
Enter
Improving tomorrow's security by decoding the quantum computing threat
EY
Building a better working world
JPMorgan Chase & Co.

Contents

01 How security protocols have evolved

02 How quantum computing will disrupt security protocols

03 How to stay ahead of the curve

01 How security protocols have evolved

Information security is now a fundamental component of IT solutions, encompassing various methods to safeguard data, whether in transit, at rest or during processing. Current protection is based on cryptography, which is the science and practice of keeping sensitive information inaccessible to adversaries. Cryptographic systems not only provide confidentiality – they also provide other security features like authentication, integrity and non-repudiation.

Modern cryptographic systems, while robust, are not infallible. In real-world IT applications, security protocols strike a balance between practicality and security. They operate under unproven assumptions that certain computational problems are hard to solve for state-of-the-art computers in reasonable time. This approach to computational security has been serving the purpose effectively over decades. Such assumptions, however, may not hold water as computer science or technology advances. What is deemed computationally difficult today may tomorrow become more manageable with advances in computing power or new algorithms. Consequently, encryption standards are in a constant state of evolution, adapting to the latest technological developments and breakthroughs. The advent of quantum computing has initiated another review cycle of security protocols. Quantum computing introduces innovative methods to solve complex computational problems, challenging existing security assumptions and exposing vulnerabilities in some security protocols.

This section takes a closer look into security protocols, their assumptions, and their applicability today and in the future – to assist those tasked with securing sensitive information in the quantum computing era.

01 Security protocols

As global digital transformation advances, enterprises increasingly store, process and communicate sensitive data over shared or untrusted infrastructure. In this landscape the need for robust data protection against unauthorized access becomes increasingly crucial.

A security protocol is an application of cryptographic mechanisms and a set of rules and operations designed to ensure their proper functioning to achieve a specific security aim.

Security protocols are based on cryptographic mechanisms, which offer an algorithmic approach to ensuring authentication, confidentiality, non-repudiation and integrity.

- **Authentication** serves as a key process in confirming the identities of parties engaged in communication. This step is essential, whether the interaction involves a user, a server or any other entity, ensuring that all communications occur with legitimate, verified sources.
- **Integrity** provides a means to maintain the original state of data, whether in transit or at rest. It acts as a safeguard against unauthorized alterations or tampering, ensuring that data remains as intended throughout its journey.
- **Confidentiality** provides that data can only be read by the intended recipient. This principle ensures that sensitive information remains private and protected from unauthorized access or disclosure.
- **Non-repudiation** ensures that a sender cannot deny the validity of the message they sent. This is crucial for legal and financial transactions where proof of participation is required.

01 Security protocols

This paper characterizes security protocols as encompassing the use of cryptographic mechanisms across various domains, including but not limited to network, hardware and software. These protocols are implemented across a range of technologies, from storage devices and databases to operating systems and applications. They are relevant to securing data in transit, at rest and during processing.
In different scenarios, unique cryptographic features are required. As cryptographic mechanisms are standardized, security protocols are often assembled in a modular fashion to achieve the necessary functionality.

Security must rely on the confidentiality of the key, rather than on keeping the system's operations obscure.

Cryptography is the practice and study of techniques for securing communication and data from adversaries.

Developing an effective cryptography protocol ranks among the toughest challenges. The playbook for modern cryptosystems traces back to guidelines established by Auguste Kerckhoffs in the late 1800s. One of the cornerstone tenets, known as Kerckhoff's Principle, states: "The cipher method must not require secrecy and should cause no harm if it falls into the hands of the enemy." The essence of this principle underscores that the true security of a cryptosystem hinges on the confidentiality of the key in use rather than keeping its workings obscure. Contemporary cryptography takes this idea a step further: a cryptosystem should remain secure even when its algorithms are public knowledge.

In modern cryptography, algorithms often become public before they are officially standardized. This transparent strategy is championed by organizations such as NIST, BSI and ANSSI. By doing so, they invite scrutiny from a broad spectrum of experts — enthusiastic cryptographers, academics, and industry practitioners. This collective vetting serves a critical function of helping uncover design flaws at an algorithm's early stages. Consequently, a widely reviewed algorithm is significantly less likely to contain undiscovered vulnerabilities, although they may remain.

To provide some historical context, even well-accepted algorithms like DES and SHA-1 had design flaws that were only discovered after their widespread adoption. Read more on page 18 below.

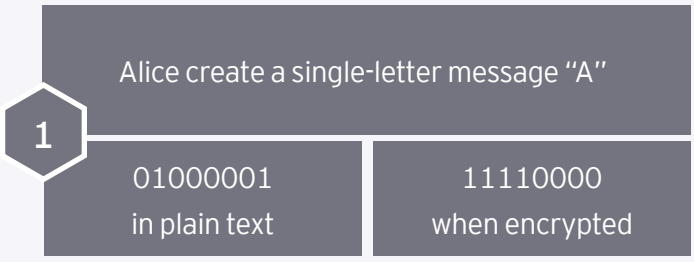
01 Security protocols

In contemporary cryptography, a paramount benchmark entails cryptosystems that remain "provably secure" even when challenged by adversaries with arbitrarily large computational abilities. Such systems sometimes earn the title of "perfectly secure" or "information-theoretically secure". For example, a message encryption scheme will be perfectly secure when the encrypted message reveals no hints about the initial plaintext to potential interceptors. The One-Time Pad stands as a provably secure representation of this ideal cipher.

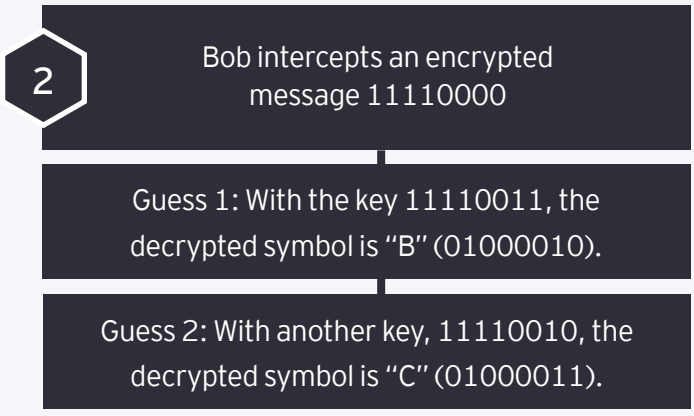
While these information-theoretically secure systems are highly attractive from a cryptographic standpoint, they come with significant practical limitations. Specifically, the key used for encryption must be as long as the sum total of all messages ever encrypted with it. Unfortunately, distributing such a large key poses its own set of challenges.

Computational security aims to overcome the practical shortcomings of information-theoretically secure systems. By slightly lowering the bar on security requirements, computational security aims to protect against efficient, real-world adversaries rather than theoretical ones with arbitrarily large computational resources. A system under this framework is considered secure if an adversary, operating within realistic computational limits – known as "probabilistic polynomial time" – has only an infinitesimal chance of successfully breaking the scheme.

Ever wondered why the One-Time Pad is touted as perfectly secure? We will not dive into the mathematical proofs but share some insights to help illustrate the concept.



Let's say a sender, Alice, wants to send a single-letter message, "A". In ASCII code, "A" is represented as 01000001. Alice selects a random key, 11110000, that is the same length as her message – 8 bits for both. She then uses the XOR operation to combine the message with the key, resulting in the encrypted message 10110001. Importantly, the encryption algorithm is public information and not a secret. Alice only keeps the key as a secret.

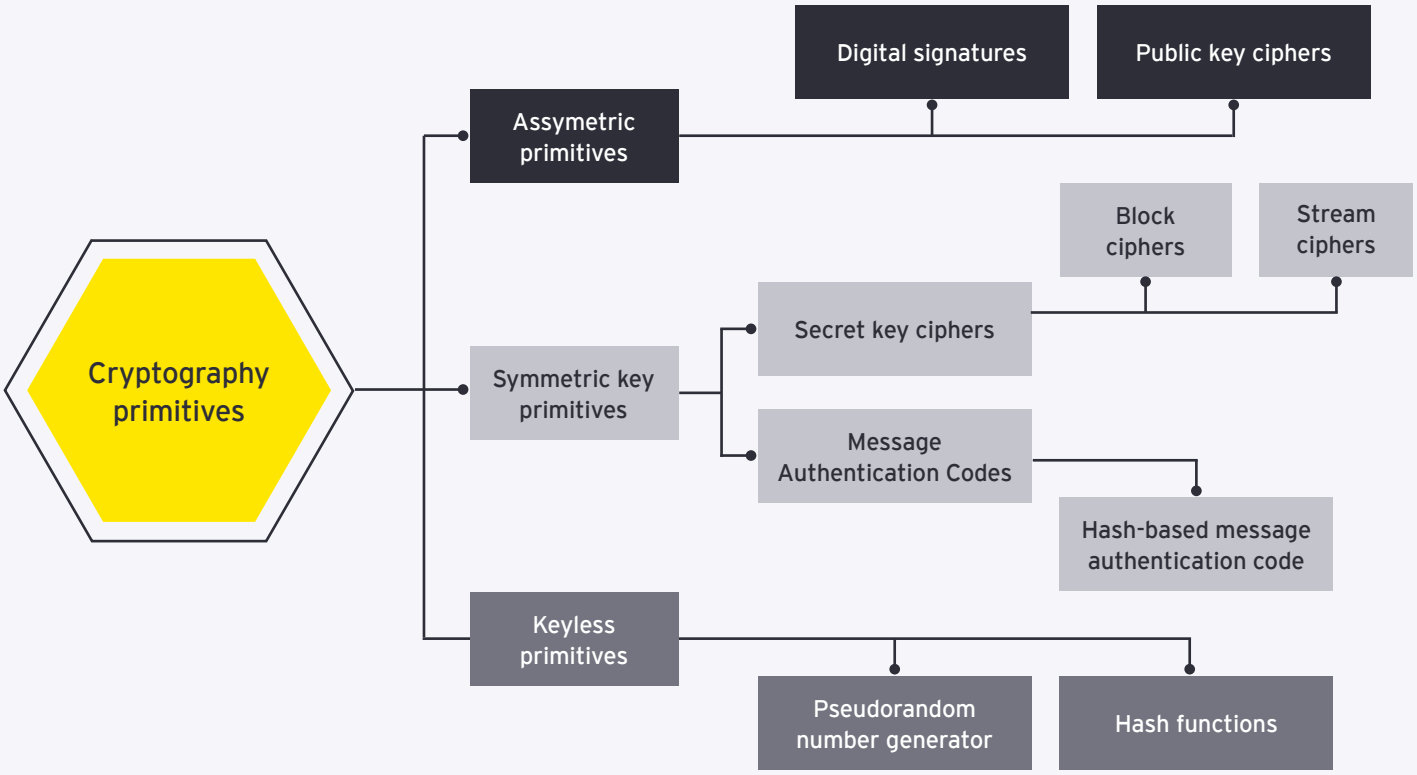


Then imagine an intruder, Bob, intercepts this 8-bit encrypted message and attempts to decrypt it without having any knowledge of Alice's secret encryption key. Given the short length, he can easily run through all possible keys in a matter of seconds. As he iterates through all possible keys, he finds that every possible ASCII character can be generated. Since the length of the original message matches the length of the key, Bob's decryption efforts lead to every possible outcome, providing him with zero clues about the original message.

