Aliro QUANTUM®

Navigating Security Threats Posed by Q-Day

Aliro Quantum

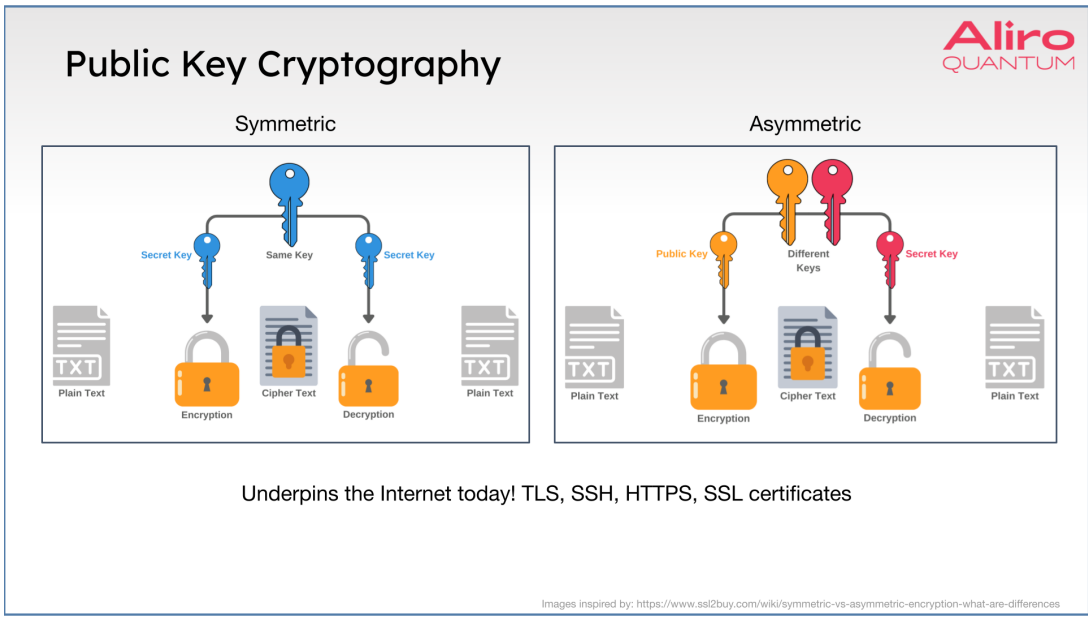
In this white paper, we aim to address what Q-Day is, how Q-Day impacts critical infrastructure, and when we expect Q-Day to arrive. In addition to these areas, we'll provide an assessment of today's encryption schemes, how they are utilized, and which schemes are most vulnerable to certain kinds of quantum attacks. We'll also discuss how and when to prepare for the inevitable arrival of Q-Day.

What is Q-Day?

Q-Day is the day that a quantum computer will be able to crack our public encryption systems. The encryption schemes that are most susceptible to quantum attacks are those that rely on large prime numbers, and it's these same encryption schemes that underpin nearly all digital communication systems. While it's a daunting prospect, being informed and understanding the implications of this level of computing power and what to do about it is an important step in mitigating the risks it poses.

An Assessment of Encryption Schemes

Many networked systems and the applications they enable – from online banking to protecting sensitive medical data to water and electricity management – rely on what's called public key cryptography or public key infrastructure. Broadly speaking, there are two types of public key encryption in use every day: symmetric encryption and asymmetric encryption. Symmetric encryption and asymmetric encryption ultimately underpin all of the Internet today. For example, if you're using Chrome as your web browser, in the top left corner of your browser window, next to the URL, you'll see a padlock icon. The padlock icon indicates HTTPS is being utilized, which makes use of both symmetric and asymmetric encryption: an HTTPS connection between a client and a server uses both symmetric and asymmetric encryption. Asymmetric encryption is used first to establish communication and exchange secrets, and then symmetric encryption is used for the rest of the communication. These two protocols in your everyday life, whether you're aware of it or not.



Symmetric Encryption

In symmetric encryption, when two parties on a network want to communicate, they do so using a pre-shared secret key. This key is only known to the two parties that want to communicate. For example, Alice wants to send a message to Bob. In a symmetric encryption scheme, Alice will encrypt her message using the secret key to transform her plaintext into ciphertext. The ciphertext is sent over to Bob. When Bob receives this cipher text from Alice, he can decrypt it back into plaintext using that same pre-shared secret key. In this scenario using symmetric encryption, there's only one key involved, but it is pre-shared. It's kept secret for the two parties that want to communicate.

Symmetric encryption is used for what's sometimes called "bulk" encryption or decryption - it can be used to send large amounts of data.[ENCRYPTION] The ciphertext is quite small relative to the data size. This can be accomplished very quickly. The key lengths are comparatively small at 128 bits or 256 bits. There's a single key for encryption and decryption.

Asymmetric Encryption

In asymmetric encryption, there are two keys. Each party on the network has what's called a public key. This public key is advertised to the world. Anyone can see it. Each party also has their own private, secret key. Using asymmetric encryption in the example, Alice will use Bob's public key to encrypt her message into the cipher text. That cipher text is then sent over to Bob. Bob can then decrypt that data using his secret key. So the security of the asymmetric encryption relies on the fact that only Bob is able to decrypt the data with the secret key that is only known to him. Anyone else who has access to that ciphertext will not be able to read it or decrypt it, unless they have Bob's secret key.

In asymmetric encryption, the ciphertext is quite large compared to the data size. It takes more compute resources, it's slower, and the key lengths are much longer - in the range of 1000s of bits. The most common asymmetric encryption is the 2048-bit RSA key. In this setup, two keys are used for encryption and decryption.[ENCRYPTION]

Hybrid Cryptosystems

Symmetric encryption and asymmetric encryption can also be used together in what's called hybrid cryptosystems. The way that some modern networks operate today is through using asymmetric encryption, like RSA or Diffie Hellman, to exchange a symmetric key. The key exchange is accomplished using comparatively less efficient asymmetric protocols. The symmetric key that is exchanged this way can then be used for the faster bulk encryption with the symmetric protocols. Some examples of these hybrid cryptosystems are PGP, SSH, SSL, and TLS.

