accenture

Accenture Labs

CRYPTOGRAPHY IN A POST-QUANTUM WORLD

Preparing intelligent enterprises now for a secure future

EXECUTIVE SUMMARY

In the digital era, data security is top of mind for many businesses and governments to protect financial records, medical histories, military strategy, confidential information and more. Organizations typically rely on vetted cryptographic algorithms to secure this information. These algorithms underpin an organization's ability to ensure the confidentiality, integrity and availability of business transaction systems, B2B and B2C processes, and digital services delivered via the Internet, cloud or as-a-service on hosted platforms.

Secured information is typically classified based on expectations that it will remain secret for a duration of time. Algorithms using traditional CPU computing have been engineered to be mathematically strong enough to support a 20-year service life requirement, meaning that the cryptographic primitive is unlikely to be broken by adversarial techniques. However, recent technology developments have cut this service life expectation in half, causing the US National Institute of Standards and Technology (NIST) to rescind the current public key standard of RSA 2048 released in 2016 and aggressively seek more complex cryptographic algorithms to thwart attackers.[1]

The looming threat to these cryptographic standards is a new paradigm of computation: the quantum computer. In 1994, Peter Shor formulated an algorithm for quantum computers that would have the power to identify secret cryptographic keys in an extremely efficient way, dramatically reducing the expected time to solve for certain current cryptographic techniques. At the time the algorithm was envisioned, the technology did not exist to build a machine that could implement the method at scale. Two decades later, researchers are starting to realize the quantum processing hardware necessary to run the algorithm. In the event of a major processing breakthrough, the disruption would be massive to businesses' ability to guarantee integrity of process, maintain data protections and ultimately compete in the marketplace.

Many academic researchers anticipate that a quantum computer will be able to implement Shor's Algorithm at a relevant scale in the 10 to 15 years. Accenture believes this inflection point will be much sooner, within the next eight years.

While eight years sounds like a long time, governments, industries and companies need to prepare now with a comprehensive strategy, upgraded infrastructure and quantum-ready security protocol to brace for this computing inflection point. This challenge is massive as described in Accenture's Security Vision: Rethinking Foundations. Like the diligent planning and deep investment that went into Y2K preparations, it will take several years to assess enterprise assets, develop quantum mitigation strategies and implement quantum-proof cryptographic services.

There is no time to waste. The advent of quantum computing is a call to action for an industry-wide shift in how cryptography is done. At an ecosystem level, this impending change will drive application, software and hardware vendors to incorporate quantum-safe solutions into their products—or risk losing their competitive advantage. In the enterprise C-suite, it will require planning and budgeting for a complex infrastructure transition for all cryptographic services spanning many business processes and communications. And in the Security function specifically, to ensure business resilience, security, application and infrastructure owners mobilize together:

Short-term. Ensure enterprise infrastructure is sufficient to maintain cryptographic services using traditional cryptographic methods of either sufficient key size. Migrate current cryptography to quantum-resistant algorithms.

Longer-term. As quantum computing hardware becomes commoditized into solutions, implement quantum cryptographic methods to reduce risk to business processes.

In this paper, Accenture Labs explores the challenges of providing communication confidentiality in a post-quantum computer world, as well as the technologies that can help organizations prepare for this disruption. We look at both current-generation (lattice-based cryptography, hash-based cryptography) and next-generation solutions (quantum key distribution, quantum random number generation) for mitigating quantum computing attacks. Most importantly, we outline an approach for combining traditional cryptography with quantum cryptography to help provide unbreakable, end-to-end encryption with the ability to detect man-in-the-middle attacks.

Why Cryptography Is Vulnerable to Quantum Computing

Cryptography is the art of writing data so that it is not readable by unauthorized users. The strength of a specific cryptographic primitive depends on the secret key length and the mathematical strength of the algorithm. Cryptographic methods rely on large key lengths along with the computational difficulty of number theory problems, such as the Discrete Logarithm problem, to provide protection from cryptanalysis techniques.

The two main techniques that cryptanalysis attackers use to break these algorithms are reverse engineering of the mathematical operations performed in the algorithm, or brute-force guessing of the secret key/s. The first technique is typically the result of human error on the software development side: when creating encryption and decryption programs, developers may inadvertently make a mistake in the implementation of the mathematical operations, opening a door for attackers to circumvent the cryptographic methods through reverse engineering.[2] The second technique of brute-forcing a properly implemented algorithm with a sufficiently complex key is often impractical for attackers. Even when armed with hardware accelerators such as Graphical Processing Units (GPUs), Field Programmable Gate Arrays (FPGA) and Application-specific Integrated Circuits (ASICs), brute forcing by checking every possible key value could take centuries of computing time. Brute force attacks remain the bastion of supercomputers.

Quantum computation takes an entirely novel approach to cryptographic techniques by transforming the number theory problems into ones a quantum computer can solve with very little computational difficulty—sometimes in a matter of seconds. Most recently, researchers have shown that quantum computing is capable of breaking the strong cryptographic primitives, such as the Diffie-Hellman key exchange.[3]

OVERVIEW OF KEY TECHNOLOGIES

1.1 Classical Cryptography Principles

In the digital world, cryptography is commonly associated with three main principles: confidentiality, integrity and authentication. These principles provide an assurance that information is trustworthy and can only be accessed by authorized users. Each principle is underpinned by the implementation of cryptographic functions. Confidentiality is provided by encryption of the data with public and secret keys. Integrity is provided by hash functions and digital signatures. And authenticity is provided by using secret keys that only the entity controls. Today, cryptography is essential to everyday business functions and is especially prevalent in the communication methods on the Internet between users and web applications.

1.2 Quantum Computing

A quantum computer is a new form of computing technology that harnesses quantum mechanical phenomena rather than binary functions to perform computational operations. To learn more, visit www.accenture.com/quantum and read the Accenture point of view, Think Beyond Ones and Zeros: Quantum Computing Now.

