Are you ready for the Quantum Cyber Shift?

EY Quantum Computing Lab
Global Innovation
April 23

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

Quantum technology will disrupt the way we treat data and handle cybersecurity

Quantum technology is finding its way out of research labs and into commercial applications. Data and computational needs are growing exponentially, frequently overwhelming binary computer systems. According to Moore's Law, the number of transistors on integrated circuits doubles approximately every two years, but capacity has been continually outpaced by the growth rate of data output.

Quantum computers (QCs) may offer superior computational power due to quantum parallelism. With the use of qubits (the computational units of QCs), quantum computers may have an exponential computational advantage compared to classical computers in a stable environment. A milestone in quantum computing development was reached in 2019 when quantum supremacy was proclaimed, proving QCs' capability of solving previously unsolvable problems for classical systems and paving the way for enhanced desirability in quantum technology investments.

The development of fundamentally new kinds of computer system architectures, communication networks, software and digital infrastructure has already started. The progression of quantum computing power and stability is completely disrupting the way we address cryptography, intensifying existing risks and giving rise to new threats, especially regarding the trustworthiness of cryptographic algorithms.

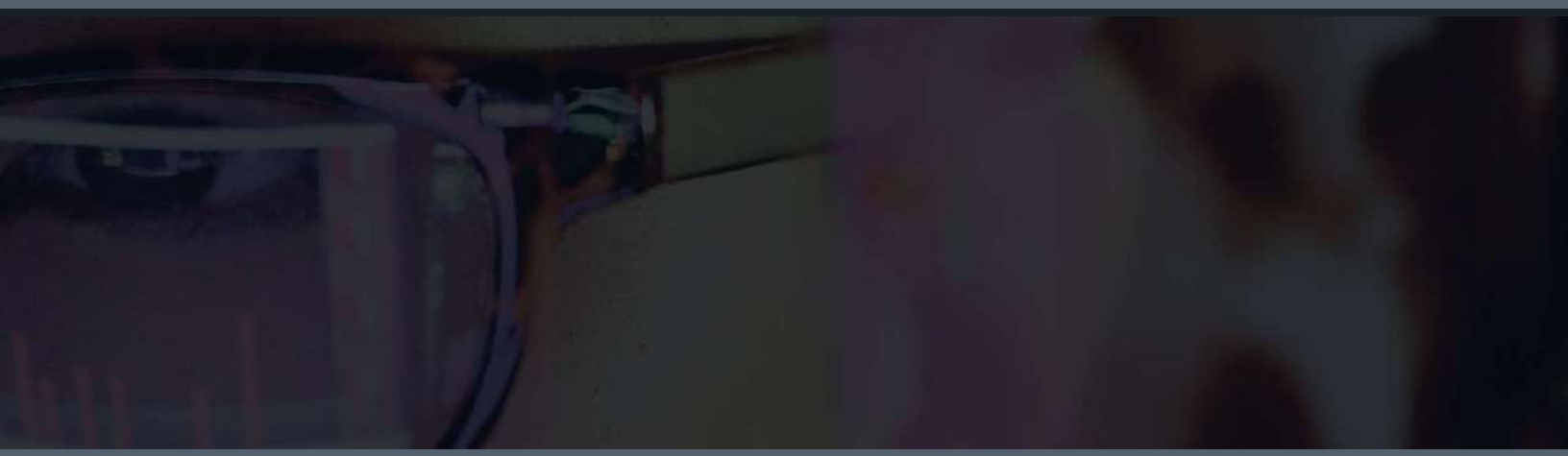
Recent conventional threats, attacks and incidences of data theft have shown how susceptible and sensitive our current approach to data security is without the inclusion of quantum technology. Various cryptographic ciphers may inevitably become obsolete and hackable with the assistance of quantum systems, including many that already have a proven technological framework. Some experts believe that major changes in enterprise business models are not far away, with only a five-year gap left until quantum computing is embraced by leading enterprises. Changes in today's enterprise architecture and cybersecurity infrastructure remain inevitable and should be addressed now.

The following paper introduces the effects of quantum technologies to specialists on the cyber industry, with a focus on securing data. A time analysis for expected development and changes, in addition to specifications on cybersecurity products and regulatory responses, is provided. In conclusion, we will offer solutions to assist in navigating the disruptive changes of the quantum era.

“

Once a new technology rolls over you, if you’re not part of the steamroller, you’re part of the road.

Stewart Brand, *writer and founder of The WELL and Global Business Network*.



Readiness assessment of a Quantum future business model

Assessment of quantum readiness in your cybersecurity business landscape:

- How well prepared do you view your cybersecurity business landscape to be?
- Do you have a full awareness of the risks and threats posed by these technologies?
- Do you have a well-prepared, quantum-guided business model at hand, ready for implementation?

How many answers to the questions did you answer in the affirmative?

0–2

Should explore quantum-related cybersecurity opportunities further

3–4

Aware of some threats and opportunities, but unsure how to address them

5

Quantum expert

Has awareness and business model for the quantum era

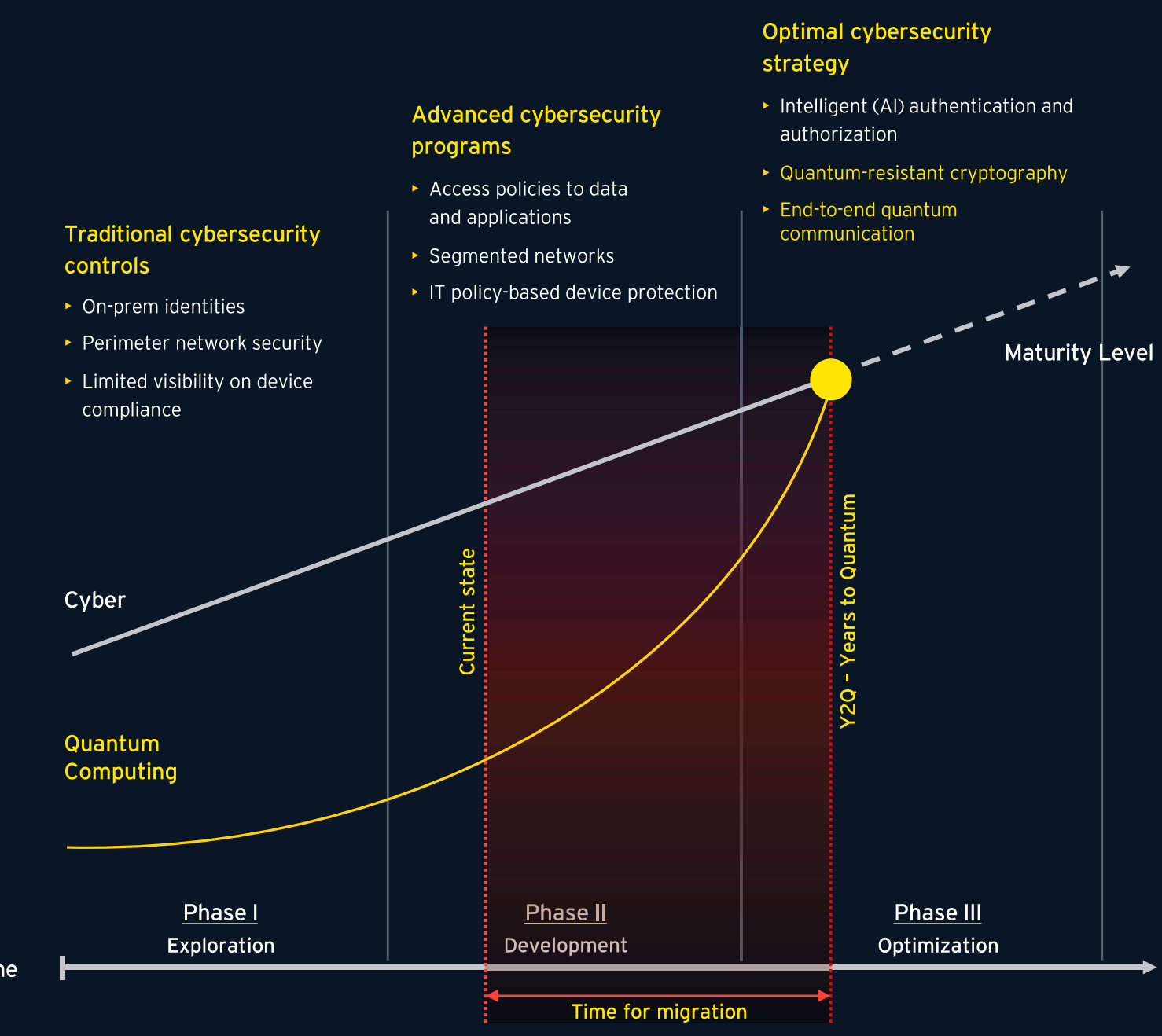
The Cybersecurity Timeline considering future developments in quantum technologies

Universal solutions will take some time to evolve; an impending paradigm shift calls for action today.