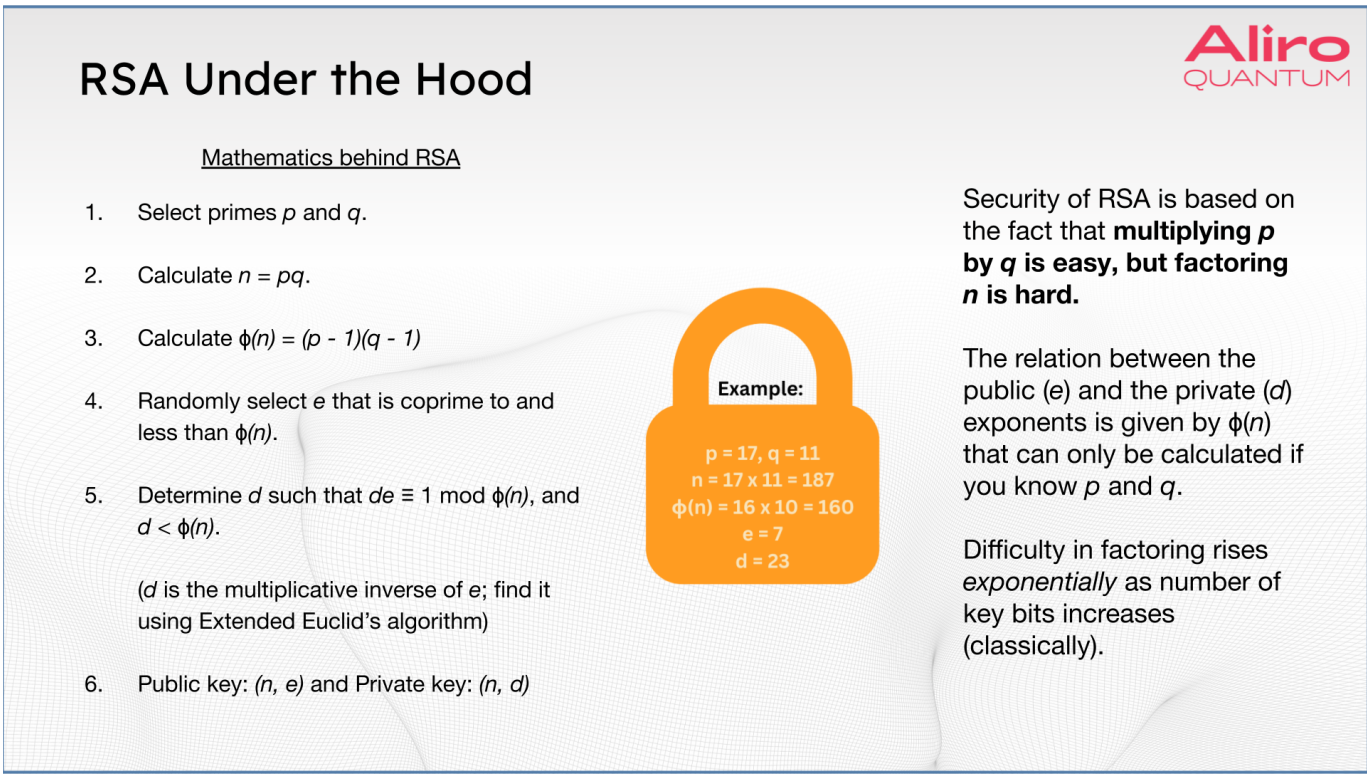
Vulnerable encryption schemes

Symmetric encryption protocols are susceptible to quantum attack, but not all of these schemes are completely broken.

Asymmetric encryption protocols, which are the most popular and integrated into most of our systems today, will be fully broken by the advent of a cryptographically-relevant quantum

computer. Protocols such as RSA, Diffie Hellman, and elliptic curve cryptography are all vulnerable.

When considering quantum attacks by quantum computers, RSA is often used as the defining example. How RSA works, where the security comes from, and how quantum computing changes that, is an important part of understanding what makes an encryption scheme vulnerable.



In the above graphic, on the left are the steps RSA takes to encrypt data. The first step is selecting two prime numbers, p and q. These are two large prime numbers that a node will select and will calculate their product, and with a bit more math it will create the public key and the private key. These are both necessary for asymmetric encryption. The security of RSA is based on the fact that multiplying the original two prime numbers is easy computationally, but factoring their product *n* into *p* and *q* is quite difficult using classical technology alone. Cracking the private key generated by RSA requires cracking that factorization. The difficulty in performing that factorization increases exponentially with the size of *n* - regardless of whether it's a laptop or the world's biggest supercomputer. The assumption that it is exponentially difficult to factor a number *n* into its primes underpins almost all of our digital systems. This assumption held true until 1994, when Shor's algorithm was developed.

Why encryption schemes are vulnerable

Shor’s Algorithm

In 1994, Peter Shor discovered what's now known as Shor's algorithm. Shor's algorithm is a quantum algorithm: an algorithm that runs on a quantum computer using qubits. This algorithm provides an exponential speed up over classical computers for solving integer factorization. Shor's algorithm can also be used to crack the discrete logarithm problem and the elliptic curve discrete logarithm problem. These other math problems are used for the elliptic curve, which are variants of the asymmetric protocols we're talking about.
By running Shor's algorithm, an adversary will be able to deduce private keys from a public key. This means that RSA, Diffie Hellman, and their elliptic curve variants - cryptosystems that we rely on heavily today - will be completely broken by a sufficiently powerful quantum computer.

Grover’s Algorithm

Grover's algorithm is a quantum algorithm that provides a significant speed up of brute-force search. Brute-force search is a technique that consists of systematically checking all possible solutions to determine which solution satisfies the problem's statement. Brute-force search is most often used when possible solutions can be reduced to a manageable size, but in the case of a quantum computer running Grover’s algorithm the manageable size is much greater than it is for a classical computer. For example, an adversary using Grover’s algorithm will be able to crack a 128-bit key much faster than is possible with a classical computer using brute-force search. Brute-force searching for a 128-bit key that successfully decrypts a ciphertext will require searching all 2^128 possible keys. However, with Grover’s algorithm, this can be accomplished by searching just 2^64 possible keys. Grover's algorithm specifically endangers data that is encrypted and stored on online servers.

Not only can it be used to speed up a brute- force search for a symmetric key, but it can also be used to reverse engineer a cryptographic hash function, which are also frequently used in current cryptographic schemes. Grover's algorithm can reduce the time it takes to find the input of a hash output. This has implications for collision attacks and birthday surprise attacks. A collision attack on a cryptographic hash is seeking to identify the two inputs producing the same hash value. A birthday surprise attack is a brute-force attack that takes advantage of the mathematics behind the birthday problem in probability theory.