Quantum computers use quantum bits (or qubits), which have special properties in that qubits can natively represent information as vectors, which is different than a classical bit that can only be set to values of 1 or 0. One of the defining features of qubits is that they can be placed in a state of "superposition," in which the value of the qubit becomes unknown during the actual calculation sequence. In addition, multiple qubits can be chained together using a method called "quantum entanglement," so that the value of a single qubit affects the value of all the other qubits. In this computing paradigm, multiple dimensions of processing can occur in a qubit itself and between qubits in a single transformation, or gate. As more qubits are interlinked, the power of the computer grows exponentially. Thus, the strength of a quantum computer is determined by the number of error-corrected qubits that can be entangled with one another.

Several quantum computing hardware companies are attempting to create quantum computers that are provably faster than classical computers and techniques for a single use case, or what is known as "quantum supremacy."

In the past, each time a claim has been made that a quantum computer was faster, academia has disproven the claim—either by creating a larger, more powerful classical computer, or by applying a new form of heuristic to a classical processing method, which decreased the time in which the algorithm could run.

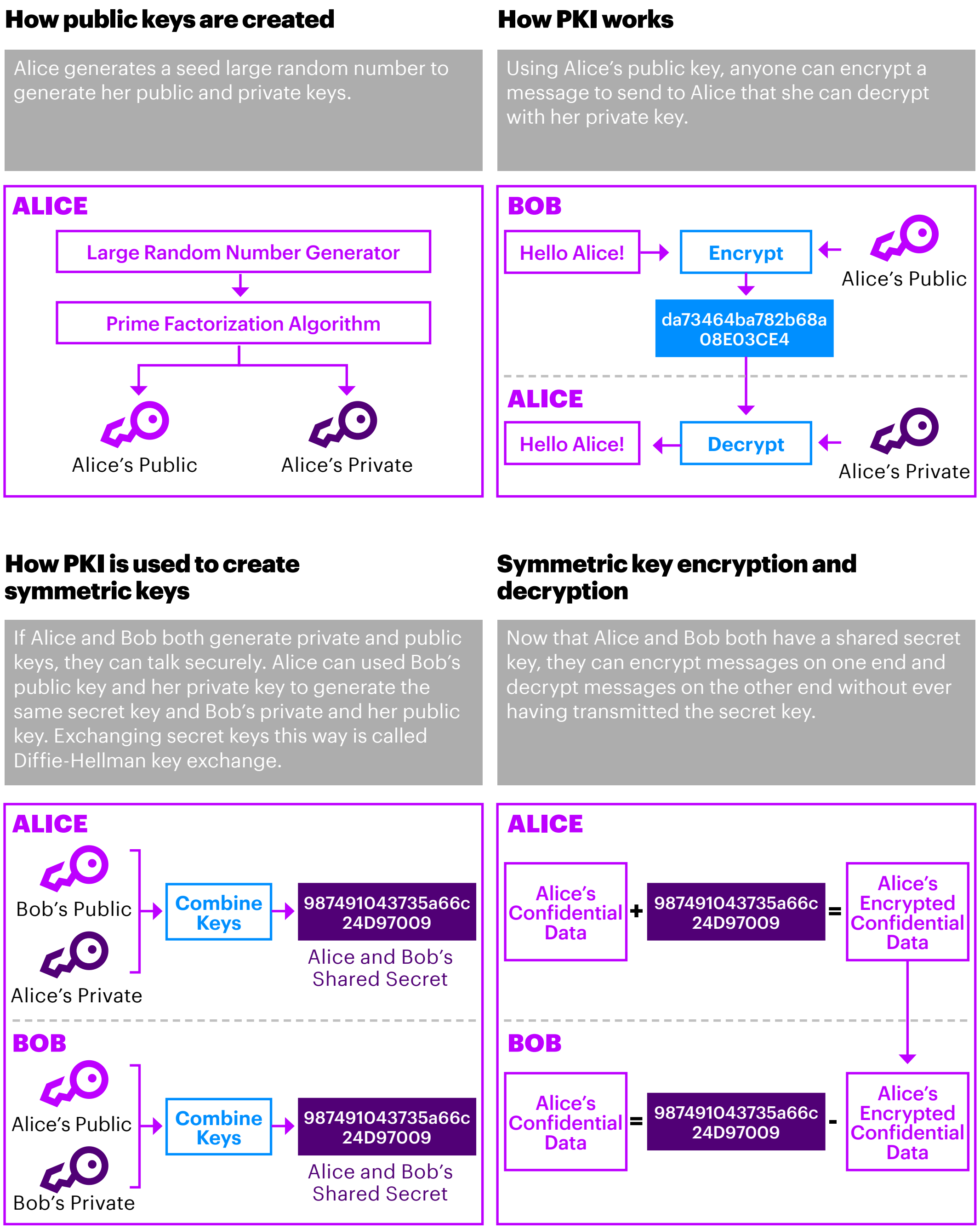
However, tech giants have now taken up the race to definitively demonstrate quantum supremacy. In March 2018, Google announced Bristlecone, a 72-qubit system for quantum processing. In 2018, IBM prototyped a 50-qubit system and simulated a 56-qubit system.[4] The development of a sufficiently large quantum computer is expected to revolutionize many fields that rely on complex simulations, like chemistry and solid-state physics, as well as offer significant speed increases for search technologies. This approach can also be applied to solving cryptographic challenges.

1.3 Quantum Computing Applied to Classical Cryptography

Classic cryptography relies on the strength of the secret key to provide cryptographic security (Figure 1). Certain number theory problems—such as the Prime Factorization problem, the Discrete Log problem and Elliptic Curve methods—underpin current cryptographic schemes. These were chosen because it is computationally easy to combine two large numbers together; however, it is computationally difficult to go the opposite way and determine what the original numbers were if only given one. For example, it is easy to calculate 173 X 191 = 33,043, but it is harder to figure out which two numbers multiplied together equal 33,043.

