

PRESCOUTER

April 2022

Quantum Computing
and Cybersecurity

Preparing for **Post-Quantum Cryptography**





Quantum computing represents the biggest threat to data security in the medium term since it can make attacks against cryptography much more efficient.

Despite encrypted data appearing random, encryption algorithms follow logical rules and can be vulnerable to some kinds of attacks. All algorithms are inherently vulnerable to brute-force attacks, in which all possible combinations of the encryption key are tried. According to Verizon's [2021 Data Breach report](#), 85% of breaches caused by hacking involve brute force or the use of lost or stolen credentials. Moreover, Cybercrime costs the U.S. economy \$100 billion a year and costs the global economy \$450 billion annually.

Nevertheless, a 128-bit encryption key establishes a secure theoretical limit against brute-force attacks, since the latter are considered to be computationally infeasible.

However, quantum computing speeds up prime number factorization, so computers with quantum computation can easily break cryptographic keys via quickly calculating and exhaustively searching secret keys. A task thought to be computationally impossible by conventional computer architectures becomes easy by compromising existing cryptographic algorithms, shortening the span of time needed to break public-key cryptography from years to hours.

In the future, even robust cryptographic algorithms will be significantly weakened by quantum computing, while others will not be secure at all.

Encryption scrambles data while in transit, making it difficult to read.

Encryption converts data from a human-readable format to a crumpled piece of information (ciphertext) to make it difficult for unauthorized parties to understand the data while it is in transit. A computer encrypts data by applying an algorithm controlled by an **encryption key** that both the sender and the receiver of an encrypted message agree upon. When the ciphertext reaches the intended receiver, it can be converted back to its original readable format using an encryption key (**decryption**).

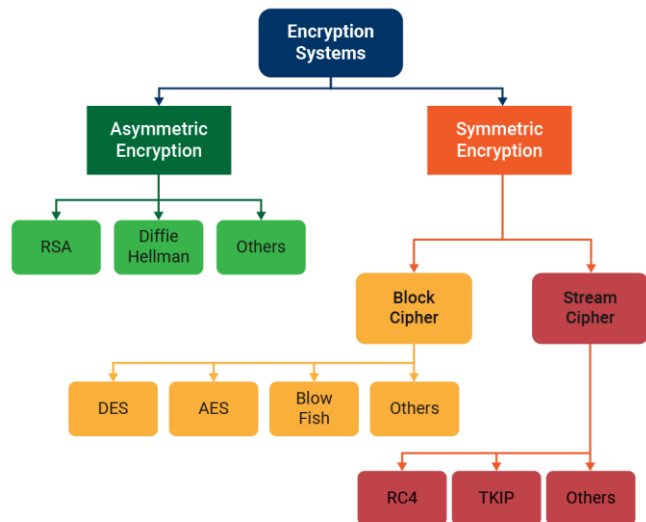


Figure: The two main types of encryption and respective algorithms

Characteristic	Symmetric encryption	Asymmetric encryption
Key used	Same key is used	One key is employed for encryption and another key is employed for decryption
Speed	Very fast	Slower
NIST recommended key length	128 bits	2048 bits
Knowledge of keys	Both parties know the key	One of the keys is known by the two parties
Usage	Encryption and decryption (confidentiality)	Encryption and decryption (confidentiality) and digital signatures (integrity and non-repudiation checks)
Main advantage	Higher operating speeds that can be used in real-time systems	More secure
Main disadvantage	Difficulty of key management	Longer key length leads to more overhead on the data packet

However, advances in quantum computing are making modern encryption more vulnerable to attacks.

Algorithms such as RSA, AES, and Blowfish remain worldwide standards in cybersecurity. The cryptographic keys of these algorithms are based mainly on two mathematical procedures — *the integer factorization problem and the discrete logarithm problem* — that make it difficult to crack the key, preserving the system's security.

However, two algorithms for quantum computers challenge current cryptography systems. Shor's algorithm is capable of solving the two mathematical problems in polynomial time, while the algorithm proposed by Grover can increase the speed of decryption keys in quadratic order.

All widely used public-key cryptographic algorithms are theoretically vulnerable to attacks based on Shor's algorithm, but the algorithm depends on operations that can only be achieved by a large-scale quantum computer (>7000 qubits). Quantum computers are thus likely to make encryption systems based on RSA and discrete logarithm assumptions (DSA, ECDSA) obsolete.

Cryptographic Algorithm	Type	Purpose	Impact from QC
AES	Symmetric key	Encryption	Secure for large keys (256 bits)
SHA-2, SHA-3	-	Hashing	Secure for large outputs (256 bits)
RSA	Public	Signatures, key establishment	No longer secure
ECDSA, ECDH	Public	Signature, key exchange	No longer secure
DSA	Public	Signature, key exchange	No longer secure

Current 128-bit and 256-bit keys are generally secure. But within the next 20 years, sufficiently large quantum computers will be able to break essentially all public-key schemes currently in use.