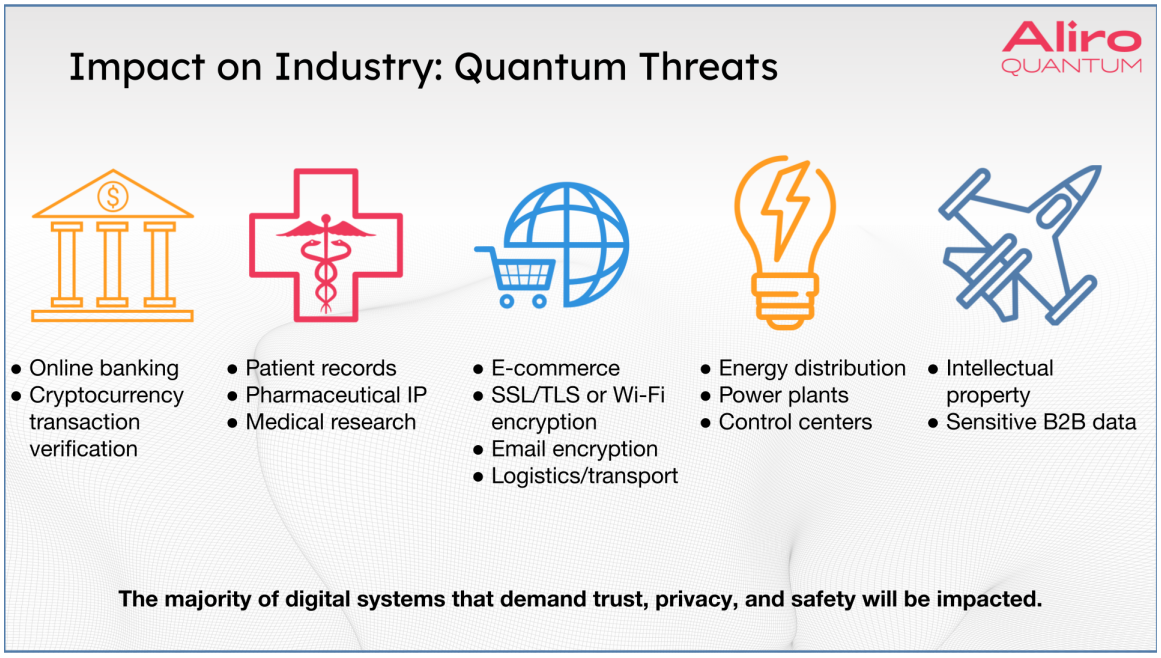
Documents, messages, web certificates, software, financial transactions can all be forged with the advent of a cryptographically-relevant quantum computer. Because of the implications of Shor's and Grover's, secret keys are exposed in the clear, and adversaries will be able to read whatever you're receiving. Internet traffic will no longer be secure.

This has implications right now, due to what's called Harvest Now Decrypt Later attacks: an adversary today can harvest and collect encrypted data. This data can't be accessed today, but as soon as a sufficiently powerful quantum computer comes into play, it will be able to

recover and decrypt all of that data. Any sensitive data that's being encrypted right now is vulnerable to quantum attack at a later date.

The impact of Q-Day: now and in the future

Nearly all industries in the US and globally rely on these digital systems. Under the hood, that means they rely on the public key infrastructure discussed previously.

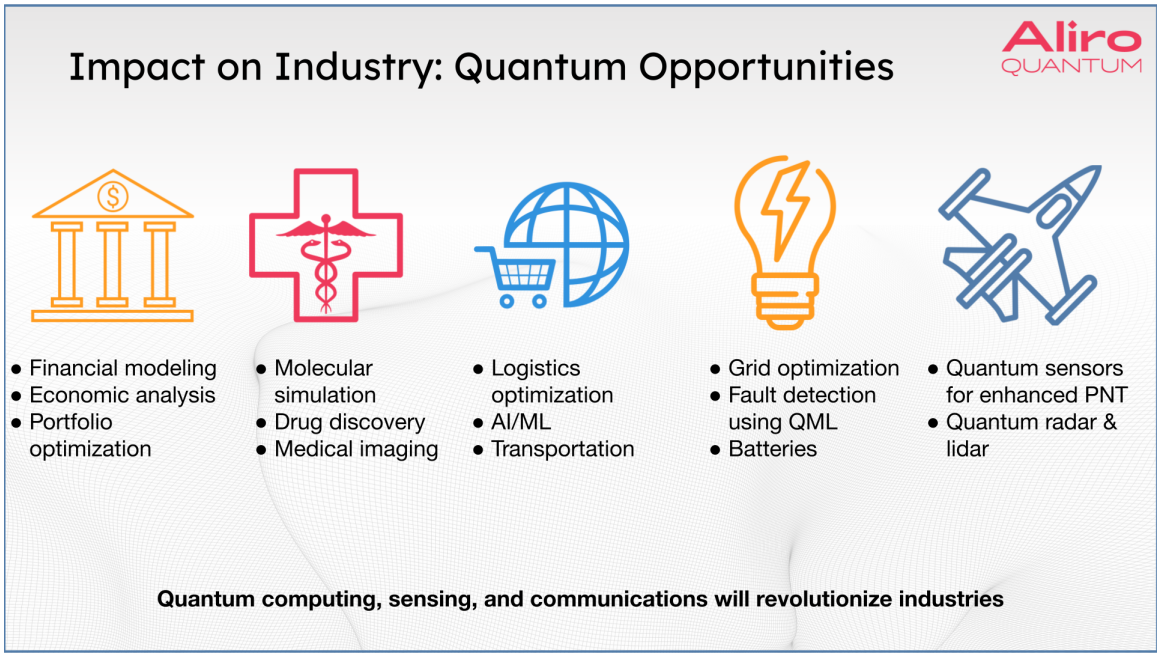


Public key infrastructure is specifically used for:

- documents, messages, certificates, code, and transactions can be forged
- identity over the internet is not guaranteed
- software authenticity is not guaranteed
- secret keys can be exposed
- internet traffic no longer secure
    - secure online banking
    - transaction verification on blockchain
    - communicate sensitive data like patient records, pharmaceutical intellectual property, and medical research data
    - making online purchases
- energy distribution in our power plants and control centers
- protecting sensitive data being shared from business to business and intellectual property for private defense

A majority of digital systems that demand trust, privacy, and safety rely on public key infrastructure and these exact systems are the most vulnerable to Q-Day impacts.
The promise of quantum technology

The quantum revolution will also revolutionize these industries in a positive way. Novel quantum applications that use quantum computers, quantum sensors, and quantum communications will shift these industries in positive ways.