Currently, there are no known mathematical shortcuts to these algorithms, meaning that every single possible combination (or brute force) must be tested to find the key number that will unlock the algorithm. Using current classical computation, and even with hardware accelerators, this could conceivably take hundreds of years. In contrast, one of the general classes of problems that quantum computers solve best is phase estimation, which can be described as identifying where two different frequencies overlap. Both the Prime Factorization problem and Discrete Log problem can be transformed into phase estimation problems. In 1994, Peter Shor showed that quantum computers could use quantum physics characteristics to efficiently solve these problems without relying on brute force, thereby rendering any information encrypted by our public key system vulnerable to decryption.

FIGURE 1. Public/Private Key Basics



How public keys are created

Alice generates a seed large random number to generate her public and private keys.

How PKI works

Using Alice's public key, anyone can encrypt a message to send to Alice that she can decrypt with her private key.

How PKI is used to create symmetric keys

If Alice and Bob both generate private and public keys, they can talk securely. Alice can used Bob's public key and her private key to generate the same secret key and Bob's private and her public key. Exchanging secret keys this way is called Diffie-Hellman key exchange.

ALICE
Bob's Public
Alice's Private
Combine Keys
987491043735a66c 24D97009
Alice and Bob's Shared Secret
BOB
Alice's Public
Bob's Private
Combine Keys
987491043735a66c 24D97009
Alice and Bob's Shared Secret

Symmetric key encryption and decryption

Now that Alice and Bob both have a shared secret key, they can encrypt messages on one end and decrypt messages on the other end without ever having transmitted the secret key.

ALICE
Alice's Confidential Data
+
987491043735a66c 24D97009
=
Alice's Encrypted Confidential Data
BOB
Alice's Confidential Data
=
987491043735a66c 24D97009
-
Alice's Encrypted Confidential Data

1.4 The Quantum Computing Threat to Cryptography

As quantum computational technology grows, it will increasingly jeopardize the security and strength of the public key cryptographic paradigm. A quantum computer could be used efficiently for the brute-force methods for each of the three cryptographic principles (confidentiality, integrity and authentication), subsequently breaking much of security systems used today.

This would endanger any data or messages that are currently protected by these cryptographic schemes, allowing anyone with a sufficiently advanced quantum computer to read any information or communications encrypted by the schemes. It could also expose any encrypted historical data collected by third parties, and even allow threat actors to impersonate authenticated users, legitimate organizations and web applications.

Although quantum cryptanalysis attacks are yet practical, NIST and other entities have been monitoring advancements in quantum computing and working to improve the current cryptography standards by identifying new quantum-safe algorithms, defining the implementation strategies, and gaining broad consensus on the approach such that it will be adopted. In 2016, NIST released a report on Post-Quantum Computing that announced a preliminary standardization plan and called for new algorithmic proposals. The deadline for submissions closed at the end of 2017. NIST is currently analyzing the proposals and expects to report its findings and have draft standards ready between 2022-2024.[5]

Quantum computing research has advanced to the point where a functional quantum computer capable of breaking current-grade cryptography will arrive arrive within the next ten years. Accenture believes this inflection point will be much sooner, within the next eight years. To maintain secure communications and encryption, Global 2000 companies in every industry must begin now to refresh the technologies underpinning cryptography. This is the only way to prepare for a future filled with quantum computers that can break classical cryptography.

> “
>
> **Quantum computing research has advanced to the point where a functional quantum computer capable of breaking current-grade cryptography will arrive within the next ten years. Accenture believes this inflection point will be much sooner, within the next eight years.**

2.0 Transitional Phases for Cryptography

Accenture foresees two main cryptographic transitions, or phases, in the near-term and longer-term. As the industry awaits a new quantum-resistant standard promised from NIST between 2022-2024, organizations should prioritize their technology transition as quickly as possible. This will include near-term mitigation measures to improve the security of existing encryption methods.

First, before quantum computers can fully break classic cryptography, cryptologists will need to update classic cryptography with quantum-resistant algorithms (lattice-based and hash-based cryptography) to improve their resiliency against quantum computing cryptanalysis attacks.

Second, as quantum cryptanalysis advances, new methods discovered may break the current quantum-resistant algorithms since they are still based on the number theory, similar to Shor's Algorithm breaking Prime Factorization methods. As a result, cryptologists will need to transition to cryptography that leverages quantum mechanisms instead of number theory and traditional mathematical complexity. These techniques are provably secure in contrast to quantum-resistant algorithms that are only computationally secure.

2.1 Near-Term Transition to Quantum-Resistant Algorithms

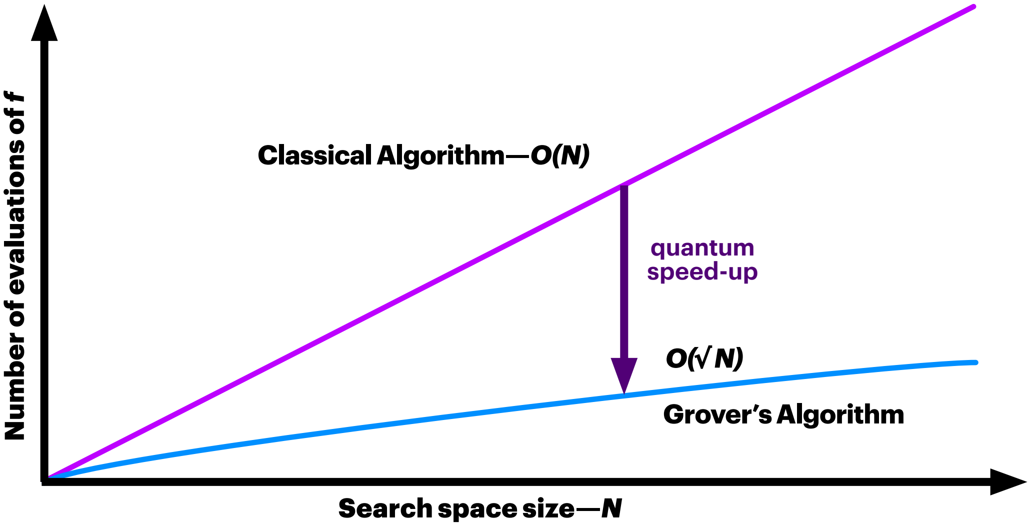
The first phase involves improving classical cryptography by transitioning to quantum-resistant algorithms. Figure 1 depicts how the current private and public key cryptography scheme works regardless of algorithm used, and highlights where the private key and shared secret keys can be exposed using quantum computing.