The principle behind the One-Time Pad's "perfect security" lies in the key's length being equal to the message length, which makes decryption a futile guesswork exercise.

01 Security protocols

Cryptography algorithms are unique among security measures, with their exclusive focus on protecting information assets through various mathematical techniques. Given the diversity of security needs, a one-size-fits-all approach to cryptography is infeasible; instead, tailored primitives are employed to serve specific purposes.



Symmetric key primitives utilize a single secret key, often referred to as a master key, for both encrypting and decrypting data. Typically, the actual encryption employs the master key indirectly. The master key derives what are called "round keys" for the encryption process. By using unique keys in each encryption round, vulnerabilities to pattern recognition in the ciphertext are minimized, making it harder for attackers to decipher the original message. However, should the master key fall into the wrong hands, all derived round keys become vulnerable. While symmetric key systems are faster and thus require less computational power than their asymmetric counterparts, they do present challenges, particularly in master key distribution and management.

Asymmetric key primitives use a pair of related keys: a public key, which can be shared openly, and a private key, which remains secret. Data encrypted with one key can only be decrypted with its counterpart. It facilitates secure communication between parties without prior key exchange (over open channels), but it is more computationally intensive than a symmetric key system.

Keyless primitives use cryptographic mechanisms that don't rely on secret keys. Random number generators are crucial for generating the unpredictable, statistically random sequences used in creating cryptographic keys. Hash functions are useful for data integrity checks and verifying the authenticity of data without revealing the data itself.

While this paper primarily concentrates on symmetric and asymmetric primitives, the inclusion of keyless primitives aims to provide a comprehensive overview for the reader.

01 Security protocols

Each kind of cryptographic primitive has unique characteristics and purposes. In production environments, these primitives often work together to form a comprehensive security protocol. For instance, the Transport Layer Security (TLS) 1.3 protocol, below, utilizes public key ciphers to facilitate secure key exchanges between the server and the client, employs symmetric ciphers for encrypting the data during transfer and uses hash functions to ensure the integrity of that data.[1]

Client Hello	**Random numbers**	The client initiates the handshake by sending a Client Hello message to the server. This message includes the TLS version, a random number called the "client random", and a list of supported cipher suites.
Server Hello	**Random numbers**	The server responds with a Server Hello message. It selects the TLS version, cipher suite and other parameters for the connection. The server also sends its own random number called the "server random".
Key Exchange	**Public key ciphers**	The key exchange is performed using a mechanism called Elliptic Curve Diffie-Hellman (ECDH). The client and server exchange key share messages, which allow them to compute a shared secret without transmitting the secret over the network.
Authentication	**Public key ciphers and digital signatures**	The server sends its certificate (containing its public key) to the client. Upon reciept the client validates the server's certificate, checks it against trusted Certificate Authorities, ensures the server's identity matches and then uses the server's public key to verify the digital signature to confirm the authenticity of the server.
Encryption	**Block ciphers and hash functions**	Once the shared secret is established, the client and server use it to derive the session keys for encrypting and decrypting data. The "TLS_AES_128_GCM_SHA256" cipher suite is used by default, which provides authenticated encryption and integrity protection.
Final Message	**Hash functions**	Both the client and server send a Finished message to confirm that the handshake is complete. This message includes a hash of the entire handshake process, ensuring its integrity.

01 Security protocols

Symmetric, asymmetric and keyless primitives have their foundation in different security proofs. A security proof is a formal argument demonstrating that a cryptographic scheme achieves specified security goals against adversaries of a certain computational power under defined mathematical assumptions or the assumed security properties of its building blocks.

For **asymmetric primitives**, a common approach is to build the proof on a mathematical challenge that is assumed to be hard.[2] Those challenges are not only hard but also one-directional: easy in one direction and daunting when reversed. Essentially, the keyholder can execute a straightforward task while any attacker grapples with its complex counterpart.

An example is the factorization problem, which operates on the assumption that, while multiplying numbers is straightforward, reversing this process — specifically, determining the prime factors of a large composite integer — is computationally challenging. Similarly, the discrete logarithm problem is premised on the ease of calculating powers of a number g within the confines of a particular mathematical group defined by a prime number p, yet finding the original exponent in this context, known as computing the discrete logarithm, is a complex task.

The perceived difficulty of these challenges stems from computational complexity theory. As this theory evolves or as new methods emerge, some of the foundational assumptions might be upended, potentially jeopardizing the security of cryptographic systems.

For **symmetric primitives**, a common approach is to build the proof by assuming that a cipher exhibits some specific security properties considered robust. The two most typical properties are pseudorandom permutation (shuffling symbols) and pseudorandom function (substituting symbols). Both concepts utilize the idea of creating something that seems random and unpredictable unless the secret key is present.

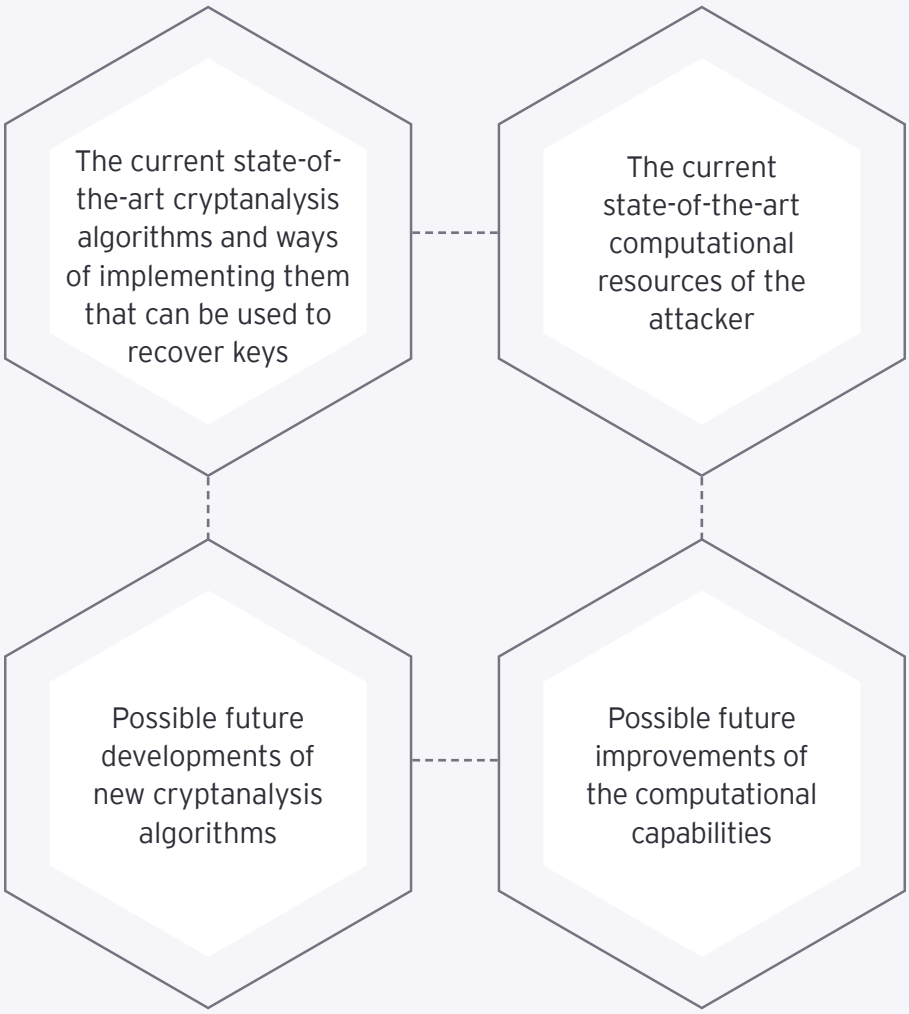
- A pseudorandom permutation rearranges symbols in a seemingly random order, but in a way that can be reversed with the correct key.
- A pseudorandom function replaces symbols with others based on a seemingly random process, which is consistent and reversible for someone with the correct key.

Once elements of a message are shuffled and substituted, it must be computationally infeasible to distinguish this encoded message from a truly random sequence and thus reverse the transformation.

These security properties are based on empirical outcomes. It is not proven that the challenges underpinning these properties are hard, but attackers are just unable to decrypt a message. Despite decades of research, an efficient attack algorithm has yet to be discovered.

Given the inherent computational security of cryptographic schemes and their foundational reliance on assumptions, the selection of key length evolves into more than a mathematical endeavor — rather, it becomes a predictive exercise for the future. Ensuring the appropriateness of key length is pivotal. While shorter keys may be simpler to implement owing to their reduced demand on computational resources, opting for an arbitrarily large key, albeit secure, may pose implementation challenges, thereby necessitating a balanced approach.

Selecting the appropriate key length is, by no means, a straightforward task. Determining key size should be contingent upon appropriate consideration of four interconnected factors, though this list is not exhaustive, and there may be additional relevant points:[3]



Standardization authorities, such as NIST[4], BSI[5] and ANSSI[6], suggest key lengths designed to withstand adversary attacks for several hundred years. These recommendations are periodically updated to account for shifts in factors influencing the security of specific cryptographic protocols.

Since cryptographic systems operate based on certain assumptions, there's always the possibility that one could identify and exploit a vulnerability.

Ciphers emerged from a fundamental need to safeguard information. However, as soon as they were created, individuals with an interest in uncovering secrets began devising ways to decipher encrypted messages. Given that cryptographic systems are predicated on specific presuppositions, a chance exists that an individual could discover and leverage a flaw. Indeed, history has shown us that this has occurred numerous times. Thus, the field of cryptoanalysis was born. It delves into the intricate study of cryptographic systems, aiming to identify potential weak points that might allow someone to decode a message without having the original key.