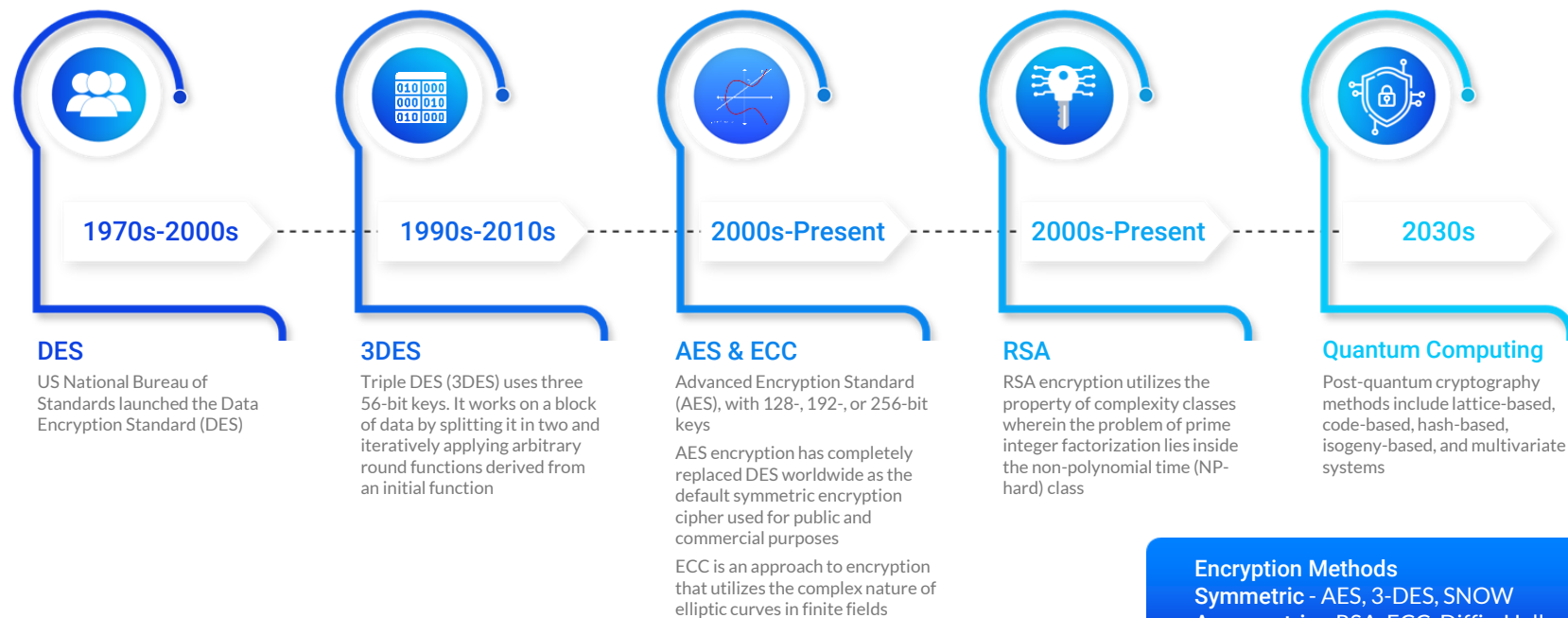
Brute-force attacks by traditional computing technologies would take time on the order of quintillions of years. And even for quantum algorithms, such attacks are still not feasible in terms of the time and energy required, given the current resources of quantum computers. For example, Grassl *et al.* calculated that the number of logical qubits required to implement an attack based on Grover's quantum algorithm ranges between around 3,000 and 7,000 logical qubits.

Why are quantum computers faster?

Quantum computers outperform conventional computers for specific problems since quantum computers leverage complex phenomena such as quantum entanglement and the probabilities associated with superpositions to perform a series of operations in such a way that favorable probabilities are enhanced. When a quantum algorithm is applied, the probability of measuring the correct answer is maximized.

THE PROSPECTS OF BUILDING LARGE-SCALE QUANTUM COMPUTERS ARE ALARMING FOR CURRENT ENCRYPTION SYSTEMS. Thus, researchers have been exploring cryptographic algorithms that run in classical computers and are resistant to quantum computing. This area of cryptography is known as post-quantum cryptography (PQC) and usually focuses on asymmetric algorithms.

Encryption beyond RSA will take another 8-10 years for quantum computing to overcome the challenges faced today.





PREPARING FOR **POST-QUANTUM CRYPTOGRAPHY**

Recent technological developments have taken QC capabilities from the realm of academic exploration to tangible commercial opportunities.

IBM



On February 4, 2021, IBM announced its roadmap for building an open quantum software ecosystem with the following targets:

- **For 2021:** The release of Qiskit runtime, which will lead to a 100x speedup in workloads that exploit iterative circuit execution. This will allow quantum systems to run jobs in just a few hours that, today, can take months.
- **By 2022:** Run a wider variety of circuits, allowing users to tackle problems previously inaccessible to any quantum processors.
- **By 2023:** Offer entire families of pre-built runtimes tailored to natural science, optimization, machine learning, and finance domains.
- **2025 and beyond:** Development of frictionless quantum computing where the hardware is no longer a concern to users or developers.

In terms of hardware developments, on Nov. 16, 2021, IBM announced its first processor to clear the 100-qubit mark with its 127-qubit processor Eagle. IBM is on schedule to develop a 1000-qubit processor by 2023.

D-Wave



D-Wave is world's first commercial supplier of quantum computers. The company uses quantum annealing that can already compete against classical computers and start addressing realistic problems. Glaxosmithkline and Volkswagen are both using D-Wave's technology in drug discovery and traffic optimization, respectively.



The global QC market is expected to grow from US\$472 million in 2021 to \$1,765 million by 2026, at a CAGR of 30.2%.

The potential threats of quantum attack capabilities range from public infrastructure to private intellectual property.

A quantum attack may cause states to gain access to sensitive information and compromise state security for governments. Or a quantum computer could allow competitors to gain access to valuable intellectual property, hijacking a drug that has been in costly development for years for pharmaceuticals, for example.

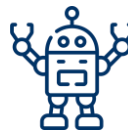
Nation-states are investing in quantum computing. In fact, countries will use systems to empower hackers as part of their increasingly popular cyber warfare and espionage activities.

Hackers are currently unlikely to have the resources to develop quantum computing systems. However, the emergence of general-purpose quantum computing will be available in the cloud as an infrastructure platform like a service, making it affordable for a wide range of users with current technological capabilities.

The public infrastructure, a set of standards, technologies, and protocols that ensure the integrity of data transmitted over the internet, are among the systems that could potentially be impacted by quantum technology.

The strength of public key infrastructure lies in its cryptographic processes that allow secure communication even over unsecured networks.

Hardware and software attacks may affect the whole system of industries such as:



Robotics



Aviation



Autonomous vehicles



Medical products such as pacemakers



While quantum computing over the cloud will give businesses the opportunity to explore potential applications, cybercriminals will leverage the technology to commit advanced data breaches around the world.

Several international organizations have been developing and standardizing post-quantum cryptography techniques.

Standardized post-quantum cryptography is expected to become available by 2030.

In 2016, the National Institute of Standards and Technology (NIST) announced a call for proposals for PQC technique evaluation and certification in terms of security and implementation performance. Some reported results and additional evaluations are available in the literature.