Current cryptographic methods are separated into two types of schemes:

Symmetric. A common attack on cryptographic systems involves a brute force against the key. Using this method, all possible key values, known as the search space, are generated and tested until the information is successfully decrypted. Techniques that reduce the search space, such as Biclique cryptanalysis, accelerate the attack. Grover's Algorithm, using quantum processing, can provide a quadratic speed-up—significantly decreasing the brute force attack time (see Figure 2).

Asymmetric. For systems that use asymmetric cryptographic schemes for encryption such as RSA encryption, a quantum computer can be used to find the private key using the public key and the algorithm used for prime factorization. Specifically, the quantum computer can use Shor's Algorithm to factor a number much more efficiently (polynomial time), greatly decreasing the computational time to determine the private keys. The Prime Factorization problem, the Discrete Log Problem (the basis for Elliptical Curve methods) are susceptible to computational speed-ups from Shor's Algorithm, meaning that a large number of secret keys will be readily calculated and subsequently compromised.

FIGURE 2. Grover's Quantum Speed Up



Any type of algorithm that belongs to a class of problems known as "hard number theory problems" and as "one-way trapdoor functions" can be used to share keys. In traditional cryptography based on classical number theory, cryptographic strength could be increased or the service life of the algorithm extended by increasing the key length. With the rise of quantum processing, increasing the key length will only provide temporary protection as quantum processing advances will overtake those protections in time. The business implications from increasing the key length must also be considered as this could impact processing performance, supporting infrastructure, and application and communication architectures.

In recent years, researchers have been working to create cryptographic schemes that preserve existing cryptographic infrastructure but swap in number theory problems that resist attacks by quantum computers.[6] This would make it possible to replace just one small piece of the public key infrastructure—the combined key space—with quantum-resistant algorithms. Lattice based cryptography and hash-based cryptography provide two options that will allow researchers to maintain the existing infrastructure that supports Diffie-Hellman key exchange and digital signing while still providing quantum cryptanalysis resistance.

Pros and Cons of Expanding Cryptographic Infrastructure

Cryptographic infrastructure is complex as it involves software, crypto-processors, hardware customization and communications infrastructure. Any changes to this infrastructure must be carefully planned and tested to ensure compatibility with existing components.

Examples of these infrastructures are crypto-processors, which are hardware chips carrying several crypto functions such as encryption, signature generation and hashing. They are embedded in many devices such as point-of-sale systems, automated teller machines, TV set-top boxes, smart identity cards and smart phones (SIM cards). These cryptosystems rely on the current cryptography standards depending on the applications. For lightweight applications with lower amounts of data, these crypto-processors mostly rely on small crypto algorithms such as AES, LED and PRESENT.

Moving to quantum-resistant crypto primitives will affect the performance of these crypto processors, since they involve more computations and even render some processors obsolete. Organizations may be required to buy new hardware with upgraded crypto-processors to handle the increased workload.

2.2 Lattice-Based Cryptography

Currently, researchers are in the process of modifying existing asymmetric public key encryption schemes so that the underlying algorithms used to encrypt and decrypt data are resistant to phase estimation transformations. These newer encryption algorithms are similar to algorithms that take advantage of the Prime Factorization and the Discrete Log problems, but because of aspects of these particular problems, still maintain currently unsolvable complexity from attacks using quantum algorithms. The Shortest Vector problem is one of the leading replacements for the Prime Factorization problem and Discrete Log problem. A form of cryptography known as lattice-based cryptography uses it to provide currently quantum-safe encryption.

Lattice-based cryptography can be used for most current cryptographic services, like encryption, message signing and hashing, making it a popular candidate for post-quantum cryptography. Research into the Shortest Vector problem has shown it resists one of the key techniques (periodicity finding) used in Shor's Algorithm. Until proven otherwise, **lattice-based cryptography** remains a safe alternative. However, lattice-based public key encryption algorithms do not scale particularly well.

There are multiple lattice-based cryptographic systems currently available for distribution, albeit the efforts are mostly from the open source community. The most mature of these offerings include NTRUEncrypt and NTRUSign (GNU General public license for development, commercial license for production), RLWE-KEX Encryption (available as an OPENSSL modification), and SWIFFT Hashing (GNU General public license).

The Challenge with Lattice

Lattice is difficult to prove hardness at scale. In cryptography, hardness is a measure of how strong the algorithm is across all conditions to simplification or attacks. Another way to think about this is how provably resilient the algorithm is to mathematical attacks.

There are tradeoffs between hardness and scalability that must be considered when selecting a lattice-based algorithm.

There are lattice-based public key encryption algorithms that have been proven to be worst-case (very strong) hardness. For these **worst-case** algorithms, any key selected will always be difficult to solve—a good property in selecting a cryptographic method. However, the current **worst-case** lattice algorithms do not scale well. Current lattice algorithms that do scale well only achieve **average-case** hardness. **Average-case** hardness means that in most cases, keys selected will be difficult to solve, but there may be mathematical conditions where they become easy to solve.