Computational power growth risk

Computationally secure ciphers, despite their strength, remain susceptible to brute-force searches across the key space. Conducting a brute-force search can be a time-intensive process. However, computational power has consistently grown, adhering to Moore's law, which in turn diminishes the time required for brute-force attempts. By Moore's estimation, the computing capacity available for a given cost doubles approximately every 18 months. Given this projection, to safeguard a data packet for two decades, the key length should increase by a minimum of 14 bits compared to what's necessary for protection against present-day attacks.[7]

As a case in point, the DES symmetric key cryptography protocol, boasting a 56-bit master key and standardized by FIPS in 1977, succumbed to a brute-force attack by 1999.

Mathematical advancements risk

Computationally secure methodologies fundamentally rely on assumptions regarding the intricacies of specific tasks. Occasionally, advancements lead to more efficient strategies. Predicting these innovations is inherently challenging without a clear metric for gauging longevity. Over time, both symmetric and asymmetric cryptography protocols, along with hash functions, have demonstrated vulnerabilities to fresh techniques.

A prominent illustration is the advent of the Number Field Sieve technique, used for integer factorization and discrete logarithm computations, which notably diminished the robustness of the RSA and DH cryptosystems.

Adversaries can be categorized as either passive or active. Also, attack scenarios targeting encryption schemes can be broken down into several distinct types.

Passive adversaries

These adversaries are characterized by passively observing communication packets. What makes them particularly elusive is their non-intrusive nature; they leave the communication channel undisturbed, making detection challenging.

1

Ciphertext-only attack

Adversaries employing this tactic capture and store encrypted packets from public communication channels, trying to deduce the original plaintext from them.

2

Known-plaintext attack

This approach involves a more adept adversary who possesses knowledge about certain plaintexts that match up with intercepted ciphertexts encrypted with the same key. Their objective is to decipher other ciphertexts for which the original plaintext remains unknown.

Active adversaries

These adversaries are characterized by having access to either the encryption system or both the encryption and decryption systems. Such access provides an additional advantage and could be employed to deduce information helping in the attack.

1

Chosen-plaintext attack

In this attack, adversaries can obtain the encryption of any selected plaintext. Their goal is to decipher a different ciphertext and determine its original plaintext.

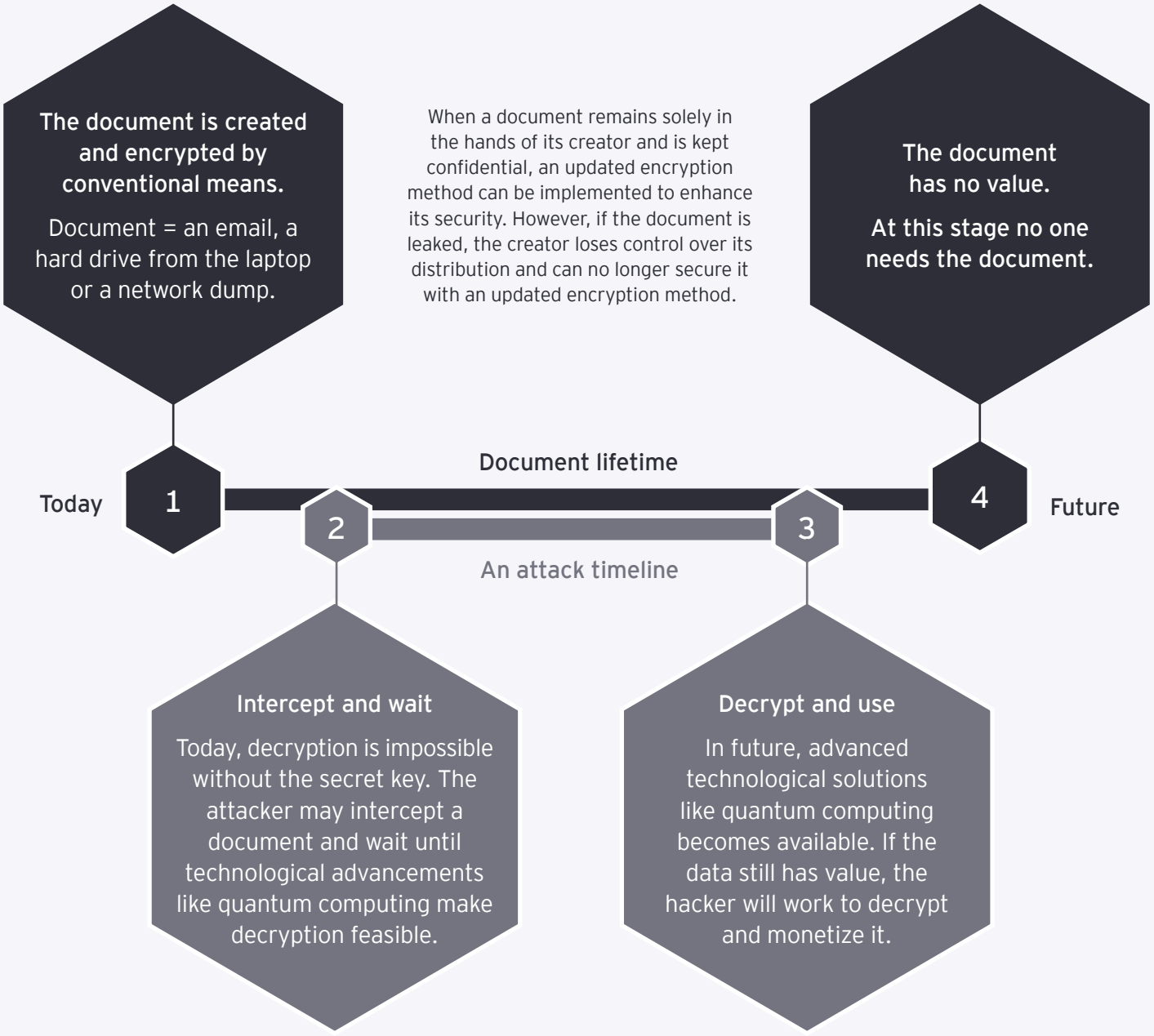
2

Chosen-ciphertext attack

In this attack, adversaries have the means to obtain the decryption of any selected ciphertext. Their goal is to determine the original plaintext of another ciphertext, one they are unable to directly decrypt.

Both passive and active adversaries might utilize a strategy rooted in the time value of information. While current techniques may be unable to break encryption methods, the evolution of technology and knowledge may enable future decryption methods before the intercepted information loses its value. This method is called "Harvest now, decrypt later".

Cybercriminals weigh costs against benefits. They typically target data with enduring relevance, preferring datasets encrypted with a single key, to maximize potential returns from a single decryption attempt.



While it may seem that intercepting certain information is implausible, or that its layers of encryption and complexity deter decryption, the actual scenario could be more concerning.

Revisiting the TLS protocol provides insight into a potential "harvest now, decrypt later" attack. During the key exchange phase of the TLS protocol, the server and client utilize a public key protocol to agree on a master key. Subsequently, this master key aids in producing further shared keys through a symmetric key cryptography protocol, encrypting messages with the newly generated keys. Even though messages are encrypted with unique keys, they are derived from the master key.

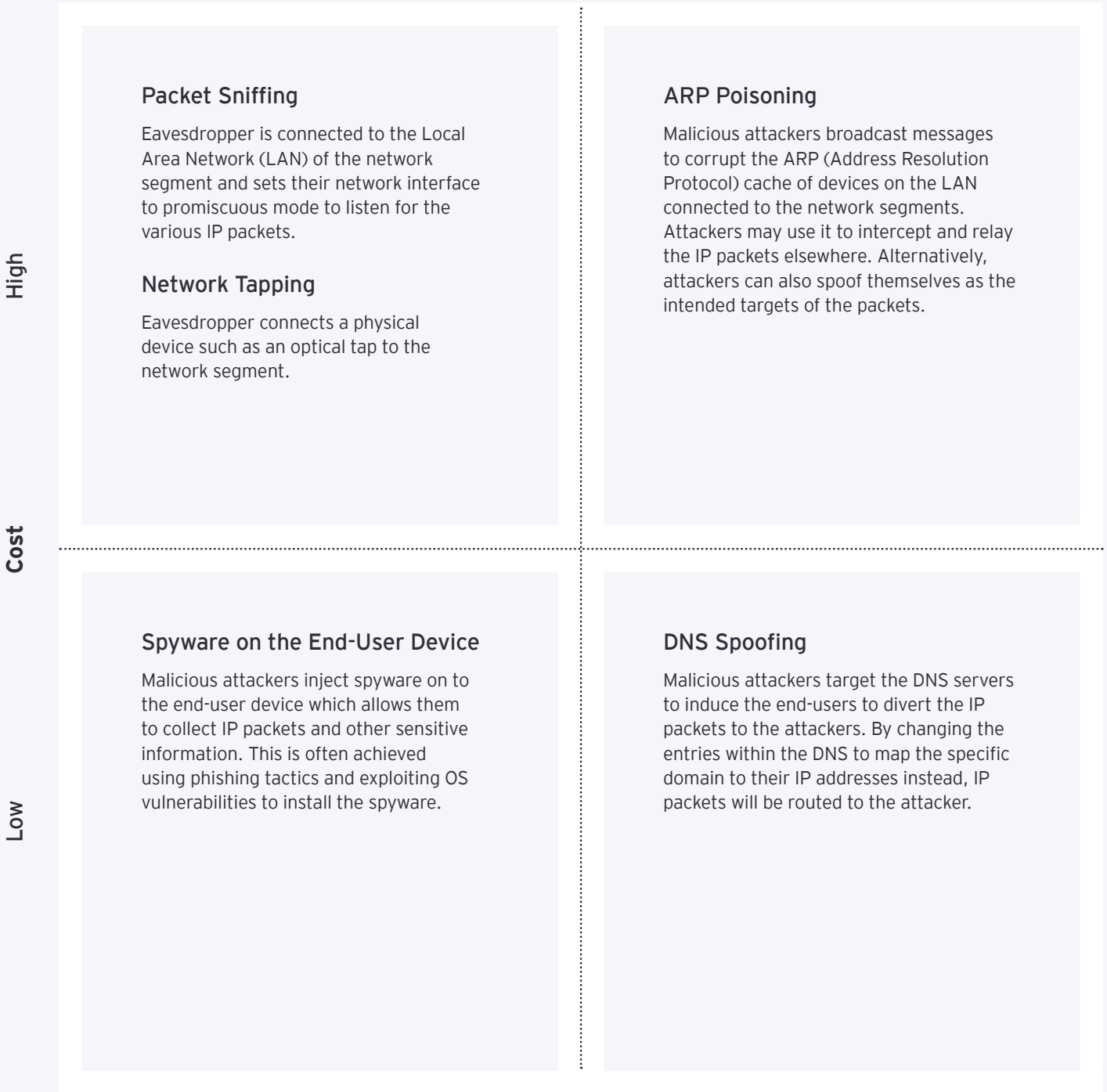
A basic passive adversary can intercept both the encrypted data packets and those pertaining to the master key exchange. At a later time, this adversary might attempt to recover the master key by compromising the public key scheme employed for the key exchange. Once the master key is compromised, the adversary has the means to determine the encryption keys for all data packets, enabling decryption of all intercepted packets. This scenario represents a straightforward harvesting approach, assuming an adversary is executing a ciphertext-only attack.