- In the financial sector there's promising research into enhanced financial modeling, better economic analysis, and portfolio optimization. Quantum algorithms for these applications have already been developed.
- Quantum computers could be used to simulate quantum reactions. This holds promise for the healthcare industry with molecular simulation, drug discovery, and vast improvements to medical imaging.
- There's potential for quantum computers to enhance AI and machine learning, with benefits in logistics optimization and transportation, as well as grid optimization and fault detection in the energy grid.
- Quantum computers could be used to simulate chemical reactions for discovering novel battery technology.
- Quantum sensors could provide enhanced position navigation and timing for our military systems and GPS infrastructure. Applications like quantum radar and quantum LIDAR could be enabled with this technology.

The quantum revolution will provide immense benefits to these industries and to society more broadly.

Critical infrastructure impacted by Q-Day

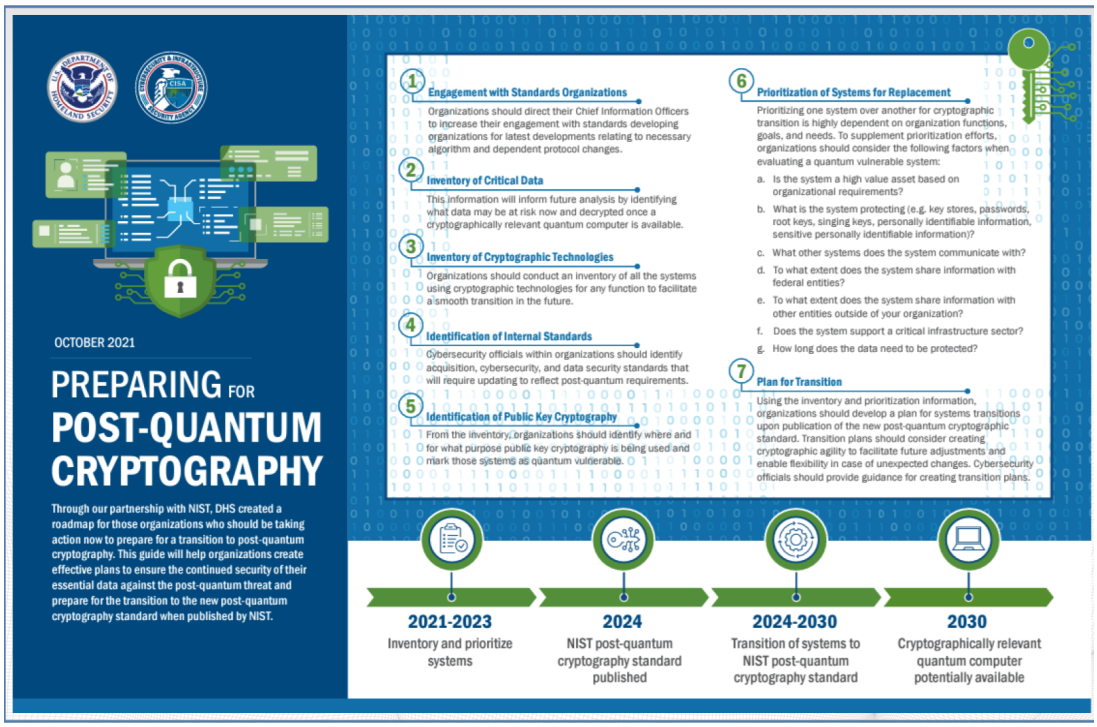
Q-Day could have a potentially catastrophic impact on critical infrastructure that we rely on day to day.

> “The security of the U.S. information and communication infrastructure is currently predicated on the assumption that it is impractically hard for computers to solve certain mathematical problems, such as integer factorization and finding the discrete logarithm of elliptic curves”
>
> Vermeer, Michael J. D., et al. Preparing for Post-Quantum Critical Infrastructure - RAND Corporation, 2022

This quote from the Department of Homeland Security’s collaboration with CIS and the RAND Corporation is acknowledging that the security of our information and our communication infrastructure is all predicated on this assumption: that in practice, there are certain math problems that are hard for classical computers to solve.[DHS] Shor's algorithm cracks these exact math problems exponentially faster. The Department of Homeland Security, and CIS, in cooperation with the RAND Corporation, released a report where they identified and assessed all 55 national critical functions, to determine the threat of Q-Day to each specific critical infrastructure. They focused on several key questions:

- What is the urgency of upgrading the system to become quantum safe?
- What's the scope of this migration?
- How much is going to cost?
- What other factors need to be considered?

The report found that all national critical functions need to prepare for the migration to a quantum-safe solution, and released a timeline for making those changes along with other recommendations.[PQC]



While these recommendations are helpful, Aliro is often asked, “When do I really need to worry about this?” There is a theorem that addresses this question, called Mosca’s Theorem.[MOSCA]

If X plus Y is greater than Z, then you should be worried. So what are X, Y, and Z in this equation? Z is the time until Q-Day. This is how long before a cryptographically-relevant quantum computer arrives. Y is the migration time. It's going to take time to upgrade these vast systems to a quantum-safe solution. X is what is referred to as the security shelf life. Depending on the data being protected and its sensitivity, it may have a particular length of time it needs to be protected. For example, storing bank account numbers has a certain shelf life where the security of that number needs to be maintained. The shelf life of a bank account number may differ from the shelf life of sensitive military data. The potential negative impacts of data becoming vulnerable also varies: who it impacts, and how broad that impact is. In Mosca’s Theorem, if X plus Y is greater than Z, then that means there's going to be a time when secret keys are compromised and vulnerable to quantum attack. These variables can be

used to help organizations determine their own level of urgency around implementing quantum-safe security measures.