Other international institutions, such as the European Telecommunication Standards Institute (ETSI), the European Union Agency for Cybersecurity (ENISA), and the International Organization for Standardization (ISO) have conducted surveys and preliminary studies regarding PQC.

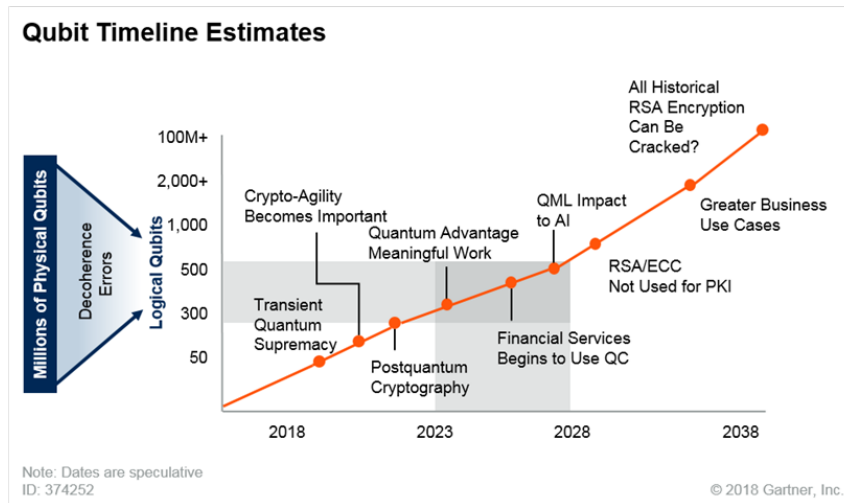


Figure: Qubit timeline estimates.

Source: [Top 10 Strategic Technology Trends for 2019-Gartner](#).

PQC standards should be addressed to attend, in a specific way, different encryption applications with their respective implementation constraints.

The replacement of encryption algorithms generally requires:

- Replacing cryptographic libraries
- Implementation of validation tools
- Deployment of hardware required by the algorithm
- Updating dependent operating systems and communications devices
- Replacing security standards and protocols

Hence, **PQC needs to be prepared for eventual threats as many years in advance as is practical**, despite quantum algorithms not currently being available to cyber attackers.

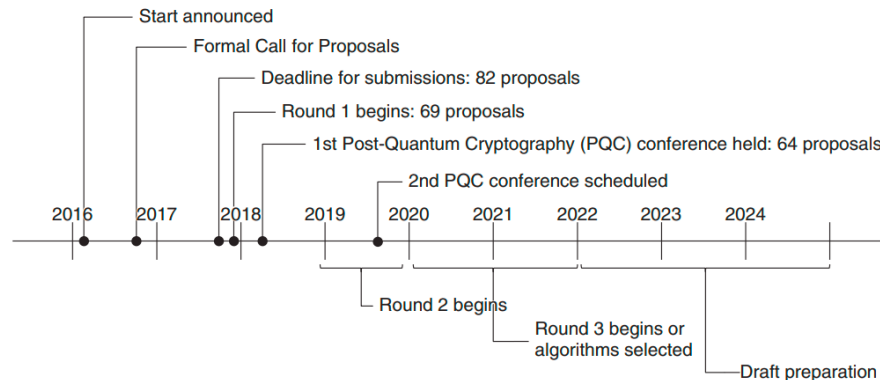


Figure: Timeline of NIST project. Source: *NTT Technical Review*, Vol. 17, No. 3, Mar. 2019

Harnessing Quantum Mechanics to Enhance Cybersecurity and Privacy

Quantum Random Number Generators

Existing encryption algorithms can be strengthened by adding genuinely random numbers. Also known as quantum keys, they are the most robust encryption keys currently available and use cosmic background energy to take advantage of the perfectly occurring randomness. Scientists measure the crackling of power in the fabric of the universe as it spontaneously creates and self-destructs. It is impossible to predict the frequency and timing of radioactive particles of cosmic origin when they hit electronic sensors, allowing quantum physicists to exploit this quantum noise and convert it into accurate random numbers.

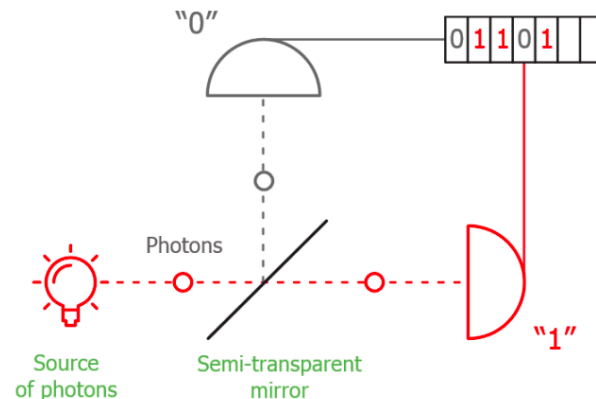


Figure: Optical system for random number generation. Source: [ID Quantique](#)

Harnessing Quantum Mechanics to Enhance Cybersecurity and Privacy

Quantum Key Distribution

Quantum key distribution is a groundbreaking technology that uses the quantum principles of superposition and entanglement. By transmitting information in quantum states, communication systems can be implemented that detect eavesdropping, making passive interference impossible.

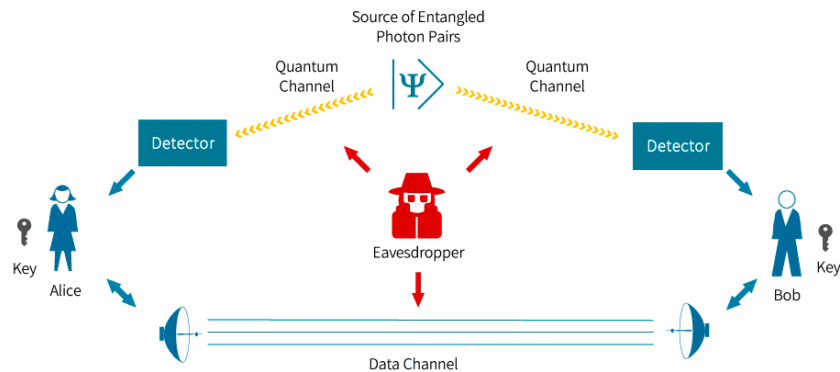


Figure: Quantum key distribution. Source: [S-Fifteen Instruments](#).