In the "harvest now, decrypt later" attack strategy, attackers generally pin their hopes on two primary decryption avenues.

First, they anticipate a surge in computational power, allowing them to cycle through all potential cryptographic keys swiftly and eventually pinpoint a key to decrypt a message. To guard against this, cryptography algorithm creators often turn to an empirical Moore's Law, offering a gauge on the growth of computational prowess. However, this doesn't account for unexpected advancements in innovative hardware.

Second, they wait for evolving knowledge to challenges existing security proofs. As previously highlighted, these security proofs largely operate on the premise that certain tasks are challenging without concrete mathematical evidence, deeming them outright impossible. If, for instance, a new algorithm emerges capable of factoring numbers, then algorithms built on this foundational belief would be rendered insecure.

For the attack strategies mentioned earlier, adversaries must access the physical infrastructure to intercept data packets. Many methods to obtain these packets exist, and some are surprisingly straightforward to implement.



01 Security protocols

Switching to a new cryptography protocol is often a lengthy process. The complexity arises from the broad spectrum of applications for cryptography protocols and the increased coordination efforts required when multiple independent entities are involved. Historically, the transition to new cryptography protocols has proven to be a significant challenge — as highlighted by the examples below.

DES

The DES algorithm, for instance, was identified as being vulnerable to brute force attacks as far back as 1999.[8] With specific hardware, it was possible then to retrieve the key within days. This algorithm found its place in numerous protocols for an extended duration. While the more secure AES has been available since 2001, many contemporary protocols still employ a DES variant known as triple DES. Over the past two decades, triple DES has demonstrated several vulnerabilities. These can potentially be exploited for more advanced attacks in the future.

SHA-1

In 2015, researchers from China highlighted a theoretical collision attack on the popular hash function, SHA-1. The real world witnessed its first successful collision attack on SHA-1 in 2017.[9,10] Intriguingly, many web browsers accepted SHA-1 certificates until early 2017, despite the presence of a more secure alternative, SHA-2, from 2001. Transitioning to this safer option took nearly two decades.

RSA

Since its inception in 1977, the RSA algorithm's minimal key length recommendations have undergone multiple revisions. These changes were spurred by advancements in prime number factoring techniques. Notably, no such advancement, aside from the Shor's algorithm covered in the next section, has successfully scaled to accommodate increasingly larger numbers. As a result, enhancing security has been less about altering the algorithm and more about extending its key length. Case in point: in 2020, factorizing an 829-bit number rendered RSA packets encrypted with shorter keys ineffective.[11]

02

How quantum computing will disrupt security protocols

Security protocols have long relied on computational assumptions, which have proven effective for decades. These assumptions were carefully chosen and have largely withstood developments in classical computing power and new mathematical techniques. However, quantum computing has challenged these assumptions, jeopardizing the security of many cryptosystems. Contrary to some perceptions, quantum computing has not introduced new risks to cryptography or data security. Instead, it has illuminated and intensified existing vulnerabilities, enabling certain attacks to gain prominence.

Quantum computing is not yet fully mainstream and currently unable to break security protocols with the key length recommended for use by standardization agencies. However, there are pressing reasons to be vigilant now. The last decade has witnessed not just advancements in quantum hardware but also significant progress in quantum algorithms aimed at breaching cryptographic protocols. Additionally, considering the time value of data – the idea that security protocols must protect information throughout its entire lifecycle – emphasizes the urgency of transitioning to quantum-safe solutions. Consider the "harvest now, decrypt later" strategy: previously, it hinged on the hope of a significant computational breakthrough. Today, it leans more toward quantum computing based attack. Secrets currently protected by conventional cryptographic algorithms could be at risk, stolen now only to be exposed in the future.

Not all cryptographic systems respond to quantum threats in the same way. They're built on varied assumptions, which means their resilience to quantum computing varies. As this section discusses, asymmetric cryptographic algorithms will need a complete overhaul, while symmetric ones will need an increase in key length used.

Quantum computing represents a fresh paradigm in computation, offering solutions to problems once deemed insurmountable. However, this innovation also poses significant challenges to the security foundations underpinning contemporary cryptographic algorithms.

Quantum computing utilizes principles of quantum mechanics to solve complex problems beyond the reach of classical computers. It uses qubits as basic units of information. Qubits have intrinsic properties, like superposition and entanglement, that enable quantum computers to process vast amounts of information simultaneously. This makes them exceptionally powerful for certain types of calculations, including optimization and algebraic problems, and quantum simulations.

Despite the great potential of quantum computing, several challenges need to be addressed before practical, large-scale quantum systems can become a reality. A primary challenge is that quantum states are extremely delicate. Environmental disturbances can result in rapid information loss.

The journey toward unlocking the benefits of quantum computing encompasses several pivotal milestones:

1. The attainment of **Quantum Advantage**, stands for the development of a quantum computer coupled with a pertinent algorithm that can help solve a real-world problem that would been otherwise slower with classical computers. These issues may have restricted practical applications. Several companies[12,13] have recently staked claims to such achievements.

2. The creation of a **Cryptographically Relevant Quantum Computer**, a device and accompanying algorithm with the power to compromise widely employed cryptographic protocols configured and used in production IT environments.

3. The development of a **Fault-Tolerant Quantum Computer**, a quantum computer with sufficient capacity to outperform even the highest-performing classical computers in commercial applications. The timeline for developing this computer may or may not align with the development of the Cryptographically Relevant Quantum Computer.

Quantum computing poses a significant threat by potentially invalidating the security proofs of existing cryptographic algorithms. When classic cryptography methods were crafted, the advent of quantum computers was largely unforeseen. As the quantum age unfolds, many foundational assumptions of contemporary cryptography will be challenged.

Shor's algorithm — threat to asymmetric primitives

In 1994, Peter Shor introduced an innovative quantum algorithm, executable only on a quantum computer, capable of identifying prime factors of vast numbers with far greater efficiency than traditional algorithms — requiring resources proportional to the polynomial in the key length.

The bedrock of RSA, a commonly employed public key cryptosystem, rests on the belief that no probabilistic polynomial-time (PPT) adversaries can discern prime factors of a sizable number. Shor's algorithm challenges RSA's core computational hardness assumption, leaving systems like these highly susceptible.

An extension of Shor's algorithm threatens the computational foundations of other public-key cryptosystems, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman.

Grover's algorithm — threat to symmetric primitives

In 1996, Lov Grover presented a quantum algorithm, tailored exclusively for quantum computers, that can search an unsorted database or solve black-box computational problems with speed markedly faster than any classical algorithm — it achieves a quadratic speedup over conventional methods.

The cornerstone of many cryptographic constructs, particularly symmetric key algorithms like AES, hinges on the idea that an adversary would need to search through half the possible keys, on average, to find the correct one. Grover's algorithm, however, can accomplish this feat with only the square root of the total number of keys, effectively halving the key length's security.

As of now, no existing quantum computer is capable of executing these formidable attacks. It's a matter of debate when a quantum machine of such prowess will emerge. Yet, considering the ongoing advancements in quantum computing, standardization agencies like NIST, BSI and ANSSI are pivoting toward quantum-resistant cryptography.

In data security, multiple diverse cryptographic primitives (encryption, hash functions, digital signatures) work in tandem to safeguard data. As they are based on different security assumptions, they are differently impacted by quantum computing.

Insecure, must be replaced with quantum-safe solutions

Asymmetric Primitives

Digital signatures

Public key ciphers

Current asymmetric primitives secure data based on the principle that certain tasks, such as identifying prime factors of substantial numbers, are computationally challenging given a polynomial resource limit. Yet, executing Shor's algorithm has demonstrated its capability in this area rendering classic asymmetric primitives insecure. Asymmetric cryptography algorithms should, therefore, be replaced with quantum-safe cryptography counterparts.

Secure if properly configured

Symmetric and Keyless Primitives

Hash functions

MACs

Secret key cipher

Quantum computing does not render hash functions and symmetric encryption primitives entirely obsolete; however, given Grover's algorithm, certain modifications need to be introduced to ensure continued security. Hash functions must be redeployed with larger output sizes. Symmetric encryption algorithms must employ longer key lengths to maintain their security.

Secure, could be improved

Keyless Primitives

Random number generators

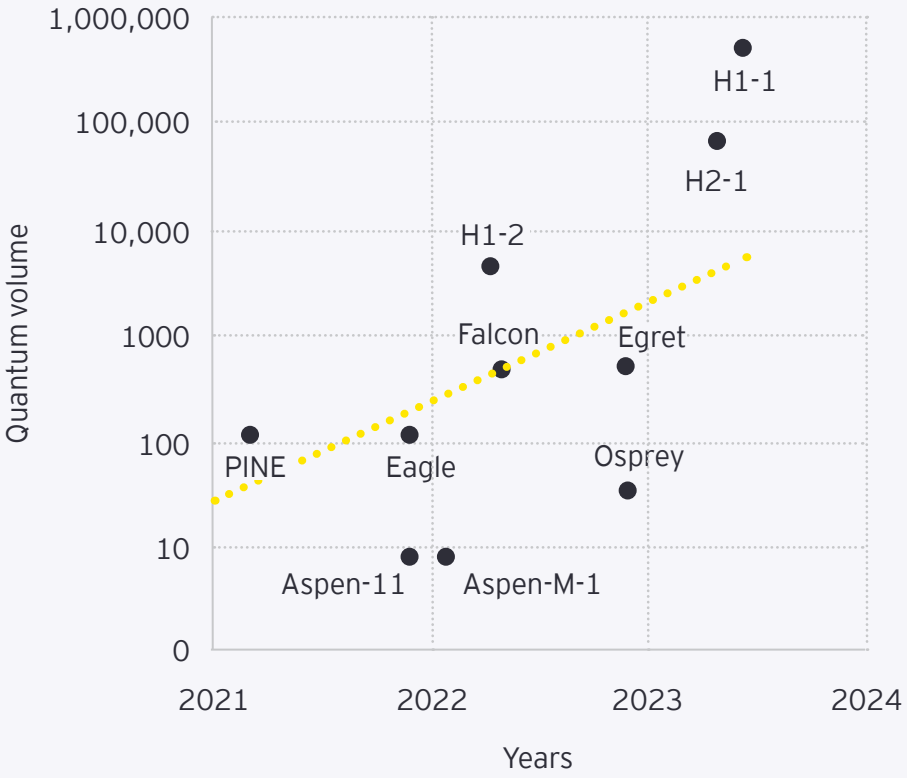
Currently, there is no direct evidence suggesting that quantum computing poses a threat to random number generators.