A timeline for Q-Day

The security implications of a cryptographically-relevant quantum computer has been known since the development of Shor's algorithm in 1994. In 2016, the National Institute of Standards and Technology (NIST), the standards body in the United States, announced a call to begin the process of standardizing the replacement of vulnerable encryption schemes with Post Quantum Cryptography (PQC). In 2019, Google declared quantum supremacy, a significant milestone in quantum computing. The timeline to Q-Day is contracting. More milestones are being achieved on the quantum computing front that are reducing the timeline. NIST is still in the process of standardizing new PQC solutions, with the final standards expected to be published in 2024. There is an aggressive view of when Q-Day will happen, and there's a more conservative view of when Q-Day will happen. Organizations presented with securing our critical infrastructure and sensitive data should probably adopt the more aggressive view of this timeline toward quantum-safe security adoption. Q-Day is likely to happen sometime in the next three to ten years, with the more aggressive estimates predicting a three to five year timescale. A quantum computer will be able to crack RSA 2048 in the future. However, data is vulnerable now due to Harvest Now Decrypt Later attacks. New research is coming out that is further contracting the estimated timeline to Q-Day. Research published December 2022 from some researchers in China claims to have developed a method to crack RSA 2048 using only 372 qubits.[SUBLINEAR] If this holds true, then Q-Day is a lot closer than originally anticipated. Additionally, new algorithmic developments, such as Variational Quantum Factoring, have opened new directions of study towards using hybrid quantum-classical algorithms to solve the integer factorization problem. Quantum computing hardware has also seen accelerated improvement, with many promising paths toward fault-tolerance and scalability. Prior to this research, it has been estimated that many thousands, up to millions, of qubits would be needed to successfully break RSA 2048.

The path to a cryptographically relevant quantum computer

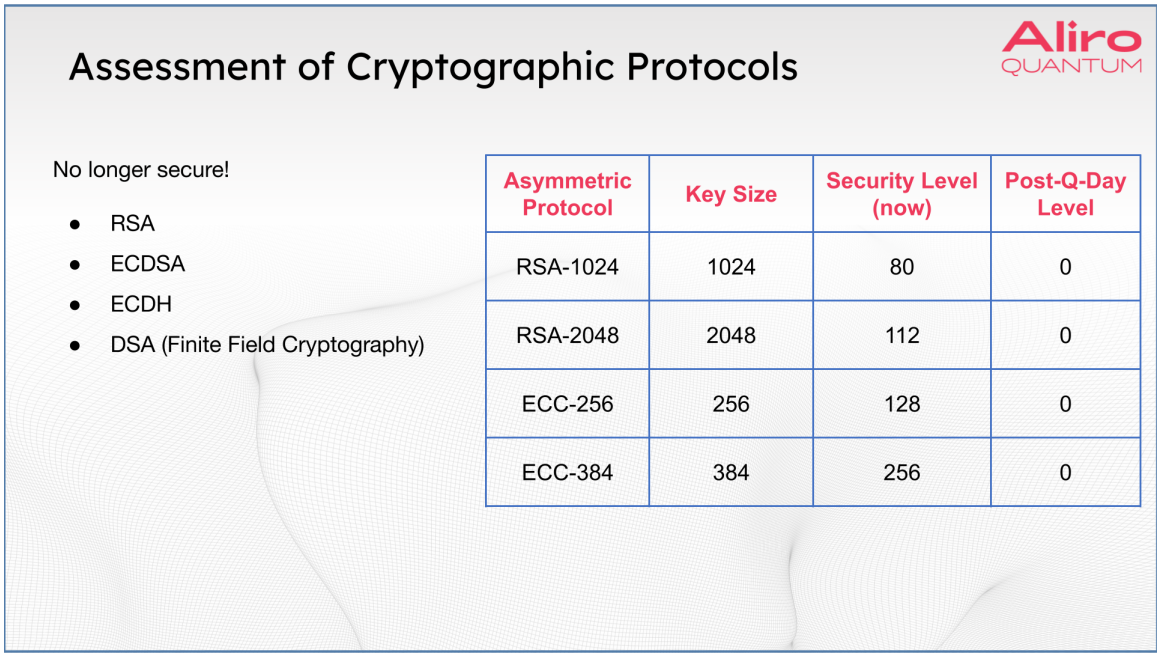
There are two branches to advancing quantum computing capabilities. The first branch is hardware development. The second branch is the algorithmic or software front of advancement. On the hardware side, a lot of progress has been made much more rapidly than expected. New claims and milestones like increased coherence times of qubits, faster gate speeds in quantum processors, and lower error rates are all contributing to quantum computing advancement. In addition, the introduction of novel qubit modalities, different kinds of technologies for quantum computing hardware, show a lot of promise and indicate that hardware advancement is being expedited by these developments. On the algorithmic and software side, there has also been quite a bit of advancement. For example, there is now a proposed algorithm called variational quantum factoring. This algorithm uses both a quantum computer and a classical computer working together to solve the integer factorization problem

underpinning so many of the encryption schemes in-use today. The researchers claim this variational approach will actually reduce the qubit overhead from previous estimates of tens of millions of qubits to perform Shor's algorithm. According to this research, only around 6000 qubits will be required to crack RSA 2048.[ZAPATA]

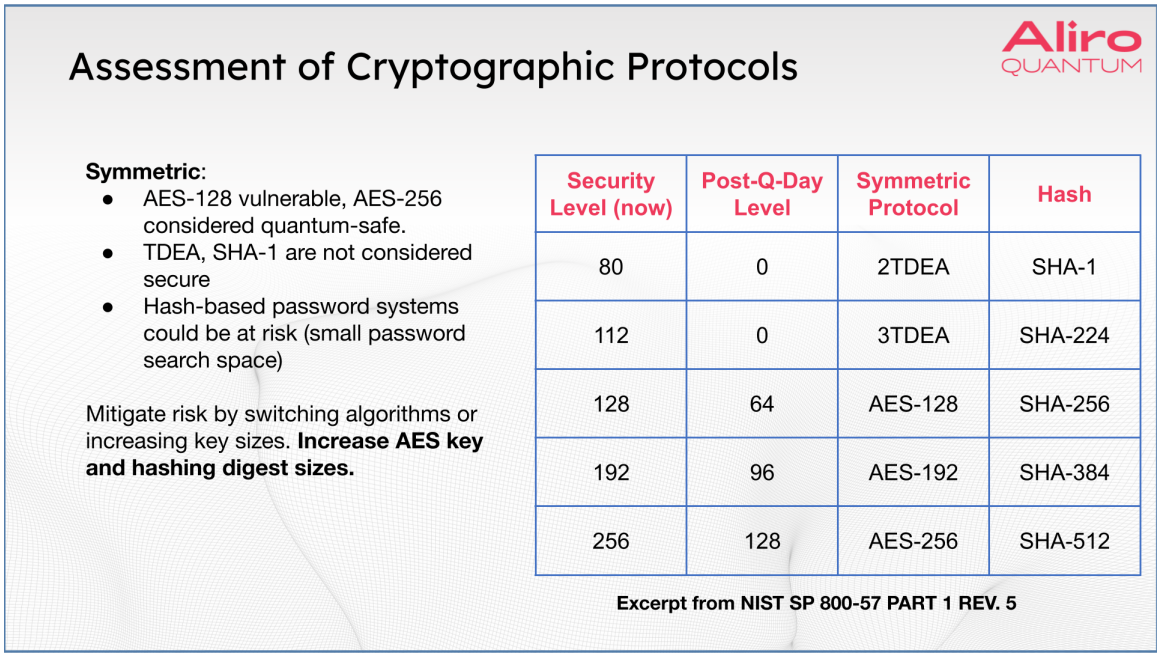
All these milestones and researched advancements are contributing to the ever shrinking estimate as to when Q-Day will actually occur.