Quantum computing technologies are moving toward commercialization as firms and researchers collaborate to develop new tools and solve real-life problems. Quantum computing threatens to render current cryptographic protocols obsolete, forcing the scientific society to research new cryptographic algorithms and security products that are resistant against quantum attacks.

While these new algorithms will allow businesses to increase their level of security with the inclusion of quantum-resistant cryptography, the security level will also depend on the level of cybersecurity maturity and controls currently in place within the business and the progression of technology in tandem with regulation.

In order to keep operating successfully and securely, businesses will need to ensure that quantum-resistant cybersecurity matures before the threat posed by quantum computing technologies.



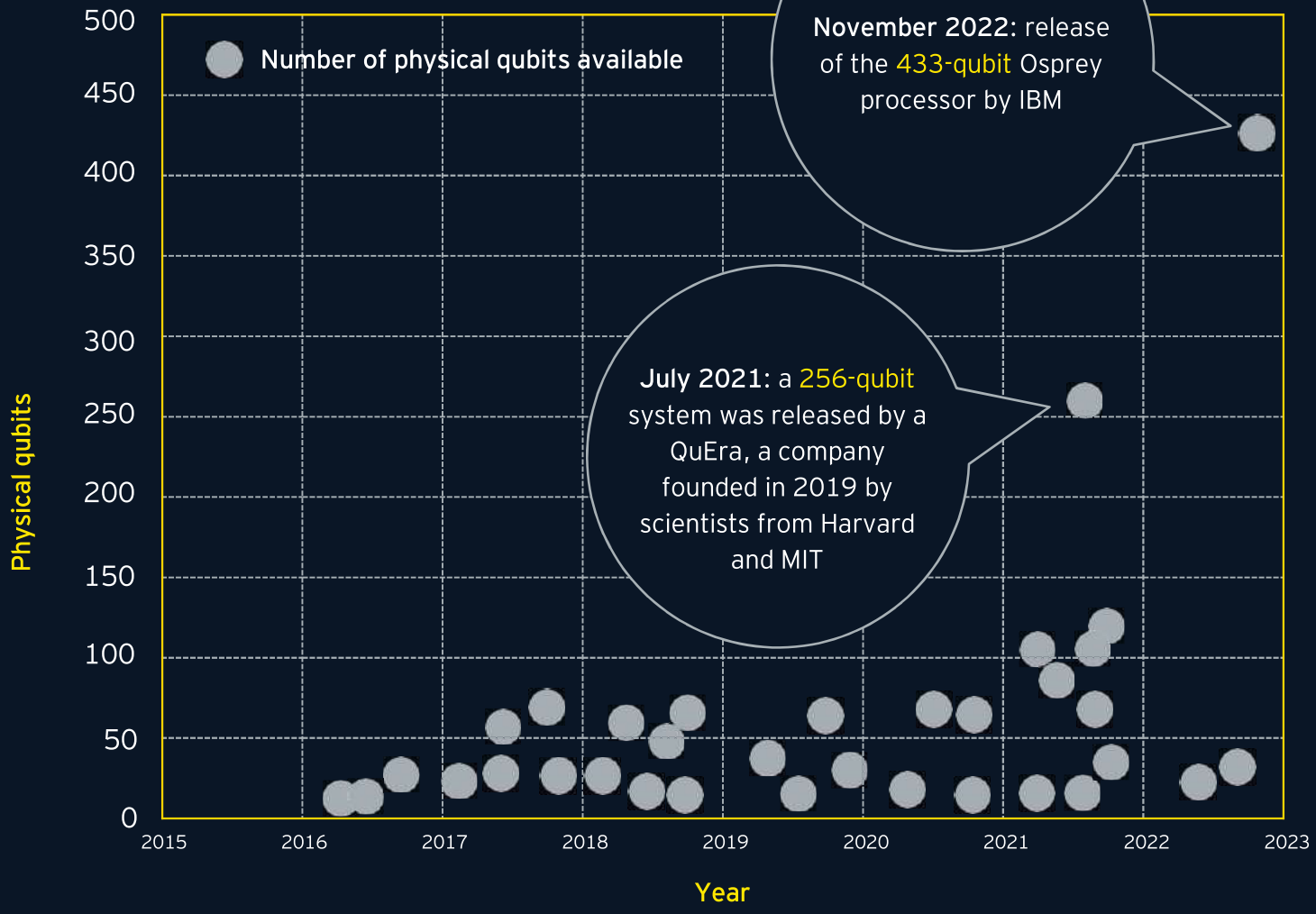
Source: EYQ, Forrester – Emerging Technology Spotlight: Quantum Computing – A First Look At Quantum Computing.

Evolution of Quantum Computing systems to commercialization

Diving deeper into the evolution of higher performance and stability in quantum computing systems to date, the graph to the right shows a selection of the currently available quantum systems with the respective number of qubits by a selected group of firms, including IBM, Google, Intel, Rigetti and QuEra. While qubit count is not the only metric that should be considered when comparing different quantum processors -qubit quality and connectivity are examples of other properties to look for-, it offers a good starting point. As presented in the graph, there has been a significant growth over the last few years.

Further acceleration in growth is forecasted by the vendors in the number of qubits available in upcoming quantum systems. IBM, for example, released its Osprey system with 433 qubits in November 2022, intends to release the Condor system with 1,121 qubits by 2023, and a 1,000,000-qubit machine by 2030.

The players in the quantum hardware developer space are increasing their expertise steadily, along with the amount of funding invested around the globe, which makes achieving the above-mentioned milestone by the end of the decade more likely. For example, PsiQuantum, a company focusing on building a large-scale, general-purpose silicon photonic quantum computer with at least 1 million physical qubits, has raised $665m since its foundation in 2016, from which $450m were raised in 2021 alone.



https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/.

An approach to Modern Cryptography with quantum computing

Modern cryptography has become more complex and is increasingly exposed to serious threats from new technologies and approaches. Quantum computing offers both an opportunity and a threat to modern cryptography that demand attention.

Currently, the power of cryptographic algorithms is based on computational mathematical complexity. For example, the use of asymmetric ciphers to solve security algorithms is not impossible but using traditional computing systems requires an abundance of time, and there currently are no solutions available other than the use of asymmetric ciphers.

Quantum computers, due to their computational advantage, will need only a tiny fraction of time required by traditional systems. Breaking a 2048-bit RSA (Rivest-Shamir-Adleman) encryption, in theory, would take between 10,000 and 100,000 years with a traditional computer system, whereas a quantum computer can break this key in less than 8 hours once machines with ~20,000,000 physical (noisy) qubits are available[1]. Furthermore, a recent article claims to be able to break that encryption with 372 physical qubits and a hybrid algorithm[2]. As previously mentioned, IBM Quantum announced a 433-qubit system to be launched in late 2022 and a system with 1,121 physical qubits is expected for 2023, as stated in their quantum hardware roadmap. QuEra, a company founded by researchers from Harvard and MIT, constructed a system with 256 physical qubits.

With the introduction of at least 100 stable logical (error corrected) qubit systems, the computational power for certain problems is expected to reach calculation powers greater than currently available.

[1] Gidney, C. (2019, May 23rd). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.
[2] Bao Yan (2022, Dec 23rd). Factoring integers with sublinear resources on a superconducting quantum processor.

Many current cryptography protocols need to be reworked due to this progress. Offering data confidentiality, as well as authentication assurance, alongside supporting non-repudiation and message integrity is a must. We have outlined some cryptographic methods that are currently in place and their implications for quantum computing.