A key metric in assessing the risk posed by quantum computers is the combination of hardware capacity and the progression of algorithms that can breach encryption. Quantum hardware has been constantly improving over the last decade. On the algorithm side, since the advent of the renowned Shor's algorithm, there have been notable enhancements and innovative concepts introduced.

Evaluating the capacity of quantum computing is challenging. This field is composed of various quantum computing implementations, including superconducting qubits, neutral atoms, cold atoms and photonic devices, each with distinct properties and advantages.

The basic method to gauge capacity is by counting the number of qubits. However, this simplistic approach often leads to misleading outcomes, as it overlooks critical factors like qubit coherence time, 1 and 2 qubit operations and system connectivity. To address these shortcomings, several alternative methods have emerged, such as quantum volume, circuit layer operations per second, among others. These metrics provide a more nuanced performance measure across different devices, albeit with their own set of limitations.

For the purpose of describing the progression of quantum computing hardware performance, the metric of quantum volume offers a more comprehensive insight compared to merely counting physical qubits.



Quantum computing systems have not yet reached the necessary capacity to execute an attack on production-used cryptographic algorithms. However, the expansion of quantum volume demonstrates the growth trend in the computational prowess of quantum computers.

The quantum volume graph above is based on the availability of data about the processor's quantum volume. The team did not run an independent quantum volume assessment. Resources [14, 15, 16, 17, 18] have been used to generate the quantum volume graph.

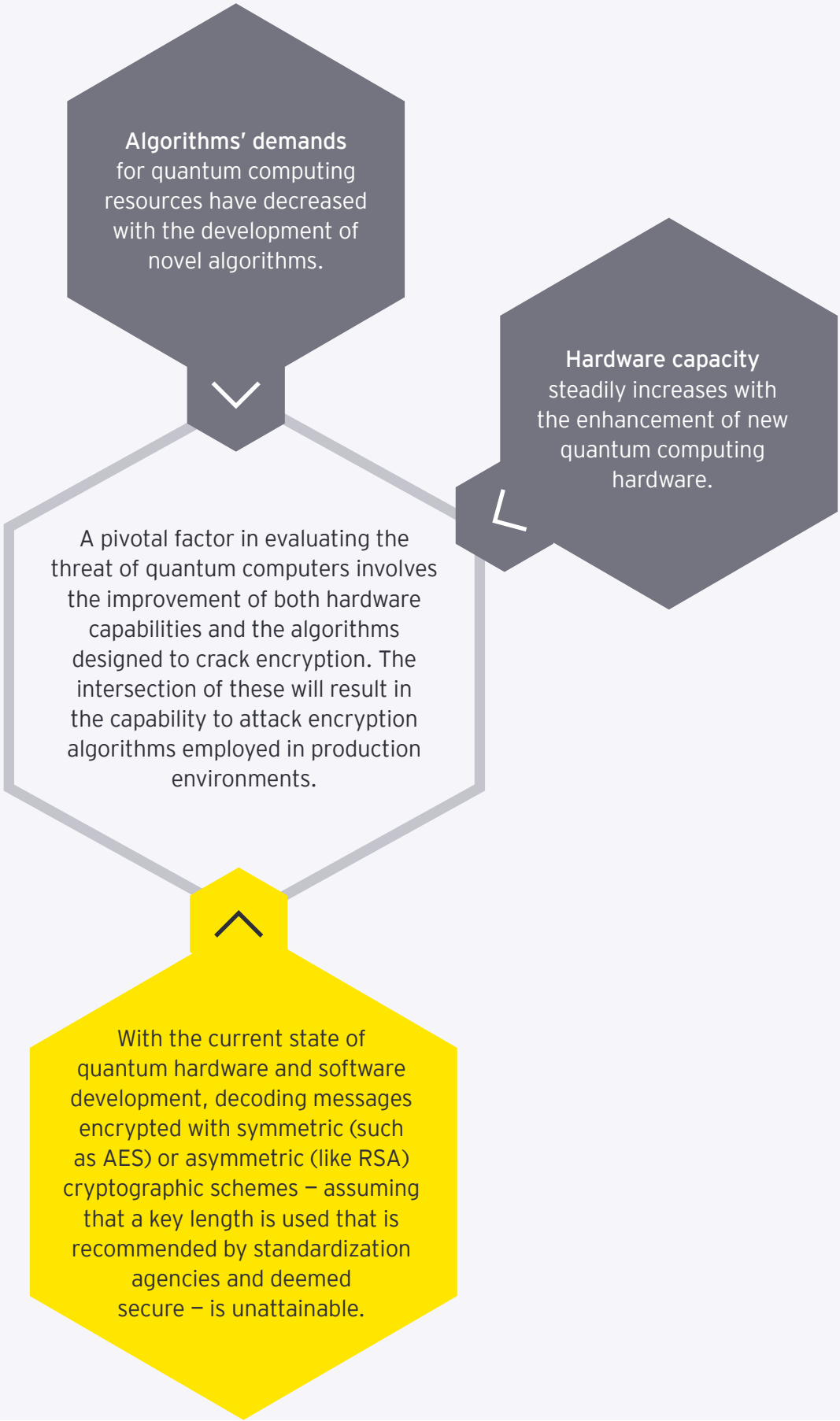
To demonstrate quantum computing offensive capabilities, an attack on an RSA 2048 scheme is often used. Once a successful attack could be shown against this algorithm, the approach could be adjusted and implemented against other asymmetric schemes. This is possible because mathematical problems underpinning various asymmetric algorithms could be reduced to the same problem that quantum computing attacks. The following table demonstrates reduction in resources over time needed to attack an RSA 2048-bit scheme.

		Capacity Logical qubits	**Workload** Megaqubitday
2002 Beauregard[19, 20]	A circuit for Shor's algorithm implementation	4,099	380,000
2012 Fowler et al[19, 21]	First workable method to break RSA encryption.	6,144	850
2019 Gidney, Ekera[19]	A method that optimizes both the overall count of modular multiplications and the cost per multiplication	6,157	5.9

- The number of logical qubits is the mainstay for algorithms to operate. Logical qubits, composed of one or more physical qubits, possess the potential for error correction and often exhibit extended coherence times compared to their physical counterparts. Depending on the error correction code, the number of physical qubits needed to implement a logical qubit varies. The recent experimental demonstration[22] of the quantum error-correcting code can improve the quality of the logical qubits and accelerate the development of cryptographically relevant quantum computers.
- The quantum computing workload, measured in megaqubitdays, relates to the duration of the program. This metric provides insight into the time a device with a given number of qubits will need to mount an attack.

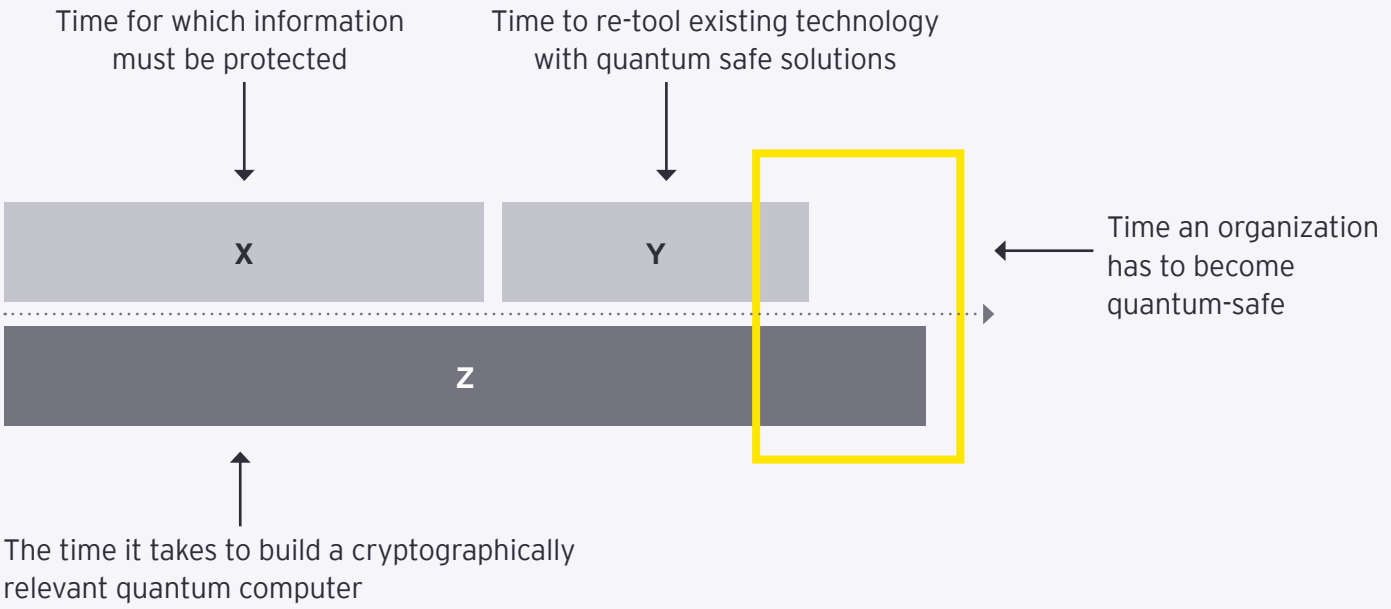
Recently, a multidimensional enhancement to Shor's algorithm was introduced by Oded Regev.[23] Regev's algorithm streamlines the process by decreasing the quantity of basic logical operations needed. When decomposing an n-bit number, Regev's algorithm requires a number of steps proportionate to power of $N^{1.5}$, compared to the N^2. requirement of the original Shor's algorithm. Although the entirety of the algorithm may not exhibit a faster runtime, the acceleration of the quantum segment due to fewer necessary steps could substantially ease its implementation in practical settings. However, the duration of a quantum algorithm's execution is only one aspect of its overall efficiency. Shor's original algorithm necessitates a linear relationship of qubits to the number of bits, n, in the number being factored. In contrast, Regev's method requires $N^{1.5}$ qubits. This distinction becomes increasingly substantial when dealing with numbers comprised of 2,048 bits in length.