Harnessing Quantum Mechanics to Enhance Cybersecurity and Privacy

Quantum Communication Networks

Quantum communication networks use quantum key distribution technology to transmit data between two points by encoding the data on individual particles. Any attempt to hack these particles automatically disconnects, notifying the parties that an intrusion attempt has been made. Since quantum communication networks use quantum physics, information cannot be hacked as it travels between two points. The world's first integrated quantum communication network combines 700+ optical fibers on the ground with two ground-to-satellite links to achieve quantum key distribution over 4,600 kilometers across China.

Quantum machine learning

Integrating quantum computing with machine learning to better analyze vast amounts of data, such as organizational network traffic, is another method for detecting malicious intrusions. These models can be trained at very high speeds to counteract the threats posed by quantum computing.

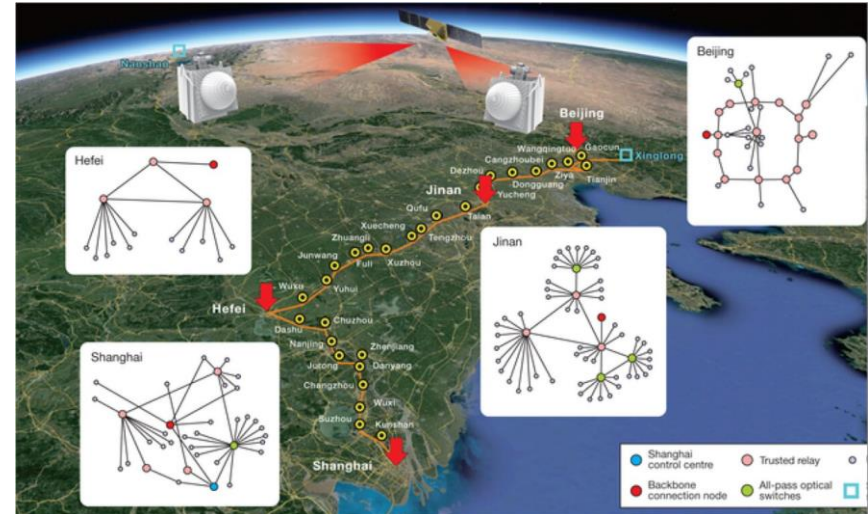


Figure: China's quantum communication network. Source: [Phys.org](https://www.phys.org)

Alternative Methods to Counter Quantum Threats

Risk Management Plans

An effective risk management program will begin with taking an inventory of affected IT assets, including hardware, software, IoT devices, and communications infrastructure and then explore and recommend alternative cybersecurity measures that cover evolving layers of defense. Some of the best practices are tokenization, quantum secure procedures, and zero-knowledge-proof systems.

White-Hat Quantum Computing Hacking

White-hat hackers will be able to protect their systems against quantum attacks in the future. With researchers, businesses, academics, and governments needing to test and identify the weaknesses in quantum computing algorithms before deploying them, a new class of quantum computing white-hat hackers can be trained to proactively find security weaknesses in new technology and fix them before they can be exploited.



Figure: The penetration testing growth rate by region. Source: [Mordor Intelligence](#).



The penetration testing market was valued at USD 580 million in 2020 and is anticipated to register a CAGR of 24.3% between 2021 and 2026.

Alternative Methods to Counter Quantum Threats

Lattice-Based Cryptography

Replacement of conventional cryptographic algorithms with lattice-based algorithms is an approach that involves hiding data inside complex math problems. These algebraic equations, which describe high-dimensional geometric structures made of a grid of dots known as a lattice, are increasingly difficult to solve as the number of dimensions increase, making it possible for cryptographers to preserve information using quantum computers. Lattice-based algorithms can plug into transport-layer security and internet key exchange protocols and protect important security protocols from quantum-based attacks. This type of encryption will prevent future quantum computing attacks by allowing users to see the data or reveal it to hackers.

One cryptosystem that utilizes this type of arbitrary computation in ciphertexts is known as fully homomorphic encryption (FHE). Some uses of FHE include analyzing and generating credit scores by a credit reporting agency without decrypting credit card data and the sharing of medical records among healthcare professionals without disclosing a patient's identity.

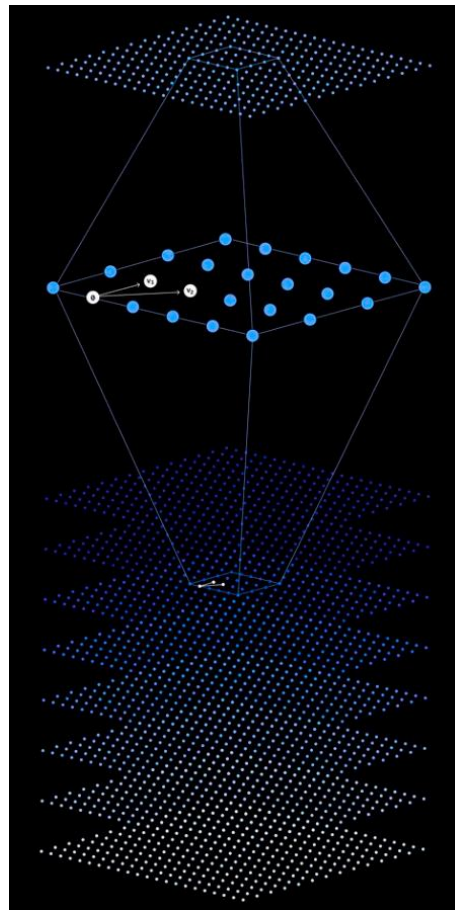


Figure: Lattice-based cryptography.
Source: [Flickr user IBM Research](#)

Alternative Methods to Counter Quantum Threats

Using a System of Propagating Radio Waves

Mixed and coherent attacks emanating from quantum computers are hypothetically capable of maliciously entangling a targeted device. Creating a defense system to mitigate such potential threats, using a procedure that emits radio waves to force constant discord around a defended network, can shield against malicious targeting attempts. Applications of ultraviolet light as a defense against quantum attacks rely on the electromagnetic character of ultraviolet light. Although ultraviolet light is unable to ionize an atom, there are properties of radio waves that are able to couple with conductors if the radio waves are at a distance that is within the propagation of the wave. Therefore, the exchange of radio waves with ultraviolet light can change the hardware.