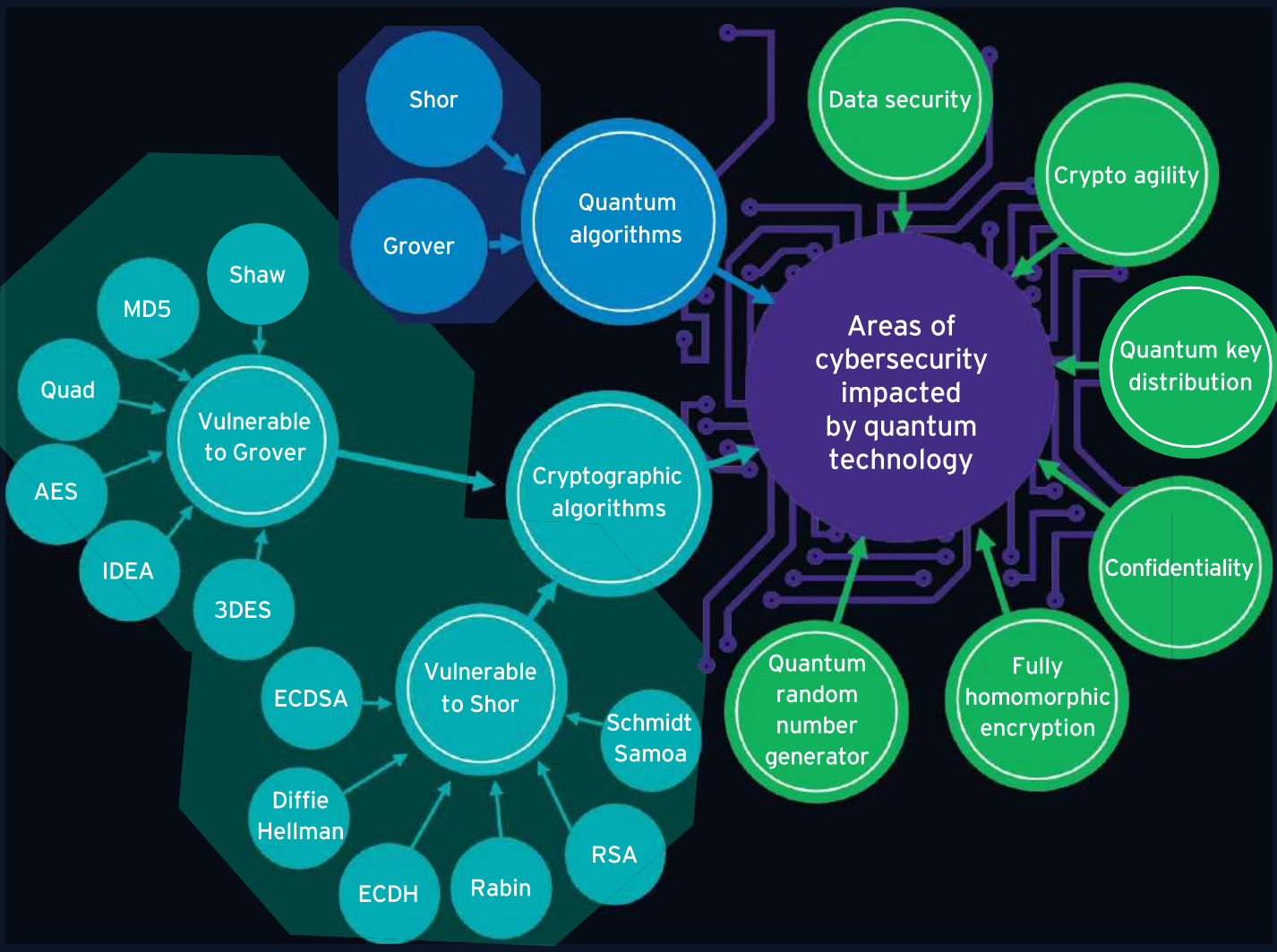
Public key cryptography (PKC), also known as asymmetric cryptography, enables encrypted communication without prior key exchange. It is often applied to securely sent keys that can then be used for symmetric cryptographic protocols. The protocols implementing RSA rely on multiplying two prime numbers, for which no efficient algorithms have yet been discovered to reverse the calculation. The risks resulting from quantum computing stem from Shor's algorithm, which can also be applied to other algorithms such as Diffie-Hellman, or forms of cryptography based on elliptic curves. Other "one-way functions" such as hash functions can also be threatened, by other quantum algorithms such as Grover's. However, lattice-based systems are considered quantum-resistant and offer opportunities.

RSA (Rivest-Shamir-Adleman) is a public key cryptosystem, which relies on the difficulty of prime factorization, as it uses the product of two large prime numbers. While multiplying large prime numbers can be done in milliseconds, factoring the resulting product to find the initial prime numbers is considered highly difficult for traditional computer systems. Intractability is achieved through mathematical complexity and insufficient computational power in traditional machines. For a traditional 2.2 GHz Opteron CPU, which represents a standard benchmark for traditional machines, a time of 10^145 years is required to factor a 1,024-bit number (7.25×10^{135} times the age of the universe). With the development of quantum computing, factorizing RSA could happen within seconds.

Mapping areas of cybersecurity impacted by quantum technology

The following map provides a visual overview of areas impacted by QC in cybersecurity, including a legend of risk areas with respect to the above-outlined cryptographic algorithms. Additionally, two examples of quantum algorithms and threats due to their evolvement have also been presented:

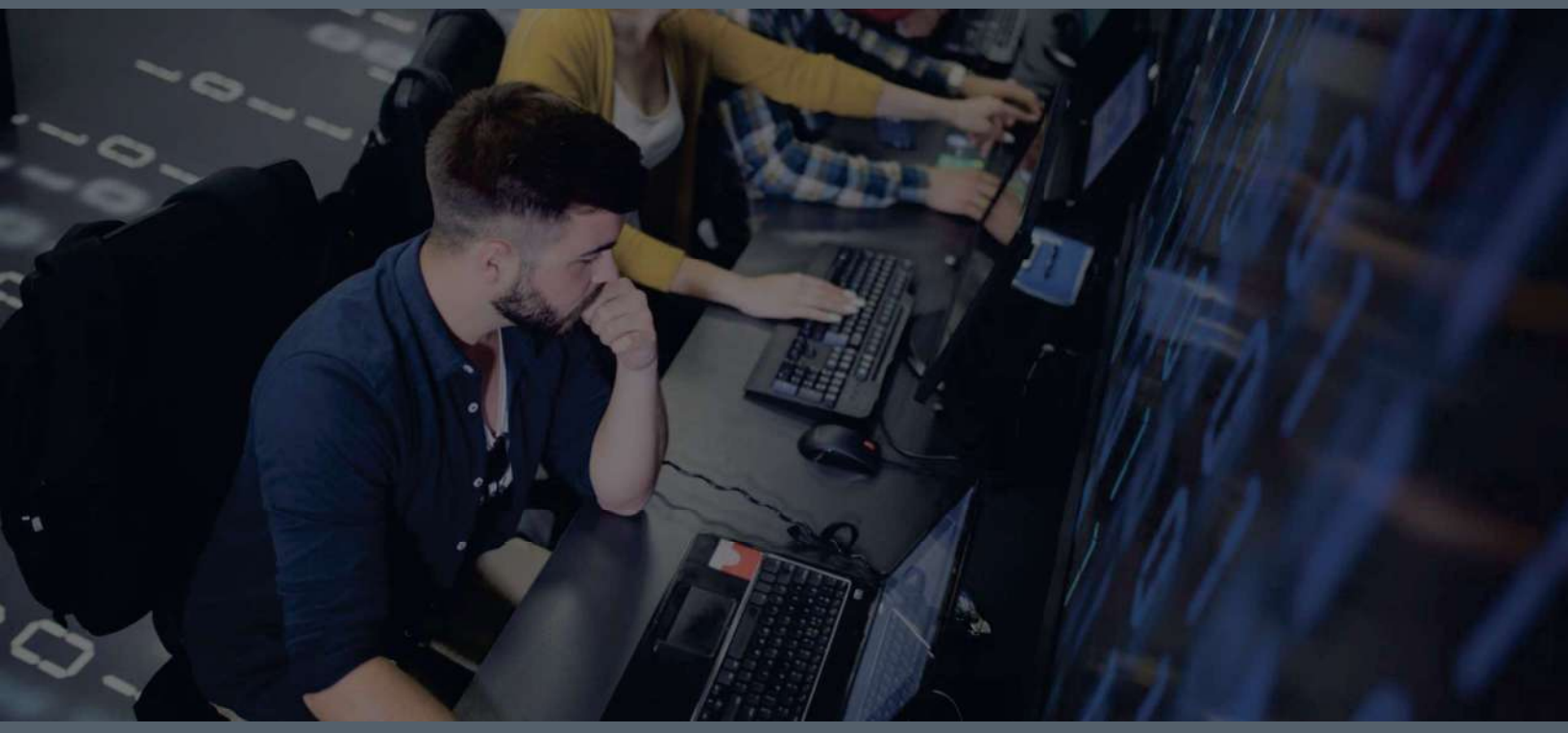
- Shor's algorithm provides the ability to use quantum computing to solve the factorization/discrete logarithm problem in polynomial time. Many of our current asymmetric ciphers as well as signatures are therefore at high risk. The image on the next page provides an overview of threatened common security products.
- Grover's algorithm allows for a quadratic acceleration of a search in an unsorted database, which puts symmetric encryption systems at risk of brute-force attacks. Primarily, algorithms that have a fixed key length/hash length, such as 3DES or MD5, are at risk. However, variants of safer algorithms, such as AES-128, are also at risk. The threats posed by Grover's algorithm can possibly be handled by a key size increase or hash length increase.