Assessment of cryptographic protocols

The most popular protocols that are vulnerable to quantum attacks are RSA, Diffie Hellman, and the elliptic curve variants. After Q-Day, the security level of these protocols goes down to zero: they are no longer secure. They are completely broken by a powerful enough quantum computer and need to be replaced with quantum-safe security measures.



The vulnerability of symmetric encryption is not as clear as the vulnerability of asymmetric encryption because Grover's algorithm (used on symmetric encryption) provides a quadratic speed up over classical computers, whereas Shor's algorithm (used on asymmetric encryption) provides an exponential speed up. What this means is that Grover's algorithm doesn't completely break all of the symmetric encryption protocols, but it does hamper their security in significant ways.



Protocols like TDEA, or SHA-1, are not considered quantum secure. For example, 2TDEA and 3TDEA will no longer be secure. AES, a very popular symmetric encryption protocol that's used in many security systems, is vulnerable but the risk posed by quantum attack can be mitigated by increasing the key sizes.[NIST] For example, AES-128 has a current security level of 128. After Q-Day, because of Grover's algorithm, the AES-128 security level is just 64. In order to maintain the 128 security level, the key size must be doubled. This approach to mitigating the quantum threat is somewhat easier than it is for asymmetric encryption.

Mitigating the threat of Q-Day for your organization

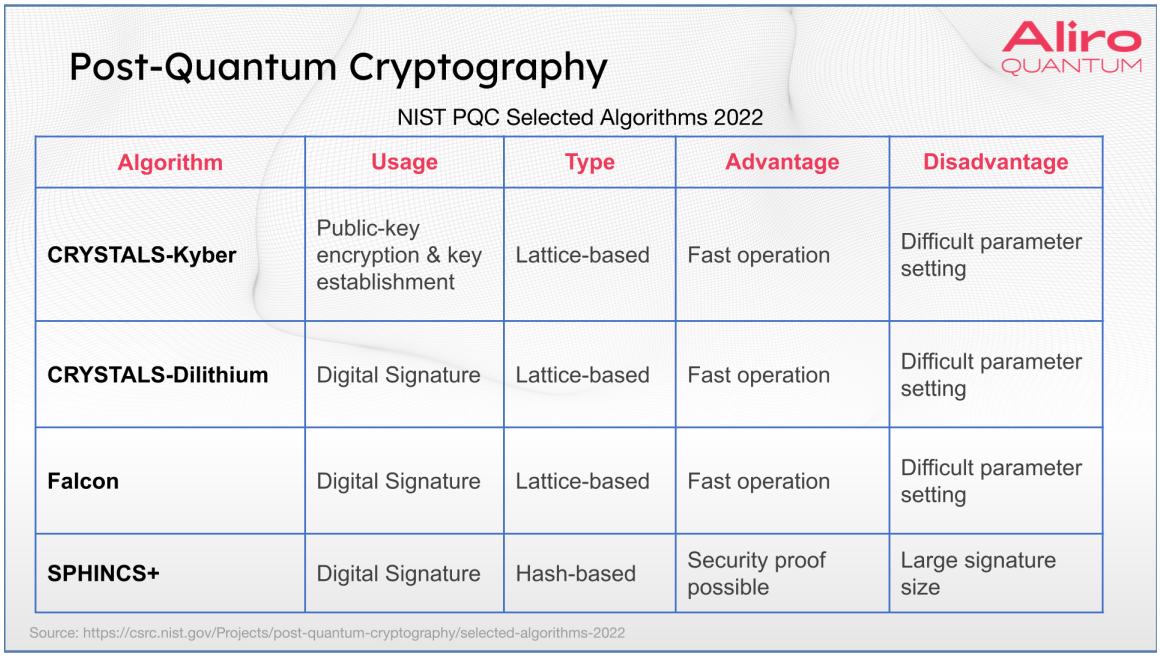
There are three main categories of post quantum cybersecurity: Post Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Secure Communication (QSC).

Post Quantum Cryptography (PQC)

Post Quantum Cryptography aims to replace the existing classical cryptography systems with new classical cryptography systems based on different mathematical problems. The National Institute of Standards and Technology (NIST) is conducting a competition to identify and standardize Post Quantum Cryptography. Those standards are due to be announced sometime next year. The candidates and finalists rely on a novel mathematical approach, sometimes referred to as a lattice-based approach. PQC substitutes the prime factorization problem with this lattice-based approach that is presumed to be difficult for both classical computers and quantum computers to break.

There are pros and cons to PQC. This is a purely classical technology, and therefore can be easier to integrate with legacy infrastructure and existing systems. It's interoperable with the classical bulk encryption and decryption hardware that we use today.[PQC-IBM] However, the security of this approach relies on the assumption that this new math problem is hard to break.

In fact, some of the finalist candidates of the NIST PQC competition have already been cracked - not by a quantum computer, but by a classical laptop.