Given that classical computers operate using quantum mechanics yet fall into the limitations of classical systems, it's clear that quantum computing can influence classical techniques, according to research led by Toshiba and its Cambridge subsidiaries. The level of threat this finding reveals, in conjunction with the race to build quantum communications emitted from satellites, provide support for the rationale behind using electromagnetic waves for computer network defense. Given that Earth's magnetic field blocks quantum communication, their conceptualization of energy excitation using radio waves to create a shield seems plausible.

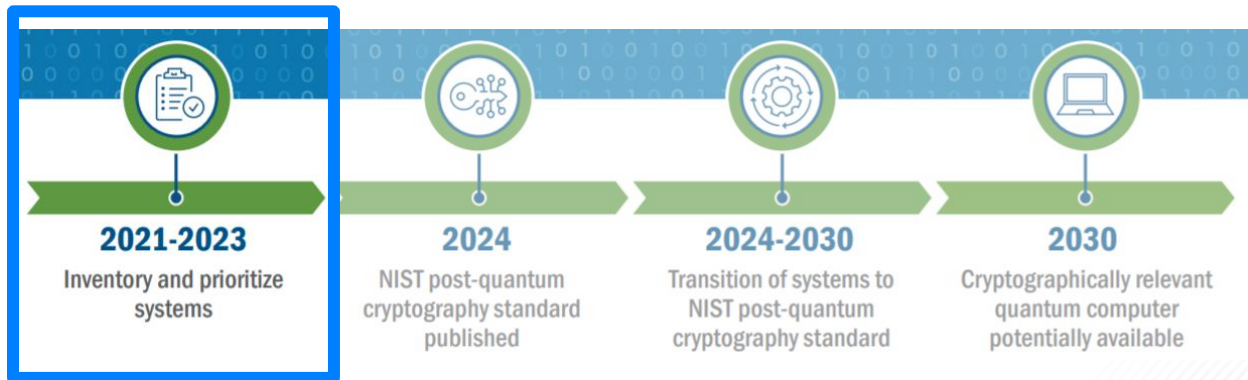
Establishing leadership in quantum cybersecurity

In January 2022, the Biden administration released National Security Memorandum 8, pushing the US government's cybersecurity infrastructure into the post-quantum era. The memorandum ordered the NSA to begin updating the Commercial National Security Algorithm Suite (CNSA), the set of secure algorithms that are government approved for use by all encrypted data users, whether in the public or private sector, to include quantum-resistant cryptography. It marked the first step in addressing the threat of quantum computing to the nation's national security apparatus and signaled that the US government recognizes the need to take a leadership role in setting standards and working to secure the cyber future.

As the Quantum Alliance Initiative has been urging since its founding in 2018, it will take an all-of-government approach, in addition to working with global allies as well as with the private sector, to achieve quantum readiness, since today's interconnected infrastructures are only as strong as the weakest link.

In the meantime, companies need not to wait for the federal bureaucracy to respond to this call to action, as companies like those profiled in the next section are already providing customers with PQC cybersecurity solutions that can protect users from current cyber threats and from future quantum threats.

Preparing for Post-Quantum Cryptography



Source: www.dhs.gov



COMPANIES OFFERING **PQC CYBERSECURITY**

QuSecure - Quantum random number generation





Company Overview:

Using their patent-pending Quantum Transport Layer Security (QTLS), QuSecure offers a software-based solution to protect user data.

With a focus on post-quantum encryption key and policy management, QuSecure offers enterprise-wide encryption solutions that add quantum random number generation (QRNG) that outputs truly random numbers. Combined with next-generation cryptographic algorithms, key management forms the basis of their suite of cybersecurity products.

AT A GLANCE



 www.qusecure.com
 dave@qusecure.com
 Menlo Park, California, US
 10-50 Employees
 2019

SUMMARY



Technology type / security type

Quantum random number generation



What makes it unique

Scalable cybersecurity for the post-quantum enterprise



Technology maturity (TRL)

7



Application / Industry

Cybersecurity

QuSecure - Quantum random number generation

Technology Details:

- Interoperable within the existing public key infrastructure
- Software-based and plugs into existing enterprise infrastructures
- Reduction of complexity, while increasing efficacy of security and performance
- Designed to work in combination with QRNG for genuinely random keys
- Supports multi-factor authentication
- Future resiliency for the upcoming FIPS 140-3 standards

The technology generates up to 60,000 keys per second, which is faster than TLS 1.2 and 1.3 and reduces the handshake time by approximately half as compared to TLS 1.3 implementation.

Partnerships:

QuSecure has raised a total of \$3.5M in funding over 7 rounds. Their latest funding was raised on Jun 10, 2021 from a Seed round. QuSecure is funded by 4 investors. Techstars Space Accelerator and Techstars are the most recent investors.

References:

1. <https://www.qusecure.com/quantum-key-management-with-entropy>
2. <https://www.businesswire.com/news/home/20210818005084/en/QuSecure-Named-as-1-of-the-Top-28-Cybersecurity-Firms-of-2021-by-CB-Insights>
3. https://www.crunchbase.com/organization/qusecure/company_financials

IBM - Quantum Computing as a Service

Company Overview:

IBM provides quantum computing solutions via systems, software, and cloud services. The IBM Quantum System One is claimed to be one the world's first integrated product offering quantum computers.

With a quantum volume of 32, IBM Quantum System One has 27 qubit Falcon processors. **The system can be upgraded to 65 qubit Hummingbird processor and 127 qubit Eagle processor, which will be available in late 2023.**

In North America, Germany, and Japan, IBM's quantum system one has been deployed. IBM helped Exxonmobil ship LNG more efficiently. IBM researchers made a way to track inventory on quantum devices that could be used on ships. It analyzes the strengths, disadvantages of different strategies for inventory and fleet routing.