As scale is a digital business imperative, we expect NIST to select an **average-case** lattice-based algorithm as the next standard. Businesses implementing average-case lattice should carefully follow all use case and implementation guidance to ensure the operational conditions continue to make them hard problems.

Accenture recommends that companies prepare to transition to lattice-based cryptography when NIST releases its next “quantum resistant” primitive standard and formalizes the algorithm. Preparation entails collecting asset lists of services that use cryptography, updating patching infrastructure, setting up governance infrastructure, and working with third-parties to make sure they are prepared for the switch as well.

2.3 Hash-Based Cryptography

Hash-based cryptography is an alternative quantum-proof cryptographic scheme that is primarily focused on digital signatures that verify that the document or message originated from the initial sender of the document. There are currently no hash-based cryptographic schemes for encrypting and decrypting messages using asymmetric public key exchange (PKE), so additional cryptographic methods would be necessary for the remaining cryptographic services.

The digital signatures that hash-based cryptography produce are not number theory problems and are impervious to mathematical optimization techniques that quantum attacks use to break current cryptography. Because signatures generated from hash-based cryptography are only suitable for one-time use, keys must be regenerated for each new message sent and old keys must be tracked to prevent recycling.

Popular hash-based cryptographic schemes typically take advantage of Winternitz one-time signatures (OTS). Winternitz-OTS uses a tuning parameter that must be set. This tuning parameter trades-off between signature size and key generation, signing and verification speed. Hash-based cryptographic implementations need to optimize this parameter in order to operate effectively.

> **“**
>
> **Preparation entails collecting asset lists of services that use cryptography, updating infrastructure, setting up governance infrastructure, and working with third-parties to make sure they are migrating to quantum-resilient cryptography as well.**

3.0 Longer-Term Transition to Using Quantum Mechanics as a Cryptographic Solution

Quantum computing provides an opportunity to improve our conventional cryptography infrastructure. Unlike conventional cryptography, which is based on number theory, quantum cryptography uses the laws of quantum physics to generate keys and transfer information. Quantum key generation and distribution has the promise to transform the quality of cryptography at large.

3.1 Quantum Key Distribution

Quantum key distribution (QKD) is a new advanced method for secure key exchange. Through QKD, parties will be able to distribute shared secret keys directly without the possibility of undetected eavesdropping or tampering. Based on the properties of quantum mechanics, any attempts to disrupt or observe the communication will leave physical traces—fingerprints of the tampering attempt.

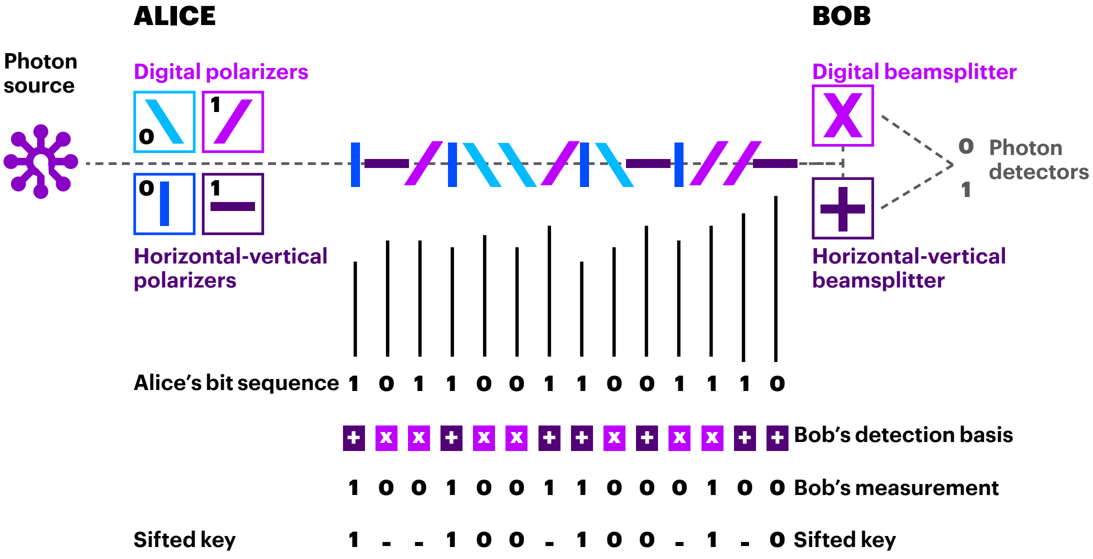
Quantum communications are naturally tamper-proof. During quantum communication, information is encoded into photons. Each photon has a quantum state that determines its position and direction in physical space. The act of measuring a quantum state will change the position of a photon and disturb the system. As a result, if an adversary attempts to measure or eavesdrop on a quantum key exchange channel, the modification will later be detected. In practice, the QKD key would be discarded and the participants notified of the compromise. At a minimum, the key would fail in usage as observing or measuring the key changes the value. This protection could be readily implemented using Wegman-Carter authentication (WCA) and would render eavesdropping attacks ineffective.

How does QKD work?

Following are the BB84 protocol steps conducted by Charles Bennet and Gilles Brassard in 1984 using a free-space or fiber quantum transmitter to send quantum states of light between a transmitter (Alice) and receiver (Bob) as shown in Figure 3. (Note: This channel does not need to be secure.)

1. Alice uses a light source to create a photon.
2. The photon is sent through a polarizer and randomly given one of four possible polarization and bit designations—vertical (one bit), horizontal (zero bit), 45 degrees right (one bit) or 45 degrees left (zero bit).
3. The photon travels to Bob's location.
4. Bob has two beamsplitters (a diagonal and vertical/horizontal) and two photon detectors.
5. Bob randomly chooses one of the two beamsplitters and checks the photon detectors.
6. The process is repeated until the entire key has been transmitted to Bob.
7. Bob then tells Alice in sequence which beamsplitter he used.
8. Alice compares this information with the sequence of polarizers she used to send the key.
9. Alice tells Bob where in the sequence of sent photons he used the right beamsplitter.
10. Now both Alice and Bob have a sequence of bits (sifted key) they both know.

