IDC Analyst Brief sponsored by Arqit
May 2024

Securing Valuable and Durable Data in a Post-Quantum World

Duncan Brown
Group Vice President, IDC

Securing Valuable and Durable Data in a Post-Quantum World

Introduction

Quantum computing may be regarded as a futuristic technology by many, but in fact it is advancing rapidly, perhaps faster than most expect. Enterprises should be preparing for quantum computing today.

Quantum computing promises great advances in computing capability. Because it can process information in parallel — rather than in series, as is the case with classic computing — it is able to perform some calculations in a fraction of the time that traditional computers would take. This means that previously difficult challenges facing computing, such as mapping chemical formulas and solving logistics conundrums, may be revolutionized using quantum computing.

The downside to this massive increase in computing capability is that it directly undermines much of our public key encryption infrastructure, which underpins ecommerce, email, VPNs, and most other forms of digital communication.

AT A GLANCE

WHAT IS IMPORTANT

Quantum computing is arriving soon — sooner than you think.

Malicious actors are harvesting data now for decryption later.

Public key cryptography, which underpins secure data transmission, is vulnerable now.

KEY TAKEAWAYS

Quantum computing should be on today's risk register, and enterprises should take mitigating steps now.

Quantum-safe approaches are available, and some are simple to deploy.

Look for solutions that are backed by standards and a credible ecosystem of regulatory bodies and technology partners.

Public key cryptography (PKC) is the mechanism most often used to secure online transactions. It is so popular because it solves a major headache in cryptography, that of key exchange: To communicate securely, two parties first need to agree a key, which is secret and needs to be agreed in advance. Public key cryptography solves this circular conundrum by allowing parties to create private keys by sharing public information.

It sounds counter-intuitive, but it is based on one-way or asymmetric mathematical functions, such as prime number factorization and elliptic curve algebra. One-way functions are easy to compute in one direction but very hard to undo using classic computing approaches. A cryptographically relevant quantum computer (CRQC) changes that equation, making it much easier to undo and therefore much easier to decrypt traffic.

Quantum computers (QCs) are not yet sufficiently stable to be commercially viable, but they are advancing at a rate that indicates a viable quantum capability will become available by 2030, if not sooner. Many nefarious organizations are capturing encrypted traffic today with the prospect of being able to decrypt these messages at some point in the future, a process known as harvest now, decrypt later (HNDL). So, even though quantum computing is not commercially available

today, enterprises need to be aware of the threat and take steps to protect their data in transmission.

Prioritizing for a Post-Quantum Era

With quantum computing arriving in the foreseeable future, valuable data that also has longevity is most vulnerable, such as:

- Data relating to defense and intelligence, and sensitive government information
- Financial services data, especially long-life information like insurance policies and long-term loans
- Healthcare data, which, by definition, lasts the lifetime of each patient
- Telecommunications data, such as subscriber databases and systems that facilitate the transmission of other enterprises' valuable data

Because of the HNDL threat, and as a matter of urgency, quantum computing should be on the risk register of companies, and board members should be asking their technology and security teams to advise on their post-quantum business and technology strategy. Enterprises should look to enhance the security of their network infrastructure, including VPNs. Datacenter-to-datacenter communication is also a matter of priority, as are multicloud environments with voluminous data transmission (ingress and/or egress). And better authentication to minimize spear-phishing attacks in particular will also be a priority for many organizations.

The good news is that several solutions are emerging that increase the security regime of data in transmission and substantially reduce the risk from quantum-based decryption. While such solutions can be complicated and expensive, they are relatively straightforward to implement and use proven approaches that have manageable risk profiles. Arqit's SKA-Platform™ is one such solution.

Benefits

There are three steps in establishing key creation and agreement based on symmetric keys and a cloud-based encryption platform:

- Initial authentication of the devices to be secured
- Key distribution or agreement (sharing or pre-sharing)
- Encryption of the message with the key

Initial Authentication

Each endpoint (physical or virtual — e.g., laptop, firewall, or cloud application) is issued with a root of trust (a pre-shared key) that establishes a trusted relationship with a cloud service (expressed as a symmetric key shared between the endpoint and the cloud service). This initial key is delivered using either a quantum-safe method, such as a mixture of post-quantum algorithms (PQAs), or "manual injection," and therefore any data sent from the cloud to the endpoint can be made quantum safe.

A mixture of PQAs is preferred, as it establishes defense in depth, meaning multiple encryption methods need to be broken to recover the encryption key, making it that much harder for an attacker. The manual (out-of-band) approach is viable but, realistically, only for low-scale use cases or when maximum security is needed.

Key Agreement

With the initial authentication between endpoints and the cloud platform in place, any pair of endpoints can agree keys with each other by receiving key material from the cloud platform. Endpoints mix the key material with other ingredients to achieve "split trust" security, meaning an attacker would need to compromise several different channels to steal the encryption key. Keys are rotated every session using the same process to minimize the amount of data encrypted using one particular key. This is good key hygiene but not as commonly practiced as it should be. A ratcheting process ensures that a new authentication key is also created every session, reducing the risk of man-in-the-middle or spoofing attacks.

Encryption

An important element is the use of symmetric encryption. In contrast to asymmetric PKC, symmetric encryption is considered quantum resistant. AES-256, for example, is considered quantum safe because it has a fundamentally different mathematical structure that is not based on asymmetric algebra. Endpoints can use AES to communicate securely using the shared symmetric key. Again, as key ingredients are mixed, the cloud service does not know the final key.