Shor
Grover
Quantum algorithms
Data security
Crypto agility
Quantum key distribution
Confidentiality
Fully homomorphic encryption
Quantum random number generator
Areas of cybersecurity impacted by quantum technology
Shaw
MD5
Quad
AES
IDEA
3DES
Vulnerable to Grover
Cryptographic algorithms
ECDSA
Vulnerable to Shor
Schmidt Samoa
Diffie Hellman
ECDH
Rabin
RSA

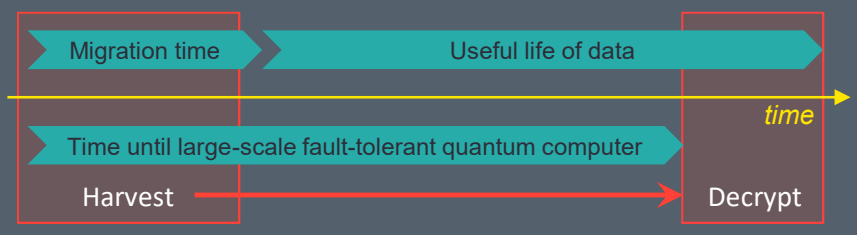
Mapping an overall view on areas of cybersecurity impacted by Quantum Technology

Despite QC technology not being fully established yet, current data can still be vulnerable to QC decryption, as the useful life of data may be longer than the time required to break current encryption methods. Consequently, assessing the risks, analyzing possible impacts, planning and taking measures in today's corporate cybersecurity ecosystem to prepare for the quantum era are essential.

Adequate preparation against the major threats of real-time attacks and harvest-then-decrypt attacks must be implemented, and post-quantum cryptography approaches must be introduced along with standard themes. State and nonstate actors and competing businesses could simply collect a company's data today and copy it (encrypted in current ciphers, such as common public keys). When their quantum system is powerful enough, these entities may use the data they collected and decrypt it using the above-mentioned quantum algorithms.



Sensitive governmental and commercial data that has long lifecycles of R&D and production such as automotive, aerospace and life sciences are extremely vulnerable. Therefore, harvesting the data to date presents one of the most severe threats that requires immediate attention. Determining when to begin the replacement of existing IT depends on the time that data must be kept safe from adversaries, along with the total time it takes to implement the system. The following timeline illustrates the immediacy of attention that this issue demands.



Attackers can harvest data from public and private networks, while it is encrypted with conventional methods, until a full migration to post-quantum cryptography is implemented. Then, they can decrypt that date once a large-scale fault-tolerant quantum computer becomes available, and while the data is still useful.

Common implications for security products due to the quantum technology progress

Below is an overview of the most used public and nonpublic cybersecurity products. This outlines what cryptographic schemes are required for operation, and it also demonstrates exposed threats when the product is working against a quantum-based solution.

The traffic lights represent a high-level risk assessment as quantum computing continues to become more powerful and commercially possible. The green light signifies that systems are secure; amber indicates that the safety implications will be less severe or are harder to be brought about by incidences of theft; red indicates that systems will be severely impacted by data theft.

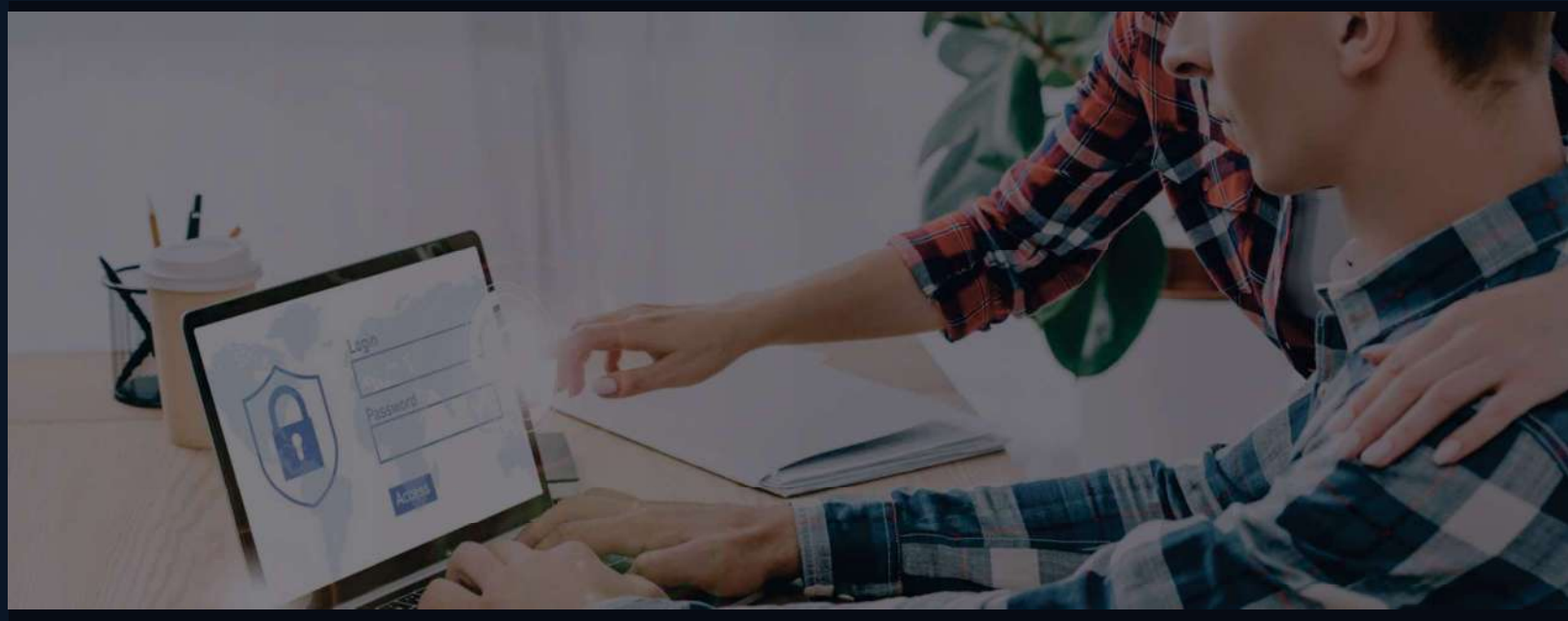
Public Key Infra-structure	Certification Authority (CA), SSL Certificates commonly used. Since 2014, nearly all commercial CAs uses RSA public keys of at least 2048 which is considered to be breakable.
Secure Software Distribution	Mostly public key-based digital signatures, containing RSA public keys.
Federated Autho-rization	Single-sign-on method such as OAuth, OpenID, SAML, among others are widely based on HTTP and once hacked are extremely vulnerable to data theft and criminal acts.
Key Exchange over Public Channel	Key-sharing only between individuals Key exchange, key agreement methods are used in network security protocols like SSHE, IKE, IPsec SSL, TLS to protect private communication. Rely to a large extent on RSA, elliptic curve cryptography or Diffie-Hellman (ECDH) algorithms.
Secure Email	Secure emails commonly via S/MIME for predominantly government entities and regulated enterprises to exchange confidential/authentic email. They largely rely on RSA public keys.
Virtual Private Network	IPSec ensures company network access, work related application access, mobile workforce. VPNs can also be used to circumvent local internet restrictions in foreign countries, creating a tunneling network enabled via RSA or ECC with key establishment protocols such as IKE or mobile IKE.
Secure Web Browsing	Secure-lock web browsing via SSL/TLS enabled websites, mostly required by regulatory requirements/compliance due to user's private information, such as payment data. RSA is still the most common authentication key.
Controller devices	In-built cryptography of controller devices in any kind of machinery (cars, airplanes, manufactory, etc.) usually don't have the storage, computing or communication capabilities to support cryptographic methods such as lattice-based ones, and they are often quite difficult to replace.
Private Blockchain Trans-actions	Blockchain protection algorithms include RSA and ECDSA, thus the crypto world must overcome factoring problem algorithms in order to remain secure. Blockchain transaction signatures for identification and blockchain nodes with internet communication are extremely vulnerable.