Beyond the deterministic approaches previously discussed, various heuristic strategies have also been introduced to challenge the RSA algorithm. One notable method is the Variational Quantum Factoring (VQF) algorithm,[24] which reframes the factoring problem as an optimization challenge, subsequently leveraging optimization algorithms for solutions. To tackle a 2048-bit RSA algorithm, the VQF method necessitates roughly 6000 physical qubits. However, since this technique remains heuristic and untested on the prime numbers integral to RSA 2048, its effectiveness in this context is not guaranteed.


Algorithms' demands for quantum computing resources have decreased with the development of novel algorithms.
Hardware capacity steadily increases with the enhancement of new quantum computing hardware.
A pivotal factor in evaluating the threat of quantum computers involves the improvement of both hardware capabilities and the algorithms designed to crack encryption. The intersection of these will result in the capability to attack encryption algorithms employed in production environments.
With the current state of quantum hardware and software development, decoding messages encrypted with symmetric (such as AES) or asymmetric (like RSA) cryptographic schemes – assuming that a key length is used that is recommended by standardization agencies and deemed secure – is unattainable.

Although a cryptographically relevant quantum computer and a corresponding attack algorithm might be years away, there are pressing reasons to start planning now.

Over the past decade, advancements to compromise cryptographic security have increased the viability of the "harvest now, decrypt later" strategy. Previously, this strategy hinged on the hope of a significant but unknown computational or mathematical breakthrough. But today, quantum computing's capability to solve mathematical problems underpinning critical algorithms provides a direct line to decryption capabilities.



Mosca's equation, as illustrated in the preceding diagram, establishes a link between the timeline for developing a cryptographically relevant quantum computer and specific organizational characteristics. This equation highlights an organization's "safety gap" on the journey toward quantum safety. The crux of the theorem spans from the need to safeguard data throughout its entire lifecycle. Thus, the selection of corresponding cryptographic tools is critical to ensure security for as long as the data retains value.

The "X" and "Y" factors in the diagram, which differ across industries and organizations, become fixed once assessed. In contrast, the "Z" factor, representing the timeline for creating a cryptographically relevant quantum computer, is in a state of continual reduction.

03 How to stay ahead of the curve

Quantum computing will increasingly impact existing threats and the cyber tools used to protect organizations. It highlights the importance of migrating to quantum-safe solutions that are robust against future quantum computing attacks. While each organization may have different priorities, overlooking the need for quantum-safe solutions risks imminent attacks culminating in data breaches. The impending threat, coupled with the long-term value of data, significantly narrows the window for proactive action.

Creating a quantum-safe environment involves deploying a comprehensive strategy that encompasses both technological and organizational elements. The sheer complexity requires widespread integration of quantum-safe cryptography components throughout the IT infrastructure. This means that remediation is necessary, not just in isolated areas, but across the entire landscape. Currently, the relevant stakeholders and communities are working together to identify best practices for quantum-safe migration and remediation.

Central to this transition is crypto-agility — the capability to update cryptographic algorithms as and when current algorithms become insecure and new algorithms are introduced.

Making an IT environment quantum-safe requires both technical and organizational steps.

Post-quantum cryptography, symmetric ciphers and quantum cryptography (e.g. Quantum Key Distribution) provide the necessary technological foundations to build quantum-safe environments. Organizational efforts, including risk assessment and transition planning, will also play a pivotal role in making a quantum-safe environment.

1

Quantum-safe components

Post-quantum cryptography (PQC) algorithms and symmetric ciphers, quantum cryptography solutions, such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG), lay the groundwork for transforming an organization into a quantum-safe entity. Their applications are broad, spanning quantum-secure communications, data protection and beyond. It is essential to integrate these elements seamlessly, aligned to cryptographic agility principle, especially when considering higher-level technology stack components and their governance processes.

2

Quantum-safe infrastructure

Quantum-safe communication networks and quantum-safe IT components are elements of the quantum-safe infrastructure. While securing the network level is vital for protecting data in transit, it is incomplete. A quantum-safe network is unable to guard against every threat requiring security enhancement at both hardware and software levels. Given the rapidly evolving nature of quantum-secure components and their associated threats, embracing principles of cryptographic agility is critical.

3

Quantum-safe strategy

Enterprises facing quantum risks should aim for a smooth integration of technical upgrades and organizational changes within their quantum-safe strategies. This involves incorporating quantum-safe components and infrastructure on the technical side and focusing on skills, processes and governance at the organizational level. A key aspect of this strategy is to set a definitive benchmark for the cryptographic agility principle, guaranteeing its comprehensive integration across the organization's core elements.

Quantum-safe components

Post-Quantum Cryptography (PQC)

Standardization agencies are developing and standardizing PQC algorithms. The PQC algorithms base their security on mathematical problems that are believed to be hard for quantum computers to solve in reasonable time.

In August 2023, NIST presented Initial Public Drafts of standards for three PQC algorithms.[25, 26, 27, 28] This reflects work that commenced in 2018 to develop PQC algorithms. By 2024, these algorithms may achieve official endorsement or final standardization status. BSI[29] and ANSSI[30] also published their recommendations.

National Security Agency (NSA) expects National Security Systems (NSS) stakeholders to transit to PQC standards by 2035, following the multi-year process described in the National Security Memorandum 10 (NSM-10).[31]

PQC Key encapsulation mechanism

- asymmetric cryptography
- replaces classical algorithms like RSA, ECC or Diffie-Hellman

For **key encapsulation mechanism**, often used to establish a secure communication channel, NIST has selected:

- CRYSTALS-Kyber algorithm.

Noteworthy benefits of this algorithm include its relatively compact encryption keys that can be effortlessly exchanged between parties and its impressive operational speed.

In contrast, BSI proposes using FrodoKEM and McEliece algorithms, and ANSSI proposes CRYSTALS-Kyber and FrodoKEM.

PQC Digital signatures

- asymmetric cryptography
- replaces classical algorithms like RSA-DA, ECDSA

For **digital signatures**, often used to verify identities during a digital transaction or for remote document signing, NIST has selected:

- CRYSTALS-Dilithium
- FALCON
- SPHINCS+

NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications needing smaller signatures than Dilithium can provide. Both BSI and ANSSI propose the same set of digital signature schemes.

Countries intent on bolstering sovereign capabilities, such as China, Russia, India and others, might introduce their own preferred sets of PQC algorithms.

Quantum-safe components

PQC Consideration: Algorithms novelty

The relative novelty of PQC algorithms contributes to a lack of time-tested assurance regarding their performance and security. The security of PQC protocols primarily depends on computational hardness assumptions, which are believed to be resistant even to quantum computing. However, most PQC algorithms are relatively new and would need more research in real-world settings to prove their effectiveness.[32]

Example 1

The Israel Defense Force's Centre of Encryption and Information Security (MATZOV) has recently proposed several classical cryptanalysis algorithms capable of reducing the security levels of Kyber, Saber and Dilithium to below NIST-defined thresholds.[33]

Example 2

The SIKE (Supersingular Isogeny Key Encapsulation) protocol, a candidate in one of the final selection stages for post-quantum cryptography, was recently demonstrated to be broken on a standard laptop in an hour.[34] This cryptographic system proposed in the protocol – Supersingular Isogeny Diffie-Hellman protocol (SIDH) – was both similar to and suitably distinct from well-known protocols. The scheme dealt with elliptic curves – the same mathematical objects used in one of the most widespread types of cryptography deployed today. But it used them in a completely different way. Another notable aspect of SIKE was its compactness, which made it one of the smallest schemes under consideration. This compactness, however, came with a drawback – SIKE was slower compared to its counterparts.[35]

General recommendations by the community: Hybrid key exchange

To increase confidence in the security of the key exchange protocols, ETSI,[36] IETF,[37] ANSSI[38] and BSI[39] recommend hybrid key encapsulation mechanisms (KEMs). In these hybrid proposals, the final key is derived by combining the exchanged keys from two or more component KEMs (e.g., a classical KEM, like ECDH, and another PQC KEM, like KYBER).

The IETF, for instance, is diligently forging ahead with the assimilation of Hybrid KEM into the TLC protocol. A draft version of the X25519[40] standard is currently in the works. NIST is working towards identifying and remedying interoperability issues among PQC, hybrid and traditional algorithms with the draft report[41] recently presented for public comments.

Quantum-safe components

PQC Consideration: Performance vs security trade-off

The inherent complexity of these quantum-resistant algorithms[42,43] will lead to the following three challenges: an increase in the size of cryptographic materials in transport, extended processing time for cryptographic operations and a larger memory footprint required for these operations.

Example 1

UDP protocol is broadly deployed in the Domain Name System (DNS). Ecosystem as a communication protocol. PQC signature schemes, due to their large sizes, exceed UDP packet size limits.[44] Methods to handle these larger responses, like fragmented responses or employing TCP, introduce issues such as increased latency, potential for failure and lack of universal support. Alternative transport options like TLS and QUIC requires careful consideration. These large signatures necessitate more memory and CPU time for resolvers and nameservers, and while increased computational demand may be mitigated by anticipated technological advancements in new equipment, it remains a concern for legacy devices with limited processing power.

Example 2

Current IKEv2 (Internet Key Exchange) protocol is primarily based on either DH (Diffie-Hellman) or ECDH (Elliptic Curve DH) key exchange methods. But the initial IKEv2 messages have a maximum size limit, making it challenging to swap out the more compact ECDH keys with the bulkier keys PQC algorithms employ.[45]

Example 3

Current resource-constrained IoT devices may face challenges in designing in designing their quantum-safe network using resource-heavy PQC algorithms [46, 47, 48]. The IoT devices use small, resource-constrained, with embedded processors, small amounts of RAM, limited flash/storage and clock speeds in order to limit the power, size and cost of these devices.

General recommendations by the community: Solution redesign or PQC algorithm security trade-off

The most straightforward approach is to upgrade the existing software or hardware to better accommodate PQC algorithms. Such upgrades could entail allocating more memory for the efficient execution of an algorithm, updating databases to provide additional space for larger keys or enhancing hardware capabilities to maintain timely calculations. A more nuanced strategy would be to balance the trade-off between security and performance, considering computational and memory requirements. Such an adjustment could include modifying the key size or implementing hybrid approaches.[41,49]

Quantum-safe components

Quantum Key Distribution (QKD)

Another quantum-safe solution that can enhance today's security protocols (including that of quantum-resistant cipher suites) is Quantum Key Distribution (QKD), which enables authenticated users to securely expand symmetric keys using the laws of quantum mechanics. Therefore, unlike the security of quantum-resistant key exchange algorithms, QKD is more robust against quantum computing threats and any unforeseen future algorithmic advances.