The benefits of this approach are:

- **Simplicity**: The symmetric key agreement approach is easy to deploy via the supporting cloud platform. It integrates with existing infrastructure, including network security equipment from leading vendors like Fortinet and Juniper Networks. It uses existing cryptographic approaches based on established and quantum-resistant symmetric encryption, and so no new or untested algorithms are required. Integration with existing key management systems is also possible.
- **Credibility**: Symmetric key agreement uses well-established encryption mechanisms backed by standards bodies, such as NIST, NSA (CSfC), the U.S. National Information Assurance Partnership, and the IETF's TLS v1.3. It is compliant with the IETF's RFC-8784 for IKE v2 standard, which supports mixing pre-shared keys into IPsec.
- **Addresses urgency**: A cloud-based and symmetric key approach can be blended into existing public key approaches or replace them. It does not require access to a quantum computer or even any non-standard infrastructure, and it works with existing cloud variants and a multitude of device types, including Internet of Things (IoT) devices.

Considerations

Are quantum computers imminent? One of the main challenges with QCs is the lack of stability of qubits. IBM has demonstrated a QC with 1,000 qubits, and DWAVE has a 5,000-qubit system on the market. The trouble is, those qubits are inherently unstable and are thus prone to error. The

standard approach to resolving this, in addition to cooling at near-absolute zero degrees, is to use more qubits to compensate for qubit instability, but the number of qubits required for this error correction increases by several orders of magnitude. Most scientists think that a QC with millions or billions of qubits is required to crack a typical asymmetric key.

However, the rate at which QCs are growing indicates that systems with 100,000 qubits are foreseeable by 2027. In addition, error correction is improving markedly, bringing the number of error-correcting qubits down to more manageable levels. And improvements on Shor's algorithm, a quantum-based method of factoring large numbers, are also happening. These three factors make the realization of a functional and useful CRQC realistic within this decade — possibly much sooner.

Introducing quantum-safe capabilities should now be on the agenda for all organizations creating long-life data that has value (either extrinsic or via compliance obligations). Several approaches are available, including replacing mathematically reliant PKC algorithms with PQAs. PQAs are theoretically quantum-resistant, but none is definitively proven to be so. In addition, they all use long key lengths (much longer than AES-256 or typical asymmetric keys), which reduces efficiency. This is important in large-scale data transmission use cases (email, ecommerce, etc.).

PQAs have limitations but can be used in a narrow way within an initial authentication stage:

- Strong PQAs can be used. These generally have much larger key lengths than those used in PKC, which impairs efficiency of transmission, but they are practical if used selectively.
- PQAs are used in a one-time manner, between endpoints and the cloud platform, and are not used on an on-going basis.
- Mixing with other PQAs reduces vulnerability resulting from a single PQA being compromised.

Key exchange must always be a consideration. Quantum technology introduces the prospect of key distribution using quantum particles that exhibit superposition. Such quantum key distribution (QKD) approaches enable keys to be exchanged with the absolute certainty that no eavesdropping has occurred. But, as highlighted by the U.S. National Security Agency and Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI), QKD requires dedicated and expensive infrastructure. This might suit some organizations, but most will seek to make incremental changes to their existing cryptographic regimes.

Trends

Implementing a cloud-based encryption platform is consistent with several current security initiatives that can be leveraged to support a cloud-based post-quantum approach to key agreement and management.

For example, secure access service edge (SASE) is an integrated cloud service that emphasizes the convergence of networking technologies, such as software-defined wide area network (SD-WAN), and network security technologies, such as firewall as a service, secure web gateway

(SWG), and cloud access security broker (CASB). The SASE approach to modern security architecture maps well onto cloud-based encryption platforms.

Similarly, zero trust is an approach that minimizes assumed verification between entities in a connected system. Zero trust architectures continually ask for authentication before allowing access to data and workloads, and they encrypt transmitted data. A more efficient and quantum-safe approach is to use a symmetric key method. Data could be exposed using a stolen key, so rotating authentication, which changes the authentication key every second, removes this risk.

Distributed infrastructure now extends to edge devices that are both high in number and low in resources. Such devices, like operational technology (OT) control systems and IoT networks, can benefit from cloud-based authentication architectures using shorter symmetric key lengths.

Conclusion

Any PKC-secured transmission of valuable long-life data is vulnerable to quantum computers, so secure (quantum-resistant) transmission is essential. Malicious actors are scooping up encrypted transmissions today for decryption once QC is available. So, companies transmitting valuable long-life data should be using quantum-resistant encryption now.

Arqit's approach to this situation is to deploy straightforward and proven standards-based solutions, coordinated via a trusted cloud service. This approach also delivers enhanced security against man-in-the-middle attacks, as well as against the future quantum threat. A cloud-based platform reduces the administrative burden and inefficiencies of current symmetric encryption solutions.

Importantly, Arqit's approach minimizes reliance on unproven and as-yet unstandardized PQAs and maximizes the use of strong, standardized, and proven symmetric methods like AES-256. Keys are generated on endpoints, not shared or distributed, thus avoiding key distribution vulnerabilities.

Enterprises must act now to protect vulnerable data. The emergence of cloud-based encryption platforms like Arqit's SKA-Platform™ means that the transition to a post-quantum architecture is manageable and affordable for affected companies.

MESSAGE FROM THE SPONSOR

Arqit supplies a unique quantum-safe encryption platform as a service that makes the communications links and data at rest of any networked device or cloud machine secure against current and future forms of attack — even from a quantum computer. For more details, please visit https://arqit.uk/.

About the Analyst

Duncan Brown, Group Vice President

Duncan Brown leads European research for the software, services, cloud, security, sustainability, digital business, and IPDS areas, as well as the channel partner and ecosystems research teams. Duncan's analysis and opinions are widely sought by industry leaders and investors, while his comments on industry trends and developments frequently appear in leading business and trade publications. Duncan Brown leads IDC's pioneering EMEA Chief Information Security Officer (CISO) research program.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data and marketing services company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.