Post-Quantum Cryptography

Aliro QUANTUM

NIST PQC Selected Algorithms 2022

Algorithm	Usage	Type	Advantage	Disadvantage
CRYSTALS-Kyber	Public-key encryption & key establishment	Lattice-based	Fast operation	Difficult parameter setting
CRYSTALS-Dilithium	Digital Signature	Lattice-based	Fast operation	Difficult parameter setting
Falcon	Digital Signature	Lattice-based	Fast operation	Difficult parameter setting
SPHINCS+	Digital Signature	Hash-based	Security proof possible	Large signature size

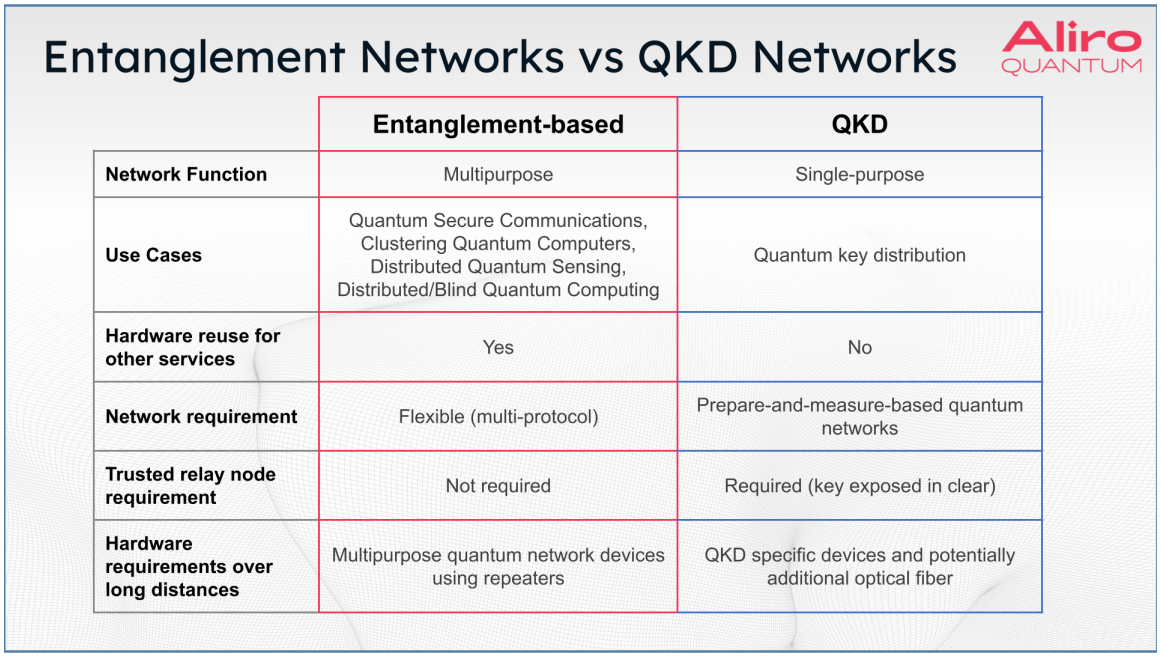
Source: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

Above is a table of the NIST PQC selected algorithms from 2022.[PQC2022] These are the candidates to replace public key encryption for key establishment and for digital signature algorithms as well. Several of these algorithms use a lattice-based approach, and one uses a hash-based approach.

Quantum Key Distribution (QKD)

Quantum Key Distribution uses physics-based security instead of math-based security to protect data. Field trials of QKD have been conducted for decades, and there are commercial off-the-shelf products that you can buy to do quantum key distribution. Many QKD field trials conducted over the past two decades have implemented a protocol called BB84, a quantum key distribution scheme that allows two parties to securely communicate a private key which can then again be turned around and used for symmetric encryption. For example, if Alice were to send Bob a message securely using QKD, Alice would first prepare randomly one of four different kinds of quantum states. In practice, this quantum state will be in a quantum photon. Alice sends this photon, a single particle of light, over to Bob, who will randomly select a basis to measure this quantum state. Alice and Bob will then communicate classically: Bob will communicate back to Alice the basis used to measure the photon, and Alice will keep the the material that matches up with Bob's basis. This means that BB84 relies on a quantum property known as superposition, such that any adversary trying to crack this system, any man-in-the-middle attack, information gain is only possible to that adversary at the expense of disturbing the signal itself. An adversary would not be able to acquire any information about the key without collapsing the system, and Alice and Bob would be aware of that collapse.

Experimentally, QKD has been used on commercial telecommunications optical fiber and over free space optical channels. Products exist today that are capable of implementing QKD.[QKD] However, there is a distance limitation on these networks of approximately 100 km. In order to increase the distance between nodes QKD requires a trusted relay node. The term “trusted relay node” is somewhat misleading, as it refers to the fact that this relay node must be considered trustworthy and doesn’t indicate that it is secured. The relay node must be trusted because the classical key material is going to be exposed in the clear at that node, which creates a significant security issue. In addition, QKD networks can only be used for key exchange. These are single-purpose networks.



	Entanglement-based	QKD
Network Function	Multipurpose	Single-purpose
Use Cases	Quantum Secure Communications, Clustering Quantum Computers, Distributed Quantum Sensing, Distributed/Blind Quantum Computing	Quantum key distribution
Hardware reuse for other services	Yes	No
Network requirement	Flexible (multi-protocol)	Prepare-and-measure-based quantum networks
Trusted relay node requirement	Not required	Required (key exposed in clear)
Hardware requirements over long distances	Multipurpose quantum network devices using repeaters	QKD specific devices and potentially additional optical fiber

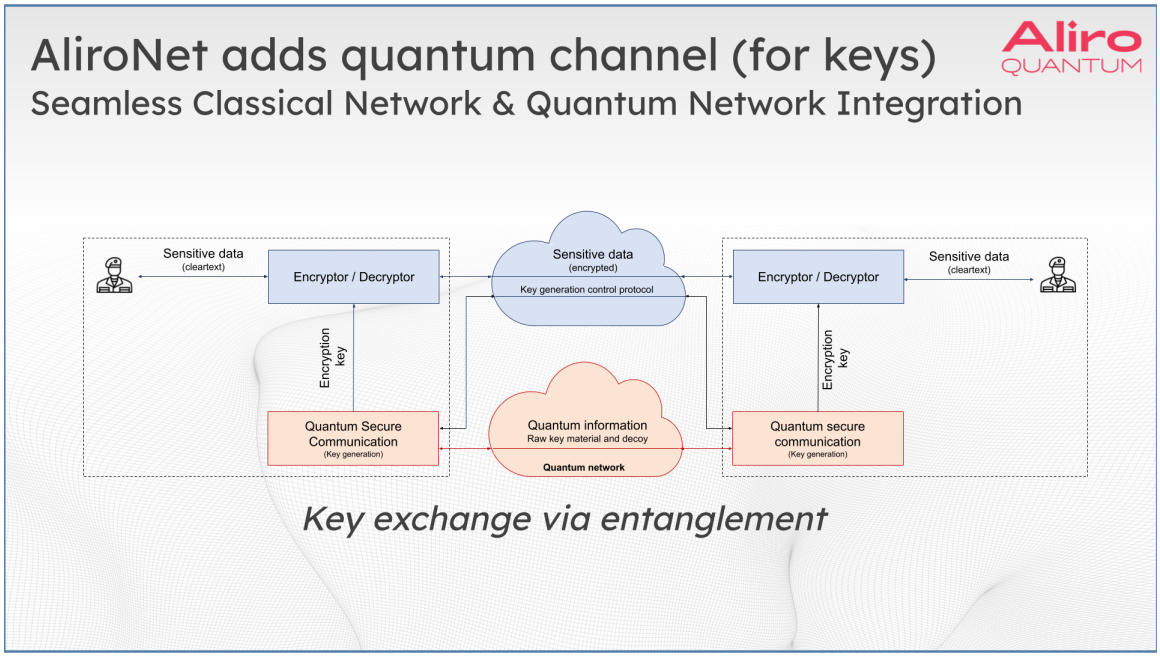
Quantum Secure Communication (QSC)