However, QKD requires optical fiber connections and suffers from fundamental rate-loss trade-off, which limits point-to-point coverage up to around 150km (or 30db loss) based on today's technology.[50] It is possible to overcome the distance limitation by leveraging trusted (intermediate) ground or satellite nodes. However, this deployment may require additional security measures to protect key exchanges in the middleboxes. For that reason, QKD is most likely to find applications in core networks and data centre interconnects.

Scope

- Allows two parties to share symmetric keys over an insecure communication channel without leaking any information about the shared key to an eavesdropper.
- Can be combined with existing authentication protocols to strengthen the long-term security of cipher suites.

Implementation security

- All real-world cryptographic systems suffer from some form of side-channel vulnerabilities — security loopholes that may arise from design or implementation flaws.
- Countermeasures against side-channel attacks for QKD systems are evolving to be more reliable and robust.

Cost

- The cost of QKD is aligned to standard high-speed networking equipment and is steadily decreasing. Significant cost reductions are expected as the technology is further streamlined and miniaturized.
- QKD infrastructure is plug-and-play, allowing it to be deployed and integrated transparently alongside standard network upgrades, just like any networking device. As demonstrated in 2022[51], QKD can be deployed without requiring new fiber connections, instead coexisting with already in-use fiber networks.

Commercial usage

- QKD-as-a-service offerings are already in production by telecommunication companies.[52, 53, 54]
- Production-level deployments have resulted in QKD integration with mainstream comms technologies/networks, preparing for future adoption.[55, 56]

Standardization and certification

- International organizations like ETSI,[57] ISO[58] and ITU[59] and national agencies[60] have already published standards, recommendations and references describing the security and network requirements for QKD modules.
- ETSI has released a Protection Profile for QKD modules.[57] The certification process of QKD modules is in a dynamic state of advancement. National organizations, e.g. BSI (Germany),[61] have formed working groups to develop similar protection profiles.

Quantum-safe infrastructure

Quantum-safe communications

Quantum-safe communication enhances network infrastructure security. In the process of outlining quantum-safe security for a network infrastructure, pinpointing the exact OSI layer appropriate for implementation is a vital step. As recommended by most remediation strategies, it is important for businesses and organizations to start planning for PQC remediation. QKD could play an important role in securing network infrastructures in the near future, complementing the baseline controls provided by PQC.

	PQC	QKD
Ease of implementation	▸ Largely software based with some potential hardware dependency ▸ For specialized hardware solutions, dependency on hardware vendors and cipher suite performance	▸ QKD solutions require QKD devices to be deployed across optically transparent networks. ▸ Current day QKD devices are largely plug-and-play and can be integrated into existing security protocols via standardized communication interfaces.[62]
Cost	▸ The cost of migrating to PQC algorithms varies significantly based on the target application. Migration can present challenges due to incompatibilities between existing and PQC cryptography algorithms.	▸ The cost of current QKD devices is comparable to networking equipment like enterprise firewalls. ▸ If the existing networks are unable to support QKD deployment, then additional investments have to be made to provide suitable fibers and other operational facilities.
Potential for scalability	▸ Likely to be highly scalable, although its applicability to resource-limited, lightweight devices requires further investigation	▸ Not scalable like public-key cryptography – currently limited to optically transparent metropolitan networks, e.g. data centre interconnects.
Maturity	▸ PQC algorithms are currently undergoing standardization processes and security evaluation.	▸ QKD is now commercially available off-the-shelf. These products and services are also supported by international standards, protection profiles and recommendations, with certification processes underway.

Quantum-safe infrastructure

PQC in network protocols

PQC algorithms need to be deployed at various levels within the OSI model. Each implementation carries challenges in integrating PQC algorithms into existing protocols. Protocols primarily used to transfer user data (i.e., HTTPS, IPsec) carry higher risk compared to routing protocols (i.e., DNS, OSPF) that indirectly handle user data securing routing protocols with PQC can provide additional security.

OSI layer	Selection of network protocols that would need PQC integration	Challenges
Application	▸ HTTPS ▸ SSH ▸ S/MIME ▸ DNSSEC ▸ Kerberos	1. Integration into existing infrastructure and widespread deployment ▸ Performance: Some PQC algorithms may be slower and have and have larger key sizes than their classical counterparts. PQC performance characteristics may struggle to meet the requirements for real-time or near-real-time communications. ▸ Hardware and software support: Many networking devices have hardware support for current cryptographic algorithms and software optimized to efficiently handle classical algorithms. Supporting new PQC algorithms might require new hardware and lengthy software changes. 2. Standardization: Many protocols are IEEE standardized. Any changes to the protocol, including transitioning to PQC, could need to go through the IEEE's lengthy standardization process, which involves testing, documentation and consensus-building.
Transport	▸ TLS over TCP	
Network	▸ IPsec ▸ OSPF ▸ BGPsec	
Data link	▸ MACsec ▸ PPP	

Global technology firms have begun introducing versions of services utilizing PQC algorithms within their network protocols.[63, 64] This forward-thinking move enables customers to comprehensively assess the PQC migration implications on existing infrastructure components.

Presentation (6) and Session (5) layer protocols are often bundled with the application layer in practical implementations and thus excluded from this table. Physical (1) layer deals with hardware and doesn't require cryptographic features.

Quantum-safe infrastructure

QKD in network protocols

QKD implementation will require the introduction of custom hardware solutions. QKD potential applications span various layers of the OSI model. Actual implementation would depend on various factors, including advancements in QKD technology, integration challenges, practicality of use and standardization efforts.

Although QKD can enhance a protocol's security parameters, it will not supersede the protocol's inherent authentication elements. For protection against quantum attacks, the authentication process should follow standard quantum-safe transition recommendations.

OSI layer	Selection of network protocols where QKD could replace or augment the key exchange methods
Application	▸ HTTPS ▸ SSH ▸ SMTP ▸ S/MIME ▸ IMAPS ▸ LDAPS ▸ SMPP with TLS ▸ FTPS, RDP over TLS ▸ Kerberos ▸ DNSSEC
Transport	▸ TLS over TCP
Network	▸ IPsec ▸ OSPF ▸ BGPsec
Data link	▸ MACsec ▸ PPP

Quantum-safe infrastructure

Quantum-safe IT components

Achieving quantum-safe security at the network level is critical but insufficient. It is equally important to implement crypto-agility principles and integrate quantum-safe solutions within composable IT ecosystem components, applications and services.

1. Cryptography Services

Cryptography services encompass both internal and external infrastructure elements that offer cryptographic functionalities to various applications. Notable examples include Public Key Infrastructure (PKI) services and Hardware Security Modules (HSM). Given that these services offer cryptographic capabilities to others, they become focal points for risk and, thus, merit heightened scrutiny.

2. Infrastructure and Business Components

A substantial portion of the effort is directed toward infrastructure and business components. This encompasses, but is not limited to:

- Proprietary and third-party application modules, interfaces and services
- Runtime environments and middleware components
- Operating systems
- Virtualization elements
- Storage devices
- Blockchain solutions.

Addressing concerns within these components can range from collaborating with vendors to mobilizing in-house teams. Even when a vendor oversees an application, the inherent risk still resides within the organization.

3. Cybersecurity Solutions

Cybersecurity solutions offer cyber capabilities throughout an IT environment. A transition toward quantum safety is imperative for these solutions. Some might necessitate a full replacement, while others might maintain their core utility but undergo modifications to integrate quantum-safe methodologies. For instance, secure code review tools could adjust their rulesets to bolster vulnerability detection and pattern recognition. Conversely, systems utilizing federated access may need a more comprehensive revamp.

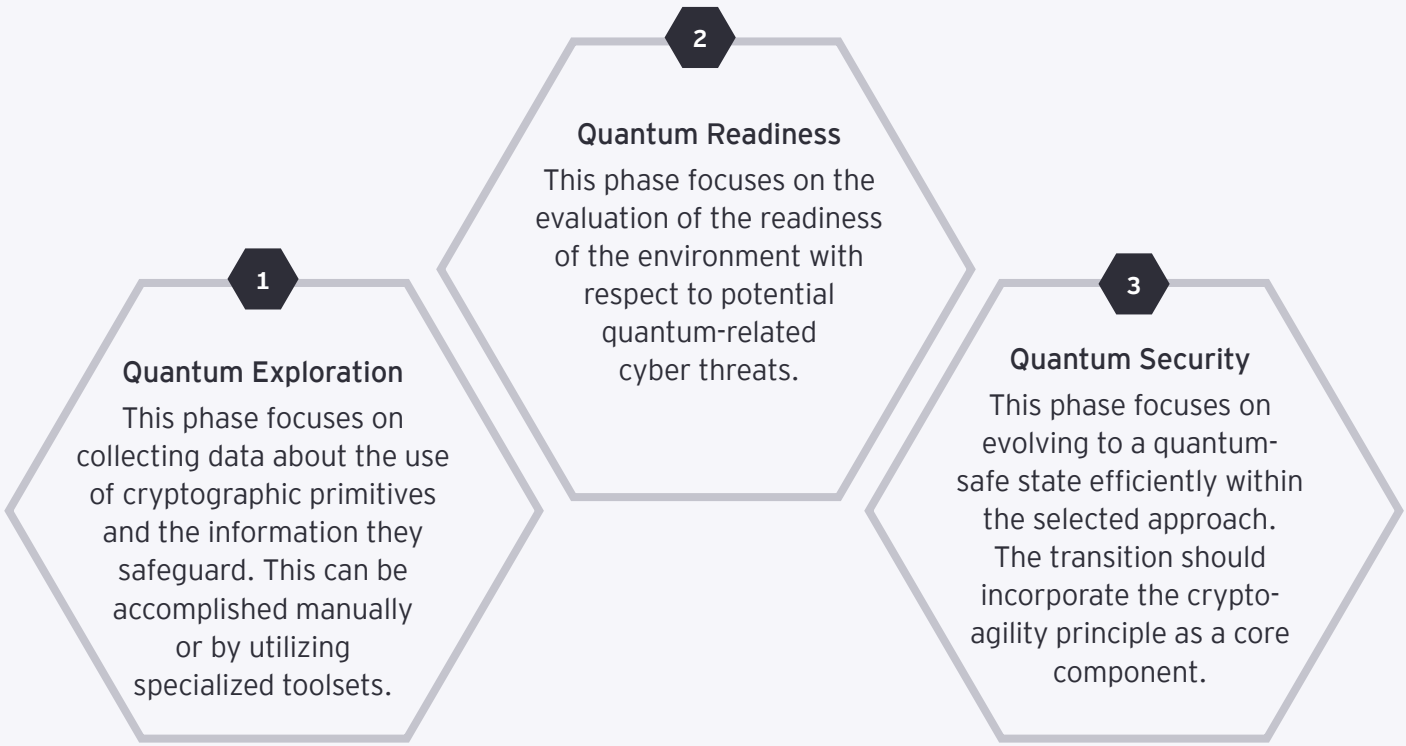
Quantum-safe strategy

Strategy elements

Transitioning an organization to a quantum-safe status involves coordinating a myriad of technical and organizational elements. As the scope of such a transition can become increasingly complex, remediation efforts must be prioritized.