AT A GLANCE



	www.ibm.com
	1-866-880-2765
	Armonk, NY, US
	500+ Employees
	1901

SUMMARY



Technology type / security type
Quantum Computing as a Service



What makes it unique
Market Leader in Quantum Computing, Largest Quantum computing capacity (127 Qbits)



Technology maturity (TRL)
8



Application / Industry
Logistics, Integrated Quantum computing, Oil and Gas, Finance, Cryptography, Artificial Intelligence

IBM - Quantum Computing as a Service

Technology Details:

IBM claims Quantum System One to be one of the most advanced cloud-based quantum computing platforms available. It has the following features:

- The Quantum systems hardware is designed for stability, and is auto calibrated to provide predictable and repeatable performance from high-quality qubits.
- The installed Cryogenic systems provide cold temperatures and consistency, helping in isolating the quantum system.
- Quantum firmware enables system upgrades without downtime for users and ensures to manage the system health. It ensures secure cloud access and execution of quantum algorithms.

IBM offers quantum services and cloud programming tools for accelerating research. These tools help researchers in drawing circuits, running experiments more efficiently, and coding algorithms.

Partnerships:

IBM is developing quantum computer solution that finds wide range of applications in finance, oil and gas to support field efficient inventory and route management operations, developing large scale carbon capture, and identification of new catalysts/active materials for low energy processing. The quantum computers also offers solutions for other application areas as well.

References:

1. <https://www.ibm.com/quantum-computing/>
2. <https://research.ibm.com/quantum-computing>

PQShield - Post-quantum cryptography

Company Overview:

PQShield is a post-quantum pioneer and participant in NIST's post-quantum cryptography standardization process. They have a deep understanding of the algorithms' computational and mathematical requirements, which has led to significant architectural and design innovations in hardware implementations.

PQShield helps customers transition their product lines from legacy RSA and elliptic curve cryptography to quantum-secure standards by offering ready-made and tailored IPs for secure elements, IoT firmware, public key infrastructure, mobile and server technologies, and end-user applications.

AT A GLANCE



	https://pqshield.com/
	Contact@pqshield.com
	Oxford, Oxfordshire, UK
	11-50 Employees
	2018

SUMMARY



Technology type / security type

Post-quantum cryptography



What makes it unique

It has a library of post-quantum cryptographic primitives



Technology maturity (TRL)

7



Application / Industry

Cybersecurity

PQShield - Post-quantum cryptography

Technology Details:

PQSLib is a library of post-quantum cryptographic primitives that can utilize a hardware blocks' computational features. The implementations match current NIST post-quantum standardization versions for digital signatures, key establishment, and encryption. These algorithms can be used to replace or complement legacy cryptography.

PQSDK Crypto Core helps organizations migrate to modern and crypto-agile solutions that are quantum resistant. It is a proprietary software library that implements NIST-standard cryptographic primitives and exposes them via common APIs and that can be used at each stage of the migration process.

The API is designed to be flexible and easy to use, allowing for rapid experimentation. Interfaces allow the interaction with classical, post-quantum, or a combination of both. The code is designed to achieve the best possible performance by leveraging the capabilities provided by the x86-64 and ARMv8 architectures.

References:

1. <https://www.prnewswire.com/news-releases/pqshield-and-kudelski-security-partner-to-address-quantum-threat-301386975.html>
2. <https://pqshield.com/partners/>
3. <https://www.crunchbase.com/organization/pqshield>
4. <https://www.microsemi.com/product-directory/mi-v-partners/5634-pqshield>

Out-of-box algorithm support: XMSS, KYBER, NTRU, SABER, Classic McEliece, SIKE, FrodoKEM, DILITHIUM, FALCON, RAINBOW, SPHINCS+

Partnerships:

PQShield and Kudelski Security have partnered to address quantum threats. Kudelski Security launched its quantum security practice in December 2020 in recognition of the threat quantum technology will raise in the future. In addition, PQShield raised \$7M for quantum-ready cryptographic security solutions.

PQShield has ported the entire PQSLIB3 algorithm suite on Microchip's PolarFire SoC FPGA. High-level functions and API calls run on the PolarFire SoC FPGA's hardened RISC-V cores, while specific cryptographic tasks can be offloaded to the FPGA fabric as required by low-latency or high-throughput applications.

TOSHIBA Quantum Security - Quantum key distribution






Company Overview:

The company said it has teamed up with Verizon Communications Inc VZ.N in the United States and BT Group BT.L in Britain in pilot QKD projects. Toshiba developed world's first QKD system based on quantum transmitter, receiver and random number generator chips. QKD addresses the demand for cryptography that will remain secure from attack by the supercomputers of tomorrow.

Toshiba has developed the first complete QKD prototype in which quantum photonic chips of different functionality are deployed. Random bits for preparing and measuring the qubits are produced in quantum random number generator chips and converted in real-time into high-speed modulation patterns for the chip-based QKD transmitter (QTx) and receiver (QRx) using field-programmable gate arrays (FPGAs). Photons are detected using fast-gated single-photon detectors. Sifting, photon statistics evaluation, time synchronization and phase stabilization are done via a 10 Gb/s optical link between the FPGA cores, enabling autonomous operation over extended periods of time. As part of the demonstration, the chip QKD system was interfaced with a commercial encryptor, allowing secure data transfer with a bit rate of up to 100 Gb/s.

AT A GLANCE

TOSHIBA

 Link
 +81334572096
 Tokyo, Japan
 10000+ Employees
 1875

SUMMARY



Technology type / security type

Quantum key distribution



What makes it unique

Toshiba has developed the first complete QKD prototype in which quantum photonic chips of different functionality are deployed.