FIGURE 3. How quantum key distribution works


ALICE
BOB
Photon source
Digital polarizers
0
1
0
1
Horizontal-vertical polarizers
Digital beamsplitter
0
1
Photon detectors
Horizontal-vertical beamsplitter
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
+ x x + x x + + x + x x + + Bob's detection basis
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's measurement
Sifted key 1 - - 1 0 0 - 1 0 0 - 1 - 0 Sifted key

Currently, countries such as Austria, China, Japan, Switzerland and the US are working to implement QKD to support one-time pad (OTP) generation. OTPs are large keys that are pre-shared between sender and recipient. Unlike other forms of cryptography in which keys are used multiple times, an OTP is a single use key to protect a single communication and must be as long as the communication itself.

As the speed of QKD increases, QKD technology offers a means of securely transmitting OTPs. Using fiber optics and FPS 3000 technology, the current standard for communications transport is 100 Gbit/s in cordless and directionless networks. Current speeds of the quantum-based communications must be significantly increased prior to adoption. A collaboration between the University of Cambridge and Toshiba using the BB84 protocol demonstrated an exchange of secure QKD keys at 1 Mbit/s (over 20 km of optical fiber) and 10 Kbit/s (over 100 km of fiber).

3.2 Quantum as a Random Number Generator

Secure cryptography does not exist without random numbers. The generation of high-quality cryptographic keys requires a reliable source of randomness. These random numbers are either used directly as keys, or they are the seeds for secure random number generators. In addition, random key generation must be implemented in such a way that adversaries cannot predict the keys. High-quality random sources are a real challenge in the field of cryptographic systems.

Current technology generating random numbers is only able to generate pseudo random numbers (PRNG). Even if the technology can pass current randomness tests, the numbers are still not provably secure in terms of their randomness. Given enough time, analysis can yield patterns that challenge the randomness of PRNG. In practice, PRNG must be monitored to maintain sufficient randomness for business protection, especially as adversaries commit additional resources to finding patterns in PRNG implementations.

In contrast, quantum random number generation (QRNG) provides not only a high bit rate, but also a physically and provably secure source of randomness due to the physics and mechanics of quantum. This also makes QRNG very attractive for the actual generation of keys and seed numbers at large, including OTP.

QRNG techniques fall into two categories: device-dependent and device-independent.

Device-dependent techniques rely on the full knowledge of the devices used in the protocol such as the input, output, operating temperature, etc. Device-dependent methods generate random numbers at a very high rate.

Device-independent techniques do not require such knowledge of the devices. Although, in theory, device-independent methods are much faster, they need state-of-the-art set-ups that can only achieve very low rates of random number generation.

Current solutions use the device-dependent methods along with self-testing techniques to verify a real-time randomness of the output using entropy measurement and the authenticity of the device. Using this emerging approach, the Hefei National Laboratory for Physical Sciences in China has produced random numbers at the rate of 68 Gbit/s.

Ongoing Research into Quantum-Resistant Algorithms and Quantum Cryptography

There are several companies working to implement lattice-based or hash-based cryptography. One example is the Post-Quantum Company, which has proposed a secure messaging app named PQ Chat that boasts an authentication technique resistant to quantum attacks. Another example is Whitewood Encryption System, which has been awarded a patent for its proposed encryption scheme using QRNG.

Research in QKD is still needed in three different directions.

1. Improve the QKD protocols (including security proofs against individual and collective attacks) and the QKD engines, especially with a view on higher bit rates. A prototype of a QKD engine producing 1 Gb/s of provably secret bits is on the horizon.

2. Explore Device Independent Quantum Information Processing (DIQIP). This connects to the fascinating physics of quantum non-locality, but should also focus on semi-DIQIP (i.e., on protocols where well-identified parts of the system are trusted).

3. Develop quantum memories and repeaters by applying experimental physics on light-matter interactions at the single-photon level. While each individual requirement for a quantum repeater (e.g., memory time, fidelity, efficiency, etc.) has been demonstrated separately, they have not been successfully demonstrated within a single implementation. The challenge is achieve this in a singe quantum repeater for distant quantum communications.

QRNG

A few companies are currently offering this capability, such as QuintessenceLabs, which has generated 1 Gbit/s of random numbers to date. These can be used to increase security on enterprise communication or in conjunction with certain machine learning algorithms to improve their effectiveness. Other companies offering QRNG services include NanoMetr and IDQ.

