authors' employers.

Endnotes

1 *MIT Technology Review,* "Einstein's 'Spooky at a Distance' Paradox Older Than Thought," 8 March 2012, *https://www.technologyreview.com/2012/03/08/20152/einsteins-spooky-action-at-a-distance-paradox-older-than-thought*

2 Gleick, J.; "Richard Feynman," *Encyclopedia Britannica*, 7 May 2022, *https://www.britannica.com/biography/Richard-Feynman*

3 US National Institute of Standards and Technology (NIST), "NIST Asks Public to Help Future-Proof Electronic Information," USA, 20 December 2016, *https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information*

4 Bennett, C. H.; G. Brassard; "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science*, vol. 560, p.175–179

5 Wootters, W. K.; W. H. Zurek; "A Single Quantum Cannot Be Cloned," *Nature*, vol. 299, iss. 5886, 1982, p.802–803

6 Heisenberg, W.; *The Physical Principles of the Quantum Theory*, Dover Publications, USA, 1949

7 Ekert, A. K.; "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, vol. 67, 5 August 1991

8 Ajtai, M.; "Generating Hard Instances of Lattice Problems," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, July 1996, p. 99–108

9 Wolf, C.; B. Preneel; "Asymmetric Cryptography: Hidden Field Equations," *European Congress on Computational Methods in Applied Sciences and Engineering*, 2004

10 Preneel, B.; "Design Principles for Hash Functions Revisited," Cryptographic Hash Workshop, National Institute of Standards and Technology, 2005, *https://csrc.nist.gov/CSRC/media/Events/First-Cryptographic-Hash-Workshop/documents/preneel_nist_v2.pdf*

11 Forcepoint, "The OSI Model Defined," *https://www.forcepoint.com/cyber-edu/osi-model#:~:text=The%20OSI%20Model%20(Open%20Systems,between%20different%20products%20and%20software*

12 Quantum Thought, "History of Quantum Computing: A Timeline," 29 June 2020, *https://www.quthought.com/post/history-of-quantum-computing-a-timeline*

13 IBM, "IBM Unveils Breakthrough 127-Qubit Quantum Processor," 16 November 2021, *https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor*

14 Homeland Security News Wire, "Quantum Keys Sent Over 200-km Fiber-Optic Link," 5 June 2007, *https://www.homelandsecuritynewswire.com/quantum-keys-sent-over-200-km-fiber-optic-link#:~:text=In%20an%20experiment%20conducted%20at%20a%20Stanford%20lab%2C,been%20sent%20over%20a%20record-setting%20200-kilometer%20fiber-optic%20link*

15 Yin, J.; Y. Cao; Y.-H. Li; *et al.*; "Satellite-Based Entanglement Distribution Over 1200 Kilometers," *Science*, vol. 356, iss. 6343, 16 June 2017, p. 1140–1144, *https://www.science.org/doi/10.1126/science.aan3211*

16 Porter, J.; "Google Wants to Build a Useful Quantum Computer by 2029," *The Verge*, 19 May 2021, *https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor*

17 IBM, "The Quantum Decade," *https://www.ibm.com/thought-leadership/institute-business-value/report/quantum-decade*

18 Martin, D.; "Turning A Million-Qubit Quantum Computing Dream Into Reality," The Next Platform, 10 May 2022, *https://www.nextplatform.com/2022/05/10/turning-a-million-qubit-quantum-computing-dream-into-reality/amp/*

19 National Institute of Standards and Technology, "Post-Quantum Cryptography (PQC)," USA, *https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions*

20 Samhitha; "Quantum Computing in 2022: A Leap Into the Tremendous Future Ahead," *Analytics Insight*, 2 January 2022, *https://www.analyticsinsight.net/quantum-computing-in-2022-a-leap-into-the-tremendous-future-ahead/*