Technology maturity (TRL)

7



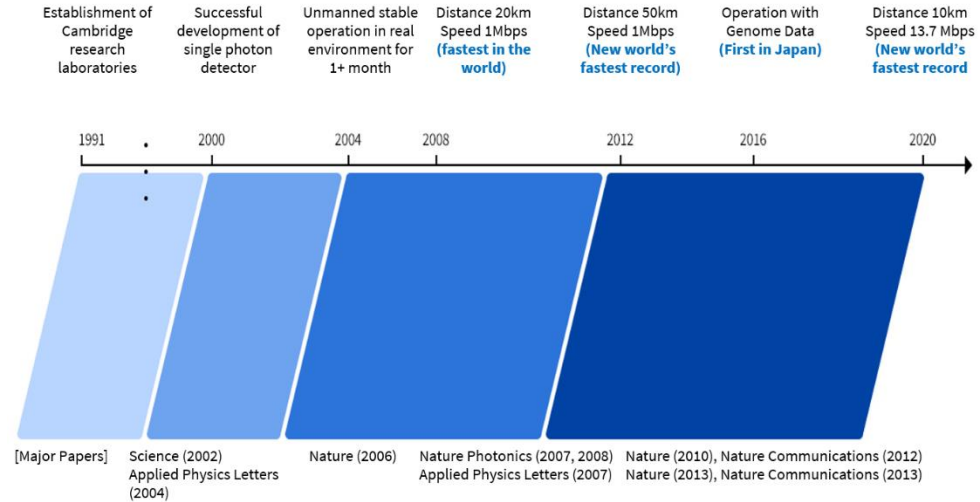
Application / Industry

Cybersecurity / Software

TOSHIBA Quantum Security - Quantum key distribution

Technology Details:

With the multiplexing capability built into Toshiba's system, the control channel and the quantum channel can be transmitted over one fiber without reducing transmission distances of the keys.



TOSHIBA Quantum Security - Quantum key distribution

Partnerships:

Outside of Japan, Toshiba Europe Ltd., in collaboration with BT Group Plc., has enabled the UK's first industrial deployment of a quantum-secure network between two industry-leading organizations and began joint verification from September 16, 2020. In the US, Toshiba has participated in the recent QKD demonstration by Verizon Communications Inc. in alliance with Quantum Xchange., announced by Verizon on September 3. From FY2021, the company will collaborate with regional business partners not only in the UK and the US, but also in Europe and Asia to promote the QKD system integration businesses worldwide.

QuantumXchange & Toshiba: Toshiba has developed a prototype QKD system that transmits secure optical keys for cryptographic operations on fiber-optic networks. When they tested their system on QuantumXchange's operational network on the East coast, the test reaffirmed the viability of the connection between the financial markets on Wall Street with offices in New Jersey.

References:

1. <https://www.businesswire.com/news/home/20211021005160/en/Toshiba-Shrinks-Quantum-Key-Distribution-Technology-to-a-Semiconductor-Chip>
2. <https://www.toshiba.co.jp/qkd/en/cases.htm>
3. <https://quantumxc.com/blog/quantum-xchange-and-toshiba-working-together-to-make-qkd-a-commercial-reality/>

ID Quantique (IDQ) - Quantum random number generation





Company Overview:

ID Quantique (IDQ) is a world leader in quantum-safe crypto solutions designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation, and quantum key distribution solutions and services to the financial industry, enterprises, and government organizations globally

IDQ also commercializes a quantum random number generator that are being used in the security, simulation, and gaming industries.

AT A GLANCE



 <https://www.idquantique.com/>
 info@idquantique.com
 Geneva, Switzerland
 11-50 Employees
 2001

SUMMARY



Technology type / security type

Quantum random number generation



What makes it unique

High performance PCIe quantum random number generator with embedded NIST-compliant post-processing



Technology maturity (TRL)

7



Application / Industry

Cybersecurity / Financials

ID Quantique (IDQ) - Quantum random number generation

Technology Details:

Various applications of QRNG includes cryptographic key generation, user and device authentication, random seeding, code signing, token generation, gaming / random drawings, numerical simulations, and statistical research.

Quantis exploit elementary quantum optic processes that are fundamentally probabilistic to produce true randomness. As the quantum processes underlying the QRNG are well understood and characterized, their inner working can be clearly modeled and controlled.

Quantis QRNGs embed elementary components that can be easily monitored to detect any failure or attacks.

Partnerships:

SK Telecom, Octacto and ID Quantique unveil the world's first fingerprint recognition security key equipped with a quantum random number generator

References

1. <https://www.dhs.gov/quantum>
2. <https://docs.aws.amazon.com/crypto/latest/userguide/concepts-algorithms.html>
3. <https://my.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf>
4. <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>
5. <https://www.britannica.com/topic/RSA-encryption>
6. <https://www.datacenterknowledge.com/data-center-world/what-has-happen-quantum-computing-hit-mainstream>
7. <https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=2655af4c7d3f>
8. <https://www.cloudflare.com/learning/security/threats/on-path-attack/>
9. <https://www.simplilearn.com/what-is-des-article>
10. <https://www.sciencedirect.com/science/article/pii/S2090123215000752>
11. <https://royalsocietypublishing.org/doi/10.1098/rsta.2019.0061>
12. <https://www.ibm.com/blogs/research/2021/02/quantum-development-roadmap/>
13. <https://arstechnica.com/science/2021/11/ibm-clears-the-100-qubit-mark-with-its-new-processor/>
14. <https://www.dwavesys.com/quantum-computing>
15. <https://www.ibm.com/topics/quantum-computing>
16. <https://www.nature.com/articles/463441a>
17. <https://www.theverge.com/circuitbreaker/2017/1/25/14390182/d-wave-q2000-quantum-computer-price-release-date>
18. <https://www.spinq.cn/products/geminiMini-anchor>
19. <https://arxiv.org/pdf/1512.04965v1.pdf>
20. <https://arxiv.org/pdf/quant-ph/0301141v2.pdf>
21. <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>
22. <https://www.etsi.org/newsroom/news/1981-2021-10-etsi-releases-two-technical-reports-to-support-us-nist-standards-for-post-quantum-cryptography>
23. <https://ieeexplore.ieee.org/document/7086640>
24. http://www.ijirset.com/upload/2015/march/43_A_COMPARATIVE.pdf
25. <https://www.semanticscholar.org/paper/Systematic-literature-review%3A-comparison-study-of-Santoso-Rilvani/a39b9e700736cf86e8b1b63141523f2d2ed3b9dd>
26. <https://www.hudson.org/research/17490-the-biden-white-house-gets-quantum-right-at-last>
27. https://www.researchgate.net/publication/323369289_Development_of_Advanced_Encryption_Standard_AES_Cryptography_Algorithm_for_Wi-Fi_Security_Protocol
28. https://www.researchgate.net/publication/283176041_A_Review_and_Comparative_Analysis_of_Various_Encryption_Algorithms
29. <https://www.encryptionconsulting.com/wp-content/uploads/2020/04/2020-Global-Encryption-Trends-Study.pdf>
30. http://article.nadiapub.com/IJSIA/vol9_no4/27.pdf
31. <https://ieeexplore.ieee.org/document/8787164>
32. <http://eprint.iacr.org/2015/1075>
33. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201903fa4.html>
34. <https://www.okta.com/blog/2019/07/the-impact-of-quantum-computing-on-cybersecurity/>
35. <https://cisomag.eccouncil.org/quantum-computing/>
36. <https://www.idquantique.com/quantum-safe-security/quantum-computing/cybersecurity-implications/>
37. <https://www.hudson.org/research/14484-quantum-computing-how-to-address-the-national-security-risk>
38. <https://www.technologyreview.com/2018/01/30/3454/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/>
39. <https://builtin.com/cybersecurity/how-neutralize-quantum-security-threats>
40. <https://www.internetsociety.org/resources/doc/2020/does-quantum-computing-put-our-digital-security-at-risk/>
41. <https://arxiv.org/abs/1610.01734>
42. <https://techbeacon.com/security/quantum-computing-end-security-we-know-it>