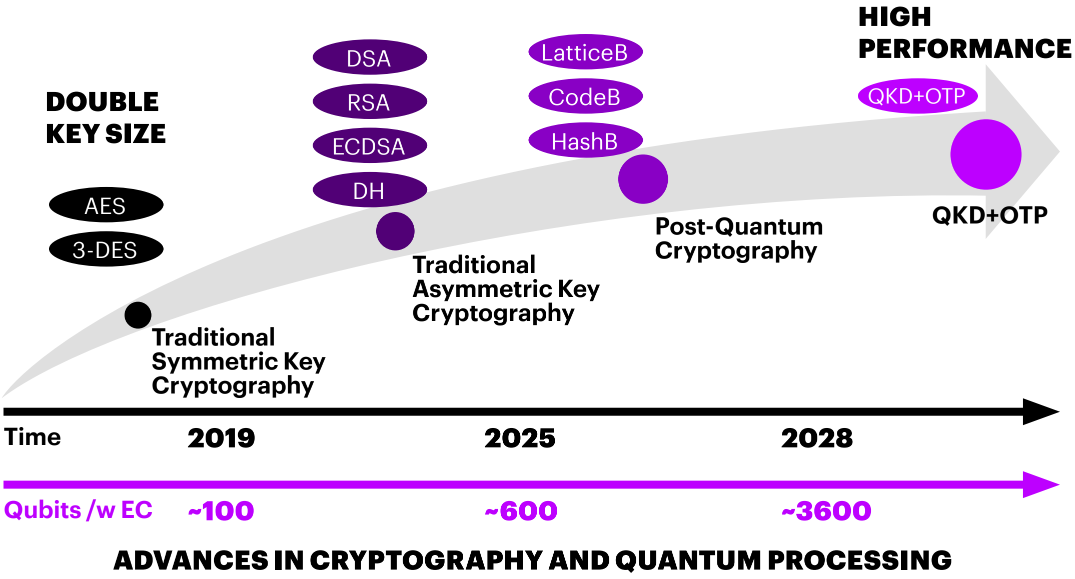
4.0 The Timeline for Quantum

Historically, it has taken NIST from three to five years to define and release each new cryptographic standard in the academic realm. Case in point: technology transitions from two-key to three-key triple DES encryption took from 2010 until 2015; transitions for RSA Key Transport and Digital Signature Generation and Verification using RSA-1024 to RSA-2048 took from 2010 to 2013; transitions for Key Derivation Functions took from 2010 until 2015; and transitions for SHA-1 to SHA-256 took from 2010 to 2013.

We can expect a similar timeframe for quantum-resistant standards to be released. NIST closed the nomination process for quantum-resistant algorithms in late 2017. As such, it is expected the new quantum-resistant standard will be available by 2022. The subsequent adoption across industries and implementation of technology transitions by individual companies will take another three to five years. In this scenario, it will be between 2025-2028 before quantum-resistant cryptographic standards are widely implemented.

Accenture believes the inflection of quantum computing is coming quickly and the ability to break classic cryptography will be reached within the next 8 years—by 2025. Given the breadth and complexity of the transition ahead, it is essential for companies to begin transitioning now. Ideally, as shown in Figure 4, every organization should work to achieve quantum-proof coverage by 2025.

FIGURE 4. Timeline for future standardization events (copyright Accenture)

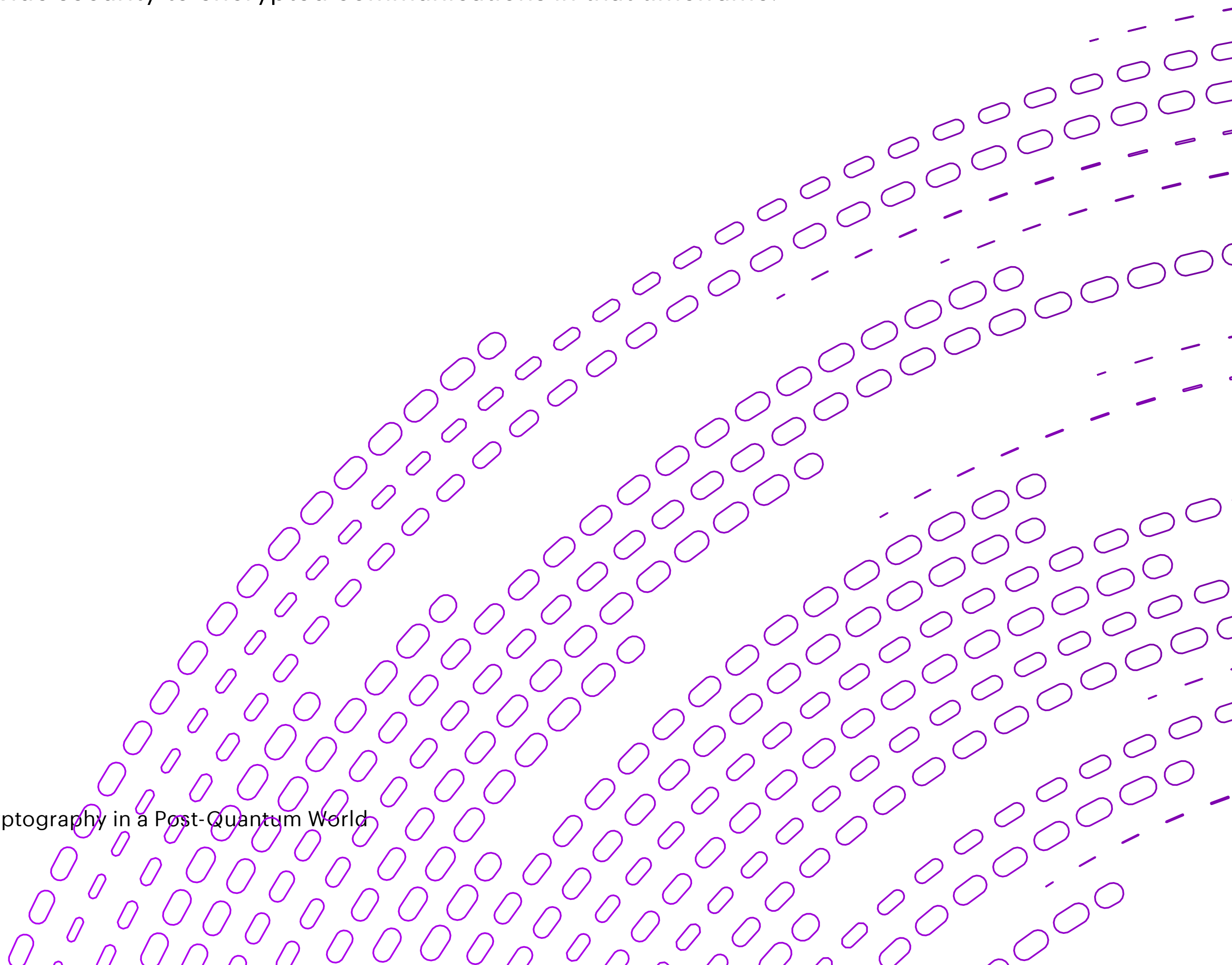

DOUBLE KEY SIZE
AES
3-DES
Traditional Symmetric Key Cryptography
DSA
RSA
ECDSA
DH
Traditional Asymmetric Key Cryptography
LatticeB
CodeB
HashB
Post-Quantum Cryptography
HIGH PERFORMANCE
QKD+OTP
QKD+OTP
Time
2019
2025
2028
Qubits /w EC
~100
~600
~3600
ADVANCES IN CRYPTOGRAPHY AND QUANTUM PROCESSING