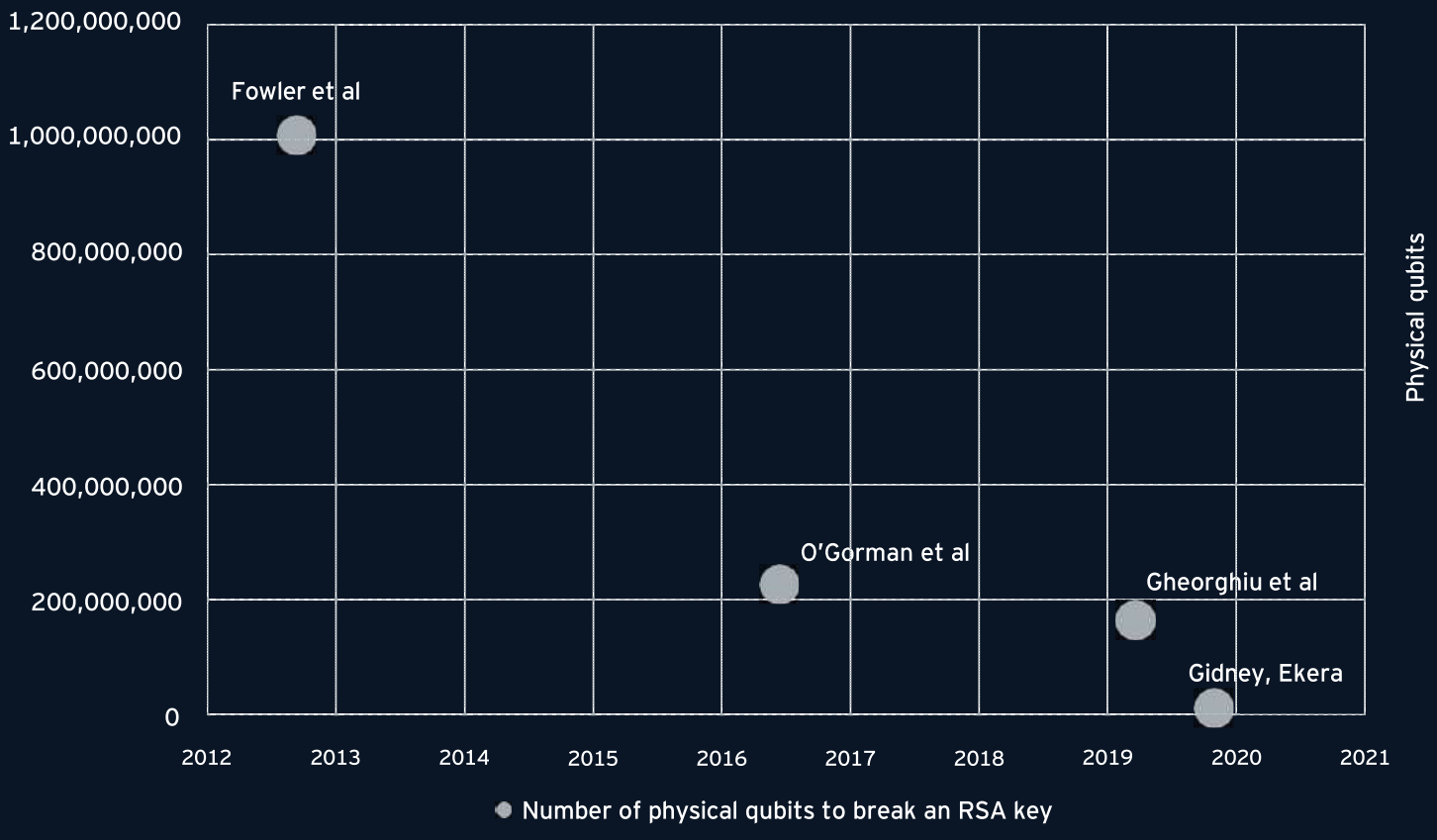
Implications of Quantum Computing on common security products – I

Most of the previously mentioned security product types are not secure with the assumption of rapid quantum technology progression. For the public key classifications of encryption, the increased operation of stable quantum devices threatens security. Specifically, RSA, Elliptic-Curve Diffie-Hellman (ECDH), DSA (Digital Signature Algorithm) and ECC (Elliptic Curve Cryptography) can easily be broken by the correct application of Shor's algorithm on a quantum machine. This is completed through integer factorization and discrete logarithms.

By analyzing the number of physical qubits required to break RSA, we can see that, with the optimization of "noisy qubits" and gate error rates, the number required sank from over 1b qubits in 2012 to 20m qubits in 2019. It is important to note that the number of logical qubits is by far lower, as it assumes that logical qubits require stable merging of various physical qubits to a calculation unit with lower uncertainty.

Researchers from Google and the Royal Institute of Technology-Stockholm have shown how it is possible to factor 2048-bit RSA integers in eight hours using 20m noisy qubits. The graph to the right shows the number of physical qubits required to break the common and widely commercially used RSA algorithm as found by different research teams.

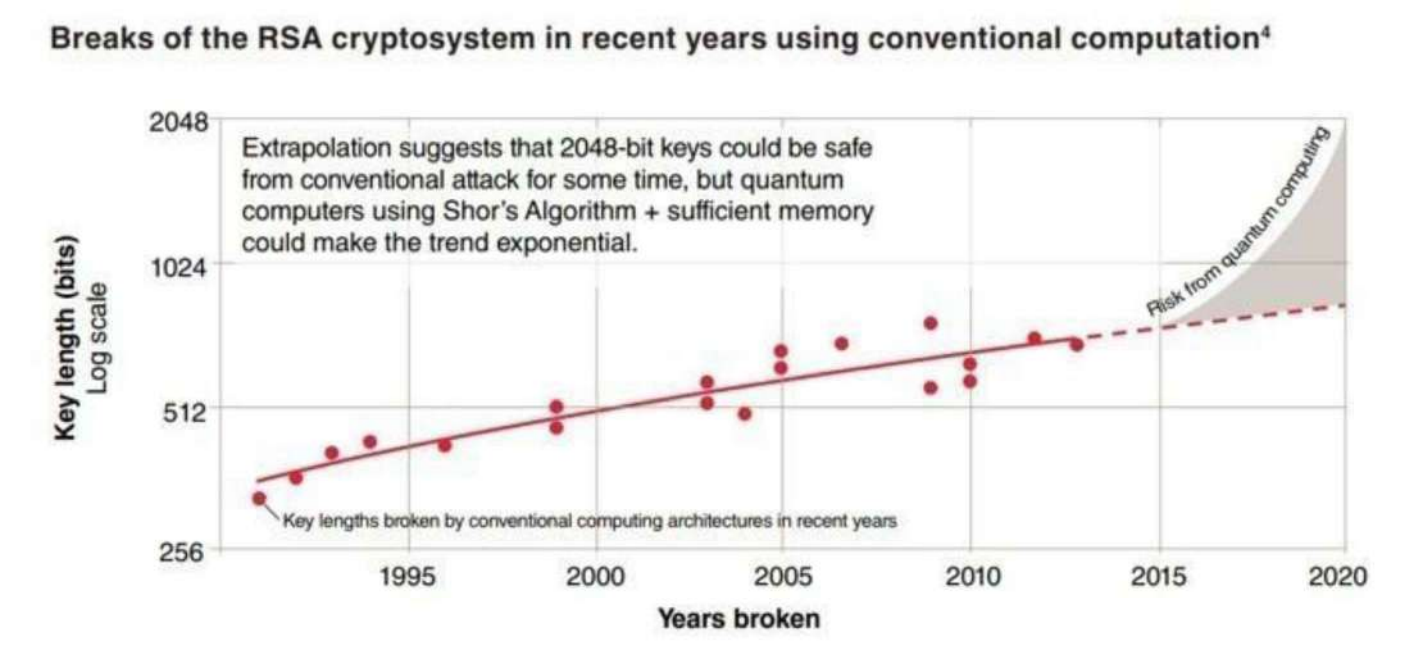




https://arxiv.org/pdf/1905.09749.pdf

Implications of Quantum Computing on common security products – II

The graph below, published by the European Telecommunications Standards Institute (ETSI), shows a representation of RSA breaks and the assumption of how quantum computing will exponentially increase the number of threats. Despite the use of RSA being widespread, threats to cyber infrastructure are increasing due to the risks associated with quantum computing capabilities, as shown on the far right of the graph.