About the authors



Sofiane Boukhalfa, PhD

Technical Director

Sofiane leads the high-tech, aerospace & defense, and automotive & logistics practices at PreScouter. For nearly a decade, he has worked with hundreds of F500 and G1000 clients across multiple industries, through which he has developed an expertise in key emerging technologies (such as 5G, IoT, AI/ML, blockchain, energy storage and generation, quantum sensing, and others) and a strong understanding of the associated business ecosystem and drivers pushing these sectors forward (e.g., key players and trends, roadblocks to commercialization, etc.). Sofiane's strategic insights have ranged from technical due diligence for acquisition targets to identifying relevant markets for newly developed products based on emerging technologies and assessing market penetration strategies. Sofiane holds a PhD in Materials Science and Engineering from the Georgia Institute of Technology, where his research focused on nanotechnology and energy storage.



Gursimran Singh Sethi

Co-Founder and Technical Lead, LATYS Intelligence

Gursimran Singh is the Co-Founder and Technical Lead of Montreal-based startup LATYS Intelligence, which develops novel reconfigurable metasurfaces for IoT and 5G applications. Gursimran earned his BEng (Hons) degree from the Hong Kong University of Science and Technology and his MASc degree from the University of Toronto in 2019.

His research has been focused on developing novel microwave and mm-wave antennas for Satellite, IoT and 5G applications. He has held prestigious research and work positions at Princeton University and Apple and has been a recipient of multiple Canadian awards and international grants by the Antennas and Propagation Society of the IEEE.

Gursimran is an active member of the IEEE, and regularly contributes to academic conferences and journal articles pertaining to next-generation reconfigurable antennas. Gursimran has also filed for two US patents with General Electric and Thales Alenia Space for his work in the area of reconfigurable antennas.

About the authors



Nayher Vallejo

Researcher

Nayher is a Chemical Engineer and Dsc Candidate with demonstrated research expertise in nonlinear dynamics, machine learning, and fault detection and diagnosis. He has rich experience in modeling and computer simulation, using several programming languages like Python, MatLab, Fortran, C/C++, and Julia. Nayher has worked on research projects in the oil & gas industry related to TI applications, online monitoring process, and automatic control. He is a motivated team player with the ability to problem-solve under challenging circumstances.



Hakan Basargan

Researcher

Hakan Basargan received the B.Sc. degrees from the Sakarya University Mechatronics Engineering and Electrical-Electronics Engineering in the same university in 2016. He completed his M.Sc. degree from the Budapest University of Technology and Economics, Budapest, Hungary, in 2018, where he is currently pursuing a Ph.D. degree with the Department of Control for Transportation and Vehicle Systems. His research has involved controlling the vertical and longitudinal dynamics of autonomous vehicles and steer-by-wire control.

Other Reports from PreScouter that You Might Like



Overcoming Semiconductor
Processing Challenges



Quantum computing in the
chemical industry



The 48V Shift in EVs & Data
Centers: Unlocking More Power
With Lower Emissions

Engage our network of experts and researchers on your topic.

[CONTACT US HERE](#)

Potential Next Steps

- ✓ PreScouter can look for more companies developing technological solutions for quantum-based cryptography
- ✓ PreScouter can conduct anonymous interviews with vendors, experts and research groups
- ✓ PreScouter can organize direct consultations between you and Subject Matter Experts (SMEs) in the space



TECHNOLOGY
LANDSCAPING



TRENDS
MAPPING



TECHNOLOGY
ROAD MAPPING



INTERVIEWING
STARTUPS



IP
LANDSCAPING



SUPPLIER
OVERVIEWS



COMPETITIVE
INTELLIGENCE



MARKET
ANALYSIS



PARTNER
OVERVIEWS



TECHNO-ECONOMIC
ANALYSIS

About PreScouter

PRESCOUTER PROVIDES CUSTOMIZED RESEARCH AND ANALYSIS

PreScouter helps clients gain competitive advantage by providing customized global research. We act as an extension to your in-house research and business data teams in order to provide you with a holistic view of trends, technologies, and markets.

Our model leverages a network of 4,000+ advanced degree researchers, industrial experts, engineers and analysts across the globe to tap into information from small businesses, national labs, markets, universities, patents, startups, and entrepreneurs.

CLIENTS RELY ON US FOR:



Innovation Discovery: PreScouter provides clients with a constant flow of high-value opportunities and ideas by keeping you up to date on new and emerging technologies and businesses.



Privileged Information: PreScouter interviews innovators to uncover emerging trends and non-public information.



Customized Insights: PreScouter finds and makes sense of technology and market information in order to help you make informed decisions.