There are additional benefits to beginning this transition early. Encrypted communications and internet traffic are currently collected by many third parties and are secured with non-quantum-resistant standards. If key exchange communications used to establish the encryption are included in the collection of this data, then third parties can hypothetically use a quantum computer to solve for the encryption keys and decrypt any subsequent communications using those same encryption keys. Historically communicated and stored business information protected by current cryptographic methods will be at risk of decryption and exposure. Quantum resilience planning needs to consider the protection of information at rest, in storage and in transit today.

4.1 Short-term and Longer-term Steps for Organizations

In the next year, companies should review their current cryptographic standards to make sure they are up to date, and that infrastructure and support exists to rapidly update when new NIST standards become available. Out-of-date cryptographic standards will be broken much faster than the current standards and updating will forestall any adversaries from breaking their encryption.

While NIST is on track to roll out the new quantum-resistant standard by 2022, businesses should prioritize their business cryptographic resiliency planning. This will likely be a stop-gap until quantum cryptography technology advances, but it will provide security to encrypted communications in that timeframe.



CORE AREAS	POTENTIAL STEPS	COMPLETE BY
1 **Understand where the business risk of quantum lies across all enterprise assets**	Update enterprise asset inventory to document where cryptographic keys and methods are being stored/utilized across applications, browsers, platforms, files and modules, as well as shared with third parties/ vendors. Capture key management practices and lifecycle. Document business processes that leverage those cryptographic methods. Ask software-as-a-service or third-party platform providers about their embedded cryptographic methods and plans for an ecosystem-level solution to protect organizations and maintain contractual obligations.	**June 2019**
2 **Develop quantum mitigation strategies**	Conduct a risk-based assessment of the cryptographic asset inventory and sensitive data flows to determine a hybrid approach that may include updating existing cryptographic methods (such as lengthening or maximizing current public key sizes), using quantum-proof methods or turning to alternative controls to protect the data.	**January 2020**
	Evaluate new standardized quantum-resistant/ post-quantum cryptographic solutions being developed by NIST and other entities that leverage new cryptographic methods and approaches (e.g., lattice-based cryptography, hash-based cryptography).	**December 2020**
3 **Plan and implement quantum-proof cryptographic services migration**	Based on business risk prioritization, update systems with new quantum-proof cryptographic methods and procedures across applications, browsers, platforms, files and modules, as well as shared with third parties/vendors. Create new quantum-proof policies, methods and procedures aligned to use cases/ requirements. Update asset inventory with newly implemented cryptographic details.	**End of 2025**

CONCLUSION

Over the past decade, our businesses have become fully digital and our marketplaces fully internet-enabled. Confidence in this digital business ecosystem rides on the security provided through modern cryptographic methods. These methods give us the confidentiality of our data and assurance in the integrity of both information confidentiality and user identity. Threats to cryptography are nothing short of a threat to business operations at large in this digital ecosystem.

The advent of quantum processors that have the capability to break our current cryptographic primitives is a very real threat on the horizon. Accenture believes quantum processor capability will be able to compromise existing cryptography within the next eight years. Businesses have a complex task ahead to identify, evaluate and prioritize the business remediation to protect their data from the cryptanalysis breaches and compromise. Much like the call to action from Y2K, the changes needed are deep in the fabric of our infrastructure. Replacing cryptographic methods across our business processes is a complex effort that will require a concerted campaign of technology and business transformation. Companies need to start preparation now for the transformation ahead, ensuring that they are resilient to the threats of quantum processing before this tipping point.

REFERENCES

[1] https://www.keylength.com/en/4/, Keylength - NIST Report on Cryptographic Key Length and...recommendations and cryptoperiods extract from NIST Special Publication 800-57 Part 1, Recommendation for Key Management.

[2] https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf

[3] Kaplan, M., Leurent, G., Leverrier, A. and Naya-Plasencia, M., 2016, August. Breaking symmetric cryptosystems using quantum period finding. In Annual Cryptology Conference (pp. 207-237). Springer, Berlin, Heidelberg.

[4] "Google Plans to Demonstrate the Supremacy of Quantum Computing". IEEE Spectrum: Technology, Engineering, and Science News. Retrieved2018-01-11.https://spectrum.ieee.org/tech-talk/computing/hardware/ibm-edges-closer-to-quantum-supremacy-with-50qubit-processor

[5] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, NIST PQC workshop
http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm
Feb 2016: NIST report on PQC—http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf
http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf

[6] https://cseweb.ucsd.edu/~daniele/papers/PostQuantum.pdf
Micciancio, D., Regev, O. 2008, December. Lattice-Based Cryptography
https://web.eecs.umich.edu/~cpeikert/pubs/suite.pdf
Peikert, C. 2014, July. Lattice Cryptography for the Internet

AUTHORS

Lisa O'Connor
Managing Director,
Cybersecurity R&D
Accenture Labs
lisa.oconnor@accenture.com

Carl Dukatz
Senior Manager,
Systems and Platforms R&D
Accenture Labs
carl.m.dukatz@accenture.com

Louis DiValentin
Associate Principal,
Cybersecurity R&D
Accenture Labs
louis.divalentin@accenture.com

Nahid Farhady
Associate Principal,
Cybersecurity R&D
Accenture Labs
nahid.farhady@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

This document makes descriptive reference to trademarks that may be owned by others.

The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.