- Data-Driven Remediation: By utilizing data-driven insights, an organization can pinpoint its most critical assets, around which remediation efforts can be prioritized. However, this requires an accurate inventory.
- Commonality-Based Remediation: Instead of requiring extensive data analytics, this method centers on addressing the most commonly important assets, like Public Key Infrastructure, certificate management tools, network connectivity components, and high-value "crown jewel" assets. This method might miss less frequent but equally severe threats due to its minimal reliance on data insights and risk analysis.

A typical quantum-safe remediation program encompasses the following three phases



Recently, NIST initiated the project to share insights and findings to ease migration from current cryptographic algorithms to PQC algorithms with the draft report[65] recently presented for public comments.

Quantum-safe strategy

Quantum exploration

The primary objective of the quantum exploration phase is to gather data that aids in making well-informed decisions about assessing and mitigating quantum-related cyber risks. This crucial phase revolves around gaining a comprehensive understanding of what data is protected and what specific security protocols are in use throughout the entire environment.

Organizations need to gain insight into the cryptographic functions and security protocol versions employed within a given environment. This process is complex, as it involves navigating the diverse landscape of various IT assets, encompassing everything from hardware, firmware, and operating systems to Edge, IoT devices and applications. Typically, this process blends manual efforts with the assistance of automated tools.

While discovery tools can be invaluable, they come with their set of challenges. Some rely on heuristic methods and provide inaccurate results that require manual validation. Others focus solely on a specific asset type, like source code, bypassing other components.

Data discovery tools identify the location and classification of data within an organization. They discover and scan structured and unstructured data repositories, classifying the data based on pre-set or customizable categories. This offer the advantage of ensuring transparency in data usage. However, drawbacks can include complexity in setup and usage, potentially high costs, and false positives/negatives.

Before diving into a comprehensive discovery process, an organization should be well-prepared, having a clear plan for handling the data the process uncovers.

Quantum-safe strategy

Quantum readiness

This phase involves translating the technical vulnerabilities in cryptographic protocols into business terms by identifying and assessing risks. It requires a thorough understanding of both the internal vulnerabilities and the evolution of external factors, including regulatory frameworks.

1 IT components review

The evaluation of a particular IT component must consider its inherent risks and also weigh the positive and negative influence of specific cyber capabilities surrounding it. It's essential to consider that IT components function as composable components. Thus, the assessment process for an IT component is twofold:

1. Examine the cryptographic components in use and their configurations.
2. Evaluate the existing cyber capabilities, like Data Governance & Management, Network Protection & Data Loss Prevention and Third-Party Risk Management. These capabilities provide insight into exposure of sensitive data to harvesting attempts by malicious entities.

2 Quantum industry state

The quantum technology landscape must be explored, understanding its maturity, and identifying the threats it poses to current cryptographic algorithms. The state of the quantum computing industry and algorithm development together set the risk profile. As we transition to scalable, fault-tolerant quantum computing, parameters like the number of physical qubits, noise, crosstalk, and the fidelity of 1-qubit and 2-qubit operations continue to evolve. These changes adjust the risk timeline for cryptographic algorithms. Concurrently, algorithms are continually refined to challenge encryption schemes, lessening the need for advanced quantum hardware.

3 Threat intelligence

System attractiveness to Threat Actors must be assessed as this directly affects the associated level of risk. Organizations should consider the landscape of potential Threat Actors must be assessed as this in terms of their sophistication and possible interest in the data processed by the current IT component.

4 Risk registration

The readiness phase should culminate in adding risk entries with mitigation strategies to internal risk management systems, allowing for better risk prioritization and management.

Quantum-safe strategy

Quantum security

This phase concentrates on transitioning efficiently to a quantum-safe state. A fundamental guideline for this change is the principle of crypto agility. By viewing cryptography components as a distinct asset class, organizations can more seamlessly and swiftly address and update insecure algorithms in the future.

1 Approach

Initiating a comprehensive program hinges on having a clear strategic vision, robust managerial support, and sufficient funding. The intricate nature of quantum risk remediation makes accurately predicting outcomes and resource requirements challenging. This complexity means that a universal solution will rarely be effective. Under these circumstances, a lean strategy could prove advantageous. Such an approach entails beginning with a smaller-scale effort and then progressively scaling up.

2 People Management

For high-complexity projects to succeed, a successful human agenda and people management is pivotal. This encompasses devising incentives to drive desired program and human outcomes and incorporating them into employee attraction, compensation, development and retention schemes.

3 Refining Internal Procedures

Achieving compliance through project initiatives is an intermediate goal, aiming to establish procedures that perpetually keep the organization compliant. This involves rethinking existing processes and improving them.

4 Implementing Quantum-Safe Components

Finally, quantum-safe elements must be integrated into an IT environment. This paper provides a comprehensive analysis of the technical aspects relating to migration. Yet, additional complexities may arise with vendor-managed software, necessitating a distinct approach from that used for in-house developed applications. Addressing internally managed applications calls for enhancing the internal team's expertise. On the other hand, remediation of vendor-managed applications will likely involve re-assessing vendor management policies, negotiating new terms with vendors and potentially revising current agreements.

Bibliography

1. https://datatracker.ietf.org/doc/html/rfc8446
2. https://www.ecrypt.eu.org/ecrypt2/documents/D.MAYA.6.pdf
3. https://eprint.iacr.org/2021/894.pdf
4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
5. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf?__blob=publicationFile
6. https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf
7. https://apps.dtic.mil/sti/pdfs/ADA389646.pdf
8. https://web.archive.org/web/20131017055750/http://cryptome.org/jya/cracking-des/cracking-des.htm
9. https://csrc.nist.gov/News/2017/Research-Results-on-SHA-1-Collisions
10. https://link.springer.com/chapter/10.1007/11535218_2
11. https://sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html
12. https://www.nature.com/articles/d41586-019-03213-z
13. https://phys.org/news/2020-12-chinese-photonic-quantum-supremacy.html
14. https://www.ibm.com/quantum/system
15. https://arxiv.org/pdf/2203.03816.pdf
16. https://www.oezratty.net/wordpress/2022/assessing-ibm-osprey-quantum-computer/
17. https://www.quantinuum.com/news/quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-volume-217-218-and-219
18. https://arxiv.org/abs/2305.03828
19. https://arxiv.org/abs/1905.09749
20. https://dl.acm.org/doi/10.5555/2011517.2011525
21. https://arxiv.org/ftp/arxiv/papers/1208/1208.0928.pdf
22. https://www.nature.com/articles/s41586-023-06927-3
23. https://arxiv.org/pdf/2308.06572.pdf
24. https://www.zapatacomputing.com/publications/variational-quantum-factoring/
25. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
26. https://csrc.nist.gov/pubs/fips/203/ipd
27. https://csrc.nist.gov/pubs/fips/204/ipd
28. https://csrc.nist.gov/pubs/fips/205/ipd
29. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4
30. https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/
31. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
32. https://link.springer.com/chapter/10.1007/978-3-031-30731-7_4
33. https://marketing.idquantique.com/acton/attachment/11868/f-0587a79f-5592-47fe-9bdf-a3f3e7f7d802/1/-/-/-/-/Report%20on%20the%20Security%20of%20LWE.pdf

34. https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf

35. https://csrc.nist.gov/CSRC/media/Events/second-pqc-standardization-conference/documents/accepted-papers/seo-sike-paper.pdf

36. https://www.ietf.org/archive/id/draft-ietf-tls-hybrid-design-04.html

37. https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

38. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html

39. https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/

40. https://eprint.iacr.org/2022/975

41. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf

42. https://content.pqshield.com/nist-post-quantum-cryptographic-standards

43. https://oaepublishstorage.blob.core.windows.net/80a2fb7e-37f6-4488-ad91-daa912af0257/5209.pdf

44. https://www.ietf.org/id/draft-fregly-research-agenda-for-pqc-dnssec-00.html

45. https://www.mnm-team.org/pub/Diplomarbeiten/heid19/PDF-Version/heid19.pdf

46. https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/atkins-requirements-pqc-iot-pqc2021.pdf

47. https://ieeexplore.ieee.org/abstract/document/9787987

48. https://ieeexplore.ieee.org/document/8932459

49. https://link.springer.com/chapter/10.1007/978-3-031-29371-9_13

50. https://www.nature.com/articles/d42473-022-00133-x

51. https://www.jpmorgan.com/technology/technology-blog/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network-critical-blockchain-application

52. https://openqkd.eu/openqkd-in-action/

53. https://www.sktelecom.com/en/press/press_detail.do?idx=1579

54. https://www.singtel.com/business/campaign/quantumsafenetwork

55. https://www.idquantique.com/idq-and-singtel-sign-memorandum-of-understanding-to-establish-a-robust-quantum-ecosystem-in-singapore/

56. https://www.global.toshiba/ww/news/corporate/2022/04/news-20220427-01.html

57. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf

58. https://www.iso.org/standard/77097.html

59. https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13990

60. https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/IMDA-Technical/1c-Draft-IMDA-RS-QKDN--Issue-1--public-comment.pdf

Bibliography

61. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Quantenkryptografie/quantenkryptografie.html

62. https://www.etsi.org/committee/1430-qkd

63. https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

64. https://blog.cloudflare.com/experiment-with-pq/

65. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

Contacts

Aaron Perryman
EY Asia-Pacific
Financial Services Consulting and Digital Leader
Aaron.Perryman@sg.ey.com

Alexey Bocharnikov
EY Asia-Pacific
Quantum Technology leader

Charles Lim
JPMorgan Chase
Global Head of Quantum Communications and Cryptography

Kaushik Chakraborty
JPMorgan Chase
Applied Research Lead in Quantum Communications

Authors

Alexey Bocahrnikov, EY
Kaushik Chakraborty, JPMorgan Chase
Albert Huang, JPMorgan Chase
Charles Lim, JPMorgan Chase

Co-authors

Jefferson Chu, JPMorgan Chase
Omar Amer, JPMorgan Chase
Marco Pistoia, JPMorgan Chase
Andrew Lang , JPMorgan Chase
Dennis Mwansa, JPMorgan Chase
Aaron Perryman, EY
Ralph Thompson, EY
Sohag Sarkar, EY
Rachpal Singh Jassal, EY

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. 011111-23-AUNZ

BMC Agency
GA 133045811

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com