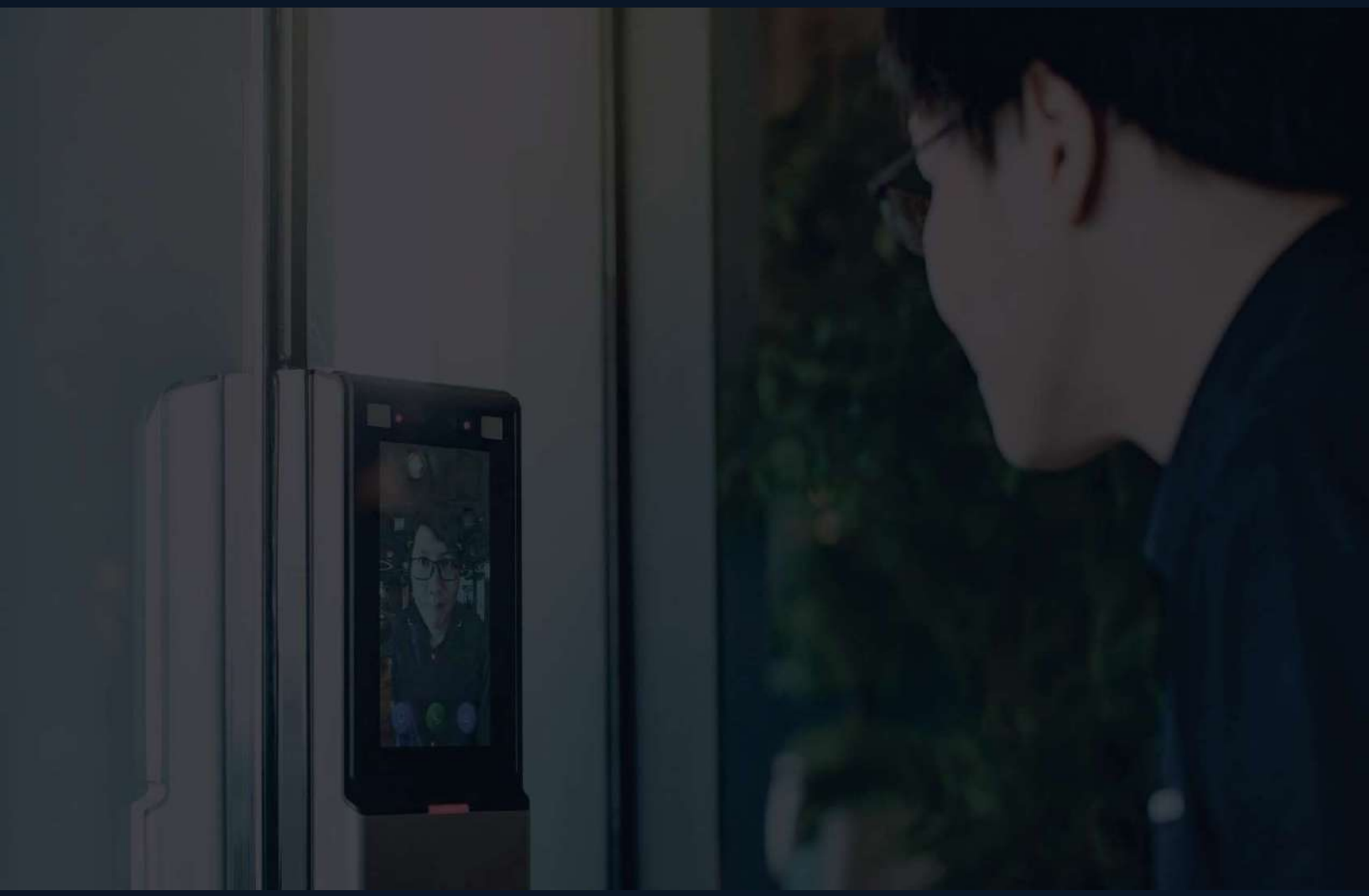


ETSI. "Quantum Safe Cryptography and Security: an introduction, benefits, enablers and challenges," ISBN 979-10-92620-03-0.

As noted in the graph, ETSI's assumption suggests that 2048-bit keys could be safe from conventional attacks for some time is correct given the fact that QCs are not commercially widespread and available. However, there are several pieces of research proving methods of breaking RSA with quantum systems. In May 2019, researchers Gidney and Ekera et al outlined how to factor an RSA-2048 in eight hours. Thus, the risk from quantum computing in 2022 must be considered a serious threat.

What about other encryption methods and their implications?

When comparing the asymmetric RSA to AES (which represents a form of symmetric encryption), it is known that longer keys are required to guarantee quantum-resistant cryptography. For SHA-2 and SHA-3 (used for hash functions), a larger output is necessary to ensure quantum resistance once larger and more stable quantum devices are in place.



Implications of Quantum Computing on common security products – III

The following table compares classical computing and quantum computing security levels of popular ciphers used for common security products, showing how severely common algorithms will be endangered. As we can see in the table, algorithms, such as RSA-2048 and ECC-256, do not show enough effectiveness in terms of key strength or security level in order to survive stable quantum machines.

The number of logical qubits needed to compromise these ciphers scales linearly with the bit length of RSA keys; thus, RSA encryption will become insecure in the future. While an eight-fold acceleration of computational power is required with traditional systems, the number of logical qubits scales linearly. Consequently, actions regarding key management are required and will be outlined further in this publication.

Algorithm	Key length	Effective key strength* / security level	
		Conventional computing	Quantum computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Source: National Institute of Standards and Technology. Report on Post-Quantum Cryptography, Chen et al. (2016), NIST.

* Different ciphers may require different key lengths to achieve the same level of encryption strength. The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values. Source: https://docs.oracle.com/cd/E19424-01/820-4811/aakfw/index.html

Defining evaluation criteria for quantum-era cybersecurity and its complexity has become essential to any business relying on secure data and the development of future business models, with respect to data security.

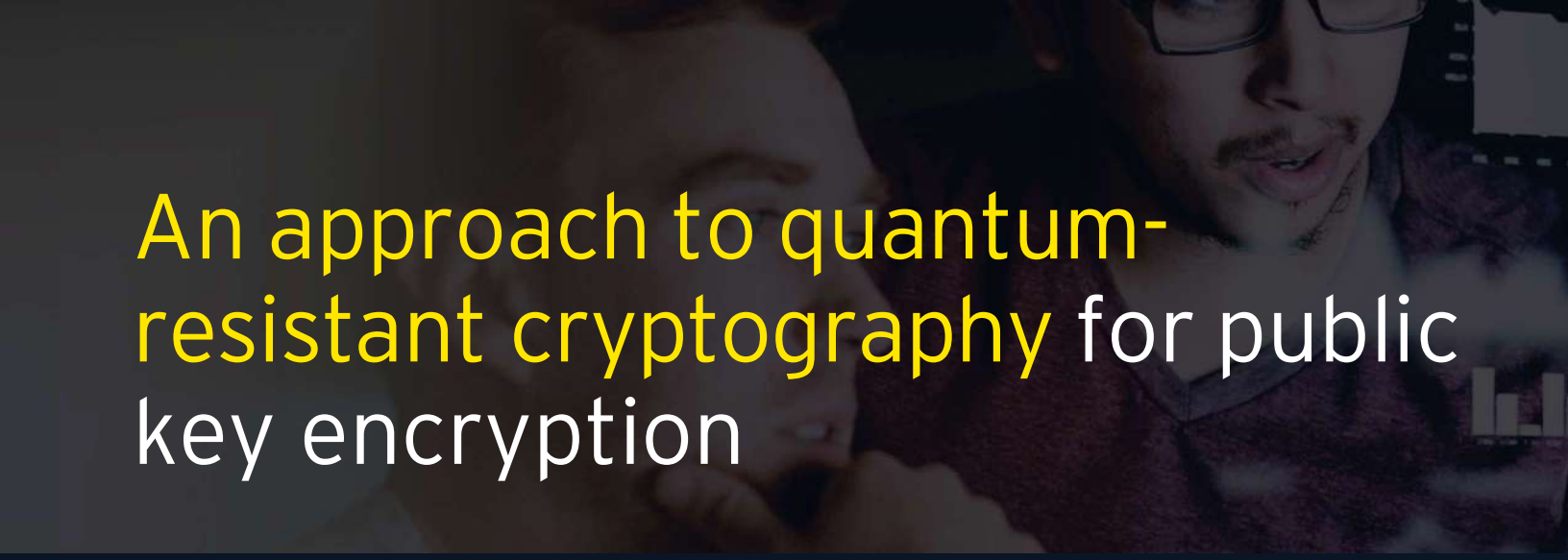
Evaluation criteria for Quantum Cryptography

The National Institute of Standards and Technology – NIST made some initial attempts to classify quantum attack complexity in terms of circuit sizes. Specifically, the complexity is compared to the effort required to break AES or SHA3. Consequently, AES, to some extent, is considered quantum safe because the cipher can adapt to a quantum attack by increasing its key size to rectify a vulnerability introduced by quantum systems.

To date, there has been no clear consensus from a public standards board on how to measure quantum attacks and assess uncertainties. For post-quantum cryptographic eras, security estimates and specific standardized parameters need to be established. Using these parameters, performance characteristics for crypto algorithms can be evaluated. By using NIST guidance and the algorithm assumptions from the table below, a subset of security evaluation criteria levels can be assessed. The security strength levels represent the possible guidance of how rating new post-quantum cryptography security standards can be introduced and implemented.