Quantum Secure Communication also uses quantum technology and the laws of quantum physics to protect from the threats of quantum physics leveraged by quantum computers. This is referred to as physics-based security: instead of relying on the difficulty of a math problem, the laws of quantum physics are used to create secure communication. QSC is the entanglement-based successor to QKD that addresses the weaknesses of QKD.

Quantum Secure Communication is enabled by entanglement-based networks, which can be used for many applications: key distribution, distributed quantum sensing, blind quantum computing, and the Quantum Internet are all made possible by a single entanglement-based network. Another distinguishing characteristic of entanglement-based networks that enable QSC versus QKD networks is that there is no trusted relay node requirement for entanglement-based networks. In QSC, entanglement based-networks do not require any trust through the node because no classical key material is revealed along the network until the entanglement has been generated and distributed to the two parties that want to communicate. Quantum repeaters are used to extend and generate entanglement between two parties. Entanglement is generated end to end, then it is measured, and then it produces key material.

This key material is never exposed at any intermediate node along the way. QSC can be implemented on existing classical networks
Implementing Quantum Secure Communication on a classical network
Most modern networks use a hybrid cryptosystem where asymmetric encryption protocols like RSA and Diffie Hellman perform the key exchange. Then, symmetric encryption such as AES is used to perform the bulk encryption and decryption of the actual encrypted communication between two parties.

In an entanglement-based network used for QSC, quantum key exchange would integrate with the existing system. There's no need to rip and replace the existing networks or the existing communication infrastructure. Only the key exchange process is affected. The initial step of generating and sharing the secret key is now replaced with an entanglement-based network running quantum secure communication protocols. An entanglement-based network will be able to generate and distribute entanglement between two parties, and that entanglement can then be used to produce secure secret keys. Those keys can then be passed up to the legacy classical encryptors and decryptors that are used today. The bulk encryption hardware does not need to be replaced and communication can continue along the classical channel.



Each of these solutions - Post Quantum Cryptography, Quantum Key Distribution, and Quantum Secure Communication - are all interoperable with each other and can help organizations create defense-in-depth. Any adversary would need to break through all these layers of security in order to capture the key.

Closing

Entanglement-based secure networks are being built today by a variety of organizations for a variety of use cases – benefiting organizations internally, as well as providing great value to an

organization's customers. Telecommunications companies, national research labs, intelligence organizations, and systems integrators are just a few examples of the organizations Aliro is helping to leverage the capabilities of quantum networking.

Building entanglement-based quantum networks is no easy task. It requires:

- Emerging hardware components necessary to build the quantum network.
- The software necessary to design, simulate, run, and manage the quantum network.
- A team with expertise in quantum physics and classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro Quantum is uniquely positioned to help you build your quantum network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part of a clear, unified solution already at work in quantum networks like the EPB Quantum Network℠ powered by Qubitekk in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based quantum network solution, consists of the software and services necessary to ensure customers will fully meet their quantum networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal with quantum networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage quantum networks as well as test, verify, and optimize quantum hardware for network performance. AliroNet™ leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment.

Depending on where customers are in their quantum networking journeys, AliroNet™ is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating quantum networks, (2) Pilot Mode for implementing a small-scale quantum network testbed, and (3) Deployment Mode for scaling quantum networks and integrating end-to-end applications. AliroNet™ has been developed by a team of world-class experts in quantum physics and classical networking.

To get started (or continue on your quantum journey), reach out to the Aliro Quantum team for additional information on how AliroNet™ can enable your quantum network.
info@aliroquantum.com
www.aliroquantum.com

For additional information or for any questions you may have about quantum networking or the content of this paper, contact Mike Gaffney at mike@aliroquantum.com or 571.340.1786.

REFERENCES

[DHS] Michael Vermeer., et al. “Preparing for Post-Quantum Critical Infrastructure.” RAND Corporation, 2022. www.rand.org/content/dam/rand/pubs/research_reports/RRA1300/RRA1367-6/RAND_RRA1367-6.pdf

[ENCRYPTION] “Symmetric vs. Asymmetric Encryption – What are differences?” SSL2Buy. https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

[MOSCA] “Quantum computer ready, set, go!” ID Quantique. March 2022. https://www.idquantique.com/quantum-ready-set-go/

[NIST] Elaine Barker. “Recommendation for Key Management.” National Institute of Standards and Technology. May 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[PQC]“Preparing for Post-Quantum Cryptography: Infographic.” Department of Homeland Security, October 2021. https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

[PQC-IBM] “What is quantum-safe cryptography?” IBM. https://www.ibm.com/topics/quantum-safe-cryptography

[PQC2022] “Post-Quantum Cryptography, Selected Algorithms 2022.” National Institute of Standards and Technology. December 2023. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[QKD] A. Carrasco-Casado, V. Fernández, N. Denisenko. (2016). “Free-Space Quantum Key Distribution.” Optical Wireless Communications. Signals and Communication Technology. 2016. https://doi.org/10.1007/978-3-319-30201-0_27

[SUBLINEAR] B. Yan, et al. “Factoring integers with sublinear resources on a superconducting quantum processor.” December 2022. https://doi.org/10.48550/arXiv.2212.12372

[ZAPATA] Yudong Cao, Jonathan Olson. “Variational Quantum Factoring.” August 2018. https://zapata.ai/publications/variational-quantum-factoring/