Level	Security description
1	Minimum difficulty to break as AES-128 (exhaustive key search)
2	Minimum difficulty to break as SHA3-256 (collision search)
3	Minimum difficulty to break as AES-192 (exhaustive key search)
4	Minimum difficulty to break as SHA3-384 (collision search)
5	Minimum difficulty to break as AES-256 (exhaustive key search)

With respect to categorization and classification of computational resources and security products in use, additional parameters, such as the number of classical elementary operations and quantum circuit size, also need to be considered. Realistic limitations on circuit depths, such as 2^{40} to 2^{80} logical gates, and the expected costs of quantum and classical gates, should be compared for all levels of security in order to obtain a generalized view.



An approach to quantum-resistant cryptography for public key encryption

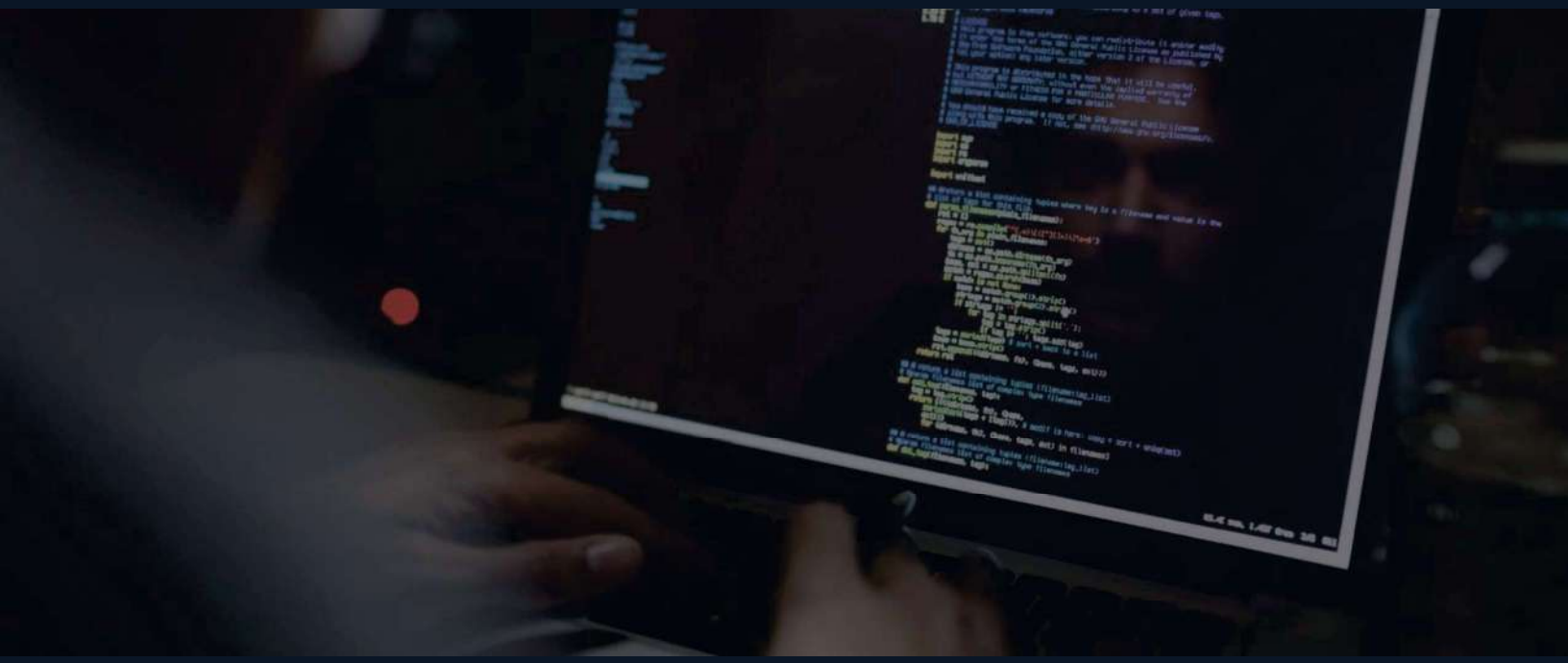
At present, symmetric cryptography is still considered useful in the quantum era, as it achieves an exponential speed-up over search algorithms that tend to be impossible, and the quadratic speed-up provided by Grover's algorithm is realizable by doubling key sizes. Current asymmetric cryptography is used worldwide to distribute symmetric keys and to prove identities with digital certification, and they are proven not to be quantum resistant.

However, new algorithms that are thought to be quantum resistant have been, and still are, under steady development to address the potential threat of quantum computers. Four of the quantum-resistant cryptographic schemes considered are presented below:

Lattice-based cryptography	Based on the NP-complex Shortest Vector Problem (SVP), lattice-based cryptography is considered strong and hard to break and is favored to succeed to the current systems.
Code-based cryptography	This cryptosystem is based on error-correcting codes and another NP-hard problem called "syndrome decoding."
Multivariate polynomial cryptography	Multivariate polynomial cryptography is based on the difficulty of resolving multivariate equations and tends to be a good alternative to quantum-secure digital signatures.
Hash-based cryptography	By combining binary trees and hash functions, hash-based cryptography offers one-time signature schemes that could be used for digital certificates.

If the cryptosystems remain quantum resistant, they also present some drawbacks that, so far, have prevented them from being widely used instead of RSA, ECC and Diffie-Hellman algorithms. Comparisons using criteria such as key generation time, signing time, verification time, encryption and decryption time have shown that these cryptosystems can deliver a similar, or better, performance than the RSA, but they suffer from much larger key, message and signature size. This can cause inconvenience and impracticability.

Additionally, these quantum-resistant algorithms have not benefited from the same level of research and cryptoanalysis that commonly used asymmetric algorithms have. If the introduction of a new set of post-quantum standards for organizations by 2025 is the goal, researchers and standardization organizations, such as ETSI, must work on potential solutions that could replace existing primitives and cryptosystems. In 2016, NIST launched the Post-Quantum Cryptography Standardization program, a four-round competition that aimed to select the best quantum-proof algorithms. Four finalists with promising results were selected in 2022. For organizations, this might also involve needing to replace existing infrastructure, as incompatibility issues may be raised for hardcoded algorithms in hardware.



Regulatory response to current and future quantum computing threats

An important step for businesses on the journey toward quantum-safe cryptography is to become aware of developments in the regulatory environment. Regulatory efforts to address post-quantum cryptography have already been initiated. Standardization institutions, such as the NIST or ETSI, are now working on the first set of standards, that is expected to be published around 2024.

The following Post Quantum Computing (PQC) methods are presented as first candidates for standardization, as they can offer long-term protection with a sufficient security level:

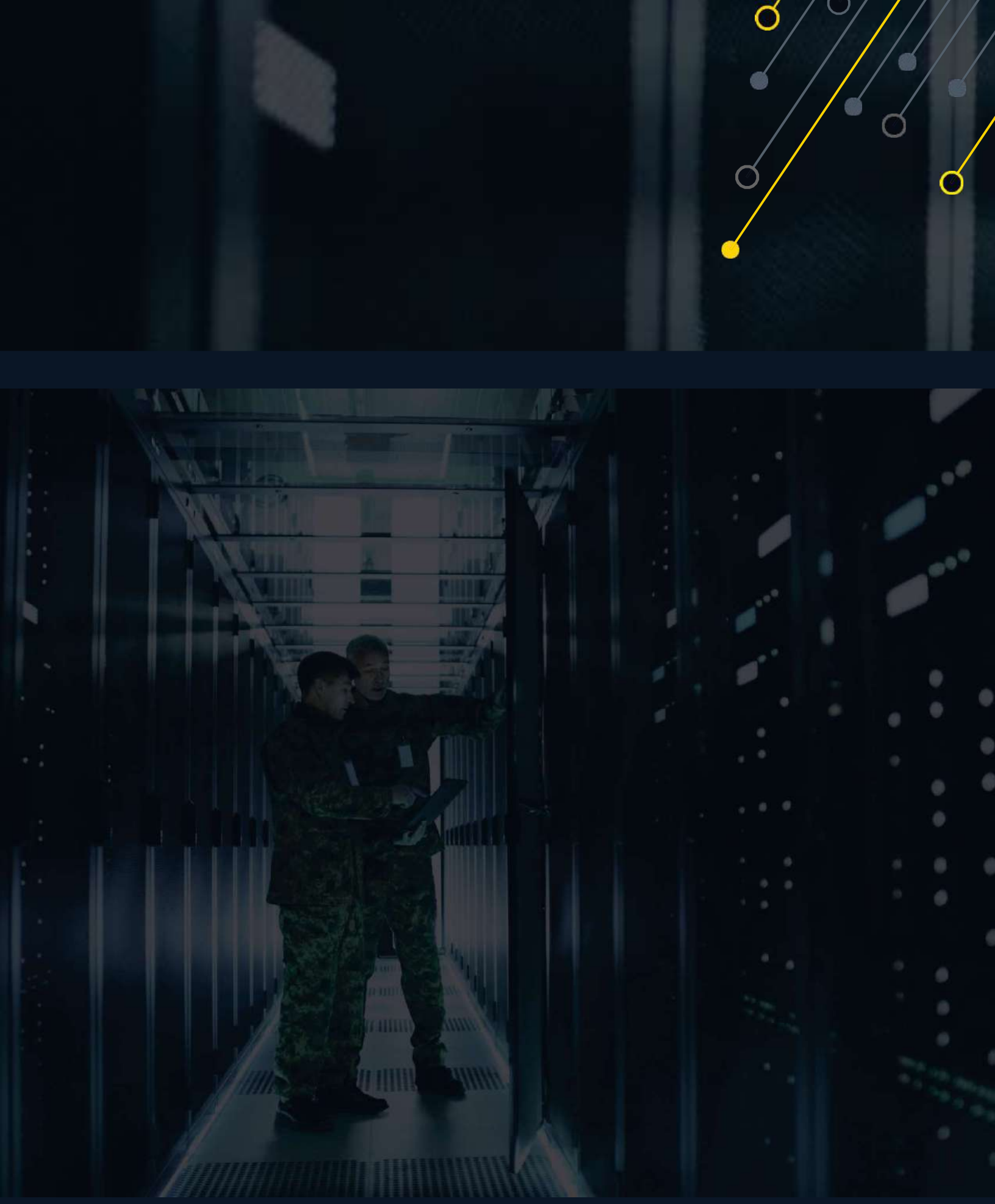
CRYSTALS-KYBER	CRYSTALS-KYBER can be used for key establishment –e.g., to access secure websites– and offers strong security and excellent performance. NIST expects it to work well in most applications.
CRYSTALS-Dilithium	CRYSTALS-Dilithium is a lattice-based signature scheme that can be used for digital signature and offers strong security and high efficiency. NIST recommends it as primary algorithm for digital signature.
FALCON	FALCON also relies on structured lattices and will also be standardized by NIST, since there may be use cases and applications that need smaller signatures than CRYSTALS-Dilithium can provide.
SPHINCS+	SPHINCS+ is a stateless hash-based signature scheme that incorporates multiple improvements, specifically aimed at reducing signature size. It will be standardized to avoid relying only on the security of lattices for signatures.

NIST's selected algorithms for Digital Signature, Public-key Encryption and Key-establishment Algorithms (2022)

Due to a lack of experience regarding the safe implementation of these new PQC methods, some standardization agencies recommend implementing these new PQC methods in combination with proven encryption methods based on either ECC or RSA, through "crypto-agile" solutions that allow security teams to swiftly change from one encryption approach to another, or even combine several of them.

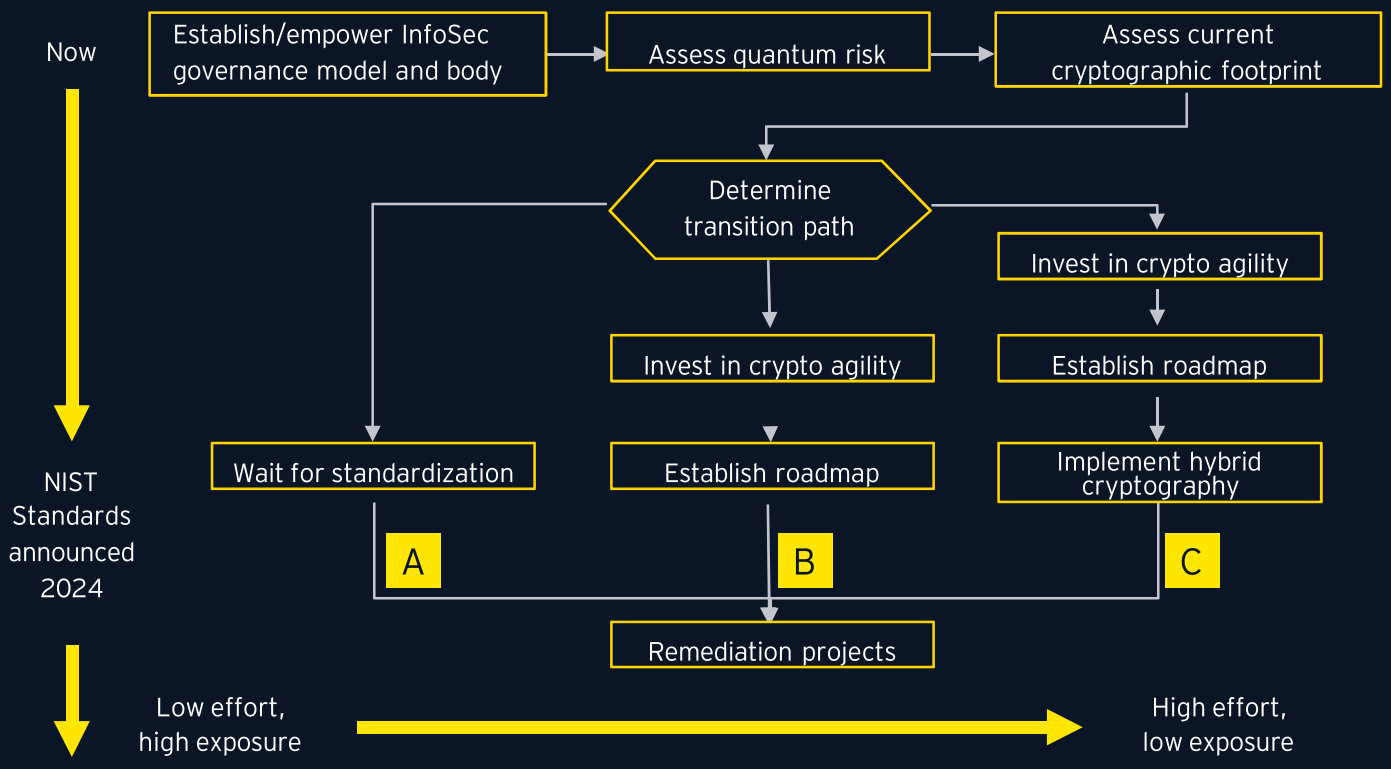
Establishing new standards and following regulations are global goals for a quantum-safe future of cybersecurity, and they require special attention by all involved in the quantum computing movement.

Source: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization



How to address quantum threats: creating a secure quantum defense today

Given the threats and regulatory response, time is of the essence to take action. With the following quantum readiness roadmap, entities can assess how ready their cyber business model is for the quantum era and reduce their exposure to quantum attacks. Once the assessment has been performed, the governance model and body can be revised and redefined on the path to a quantum-resilient future.



Source: https://queue.acm.org/detail.cfm?id=3466779

According to the Cybersecurity Research Lab at Toronto Metropolitan University and Ted Rogers School of Information Technology Management, organizations' readiness for quantum threats and standardization can be divided into three different strategies and scenarios to be applied after a thorough quantum risk assessment:

A Certain organizations will wait for standardization regulations to enter into force before taking any initiative. This includes companies whose data is of relatively low value for potential hackers or data that exists for a short period of time.

B Some organizations will invest in crypto agility beforehand and be ready to launch appropriate initiatives by the time official standards enter into force by establishing an adaptable and maintained roadmap.

C Few organizations with higher risk and sufficient resources will go beyond; in addition to being crypto agile, they will adopt a hybrid posture by implementing a quantum-resistant security layer on top of the existing one. This will help reduce the risk of data being stolen now and decrypted in the future, when fully operational quantum computers will be available for use.

Assessing and reducing the quantum risk exposure of organizations, as well as preparing for the transition to quantum resistance, appear to be essential for a quantum-resilient future.

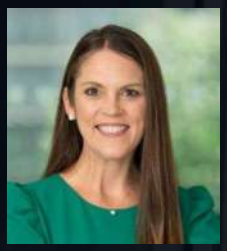
Disclaimer

The views of third parties set out in this publication are not necessarily the views of the Global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

Key contacts

Jeff Wong

Partner/Principal
EY Global Chief Innovation Officer
+1 408 947 4904
jeff.wong@ey.com



Kristin M. Gilkes, PhD

Partner/Principal
EY Global Innovation Quantum Leader
+1 202 327 7477
kristin.m.gilkes@ey.com

Chris Hall

Partner/Principal
Cybersecurity Innovation Leader
+1 412 644 7867
chris.hall3@ey.com

Additional contributors:
Deepak Arora, Alexey Bocharnikov, Guzmán Calleja, Christoph Capellaro, Rafael Martín-Cuevas.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 006278-22Gbl

2208-4075977
ED None

ey.com