Future-Proofed

The Journey Toward Quantum-Safe Security

Vanguard Report

April 2022

Commissioned by

IBM

451 Research

S&P Global
Market Intelligence

About the Author

John Abbott

Principal Research Analyst, 4SIGHT

John Abbott covers systems, storage and software infrastructure topics for 451 Research, a part of S&P Global Market Intelligence. Over a career that spans more than 30 years, he has pioneered specialist technology coverage in such areas as Unix, supercomputing, system architecture, software development and storage.

As one of the co-founders of The 451 Group in October 1999, John ran analyst operations from the company's San Francisco office. He has been a principal author on many 451 Research Special Reports, including those on storage virtualization and blade servers – the first comprehensive surveys of either subject to be published. More recently John has focused on topics such as converged infrastructure, new systems architectures, AI and deep learning accelerators. He helped establish 4SIGHT, the 451 Research framework for the forward-looking, long-term coverage of emerging technologies.

John began covering the technology sector in 1984, building on his previous experience as a technical author and direct involvement using mainframes, early PCs and Unix workstations. As a freelance journalist, he contributed to publications including Computing, Computer Weekly, The Financial Times and The Times. In 1987, he was appointed editor of ComputerWire's weekly Unix newsletter, Unigram.X, and later became editor of the company's daily Computergram International service, first in London and subsequently in San Francisco. He established the 451 Research office in San Francisco and lived there for over a decade.

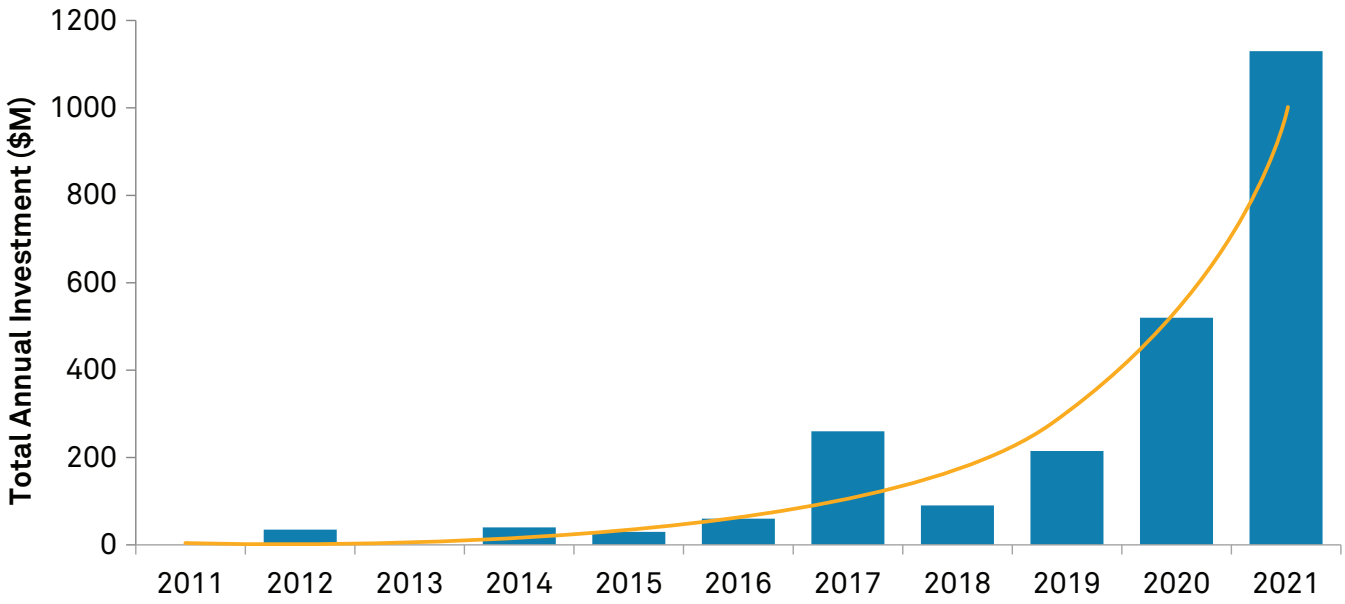
John studied music at the University of Keele and has an MA in modern English literature from the University of London.

Introduction

Quantum computing today is best described as a high-risk, high-reward investment. There are no guarantees that a universal and practical quantum computer is feasible in our lifetimes. But research labs – and, increasingly, private companies in the technology sector – are breaking barriers every day and innovating at the cutting edge of science. And the payoff could be colossal, solving problems that are currently beyond the capability of any (classical) supercomputer. This explains why both sellers and users are taking chances on the potentially disruptive technology. Data from S&P Capital IP Pro (Figure 1) shows that quantum startups won $2.4bn in investment over the past decade. 2021 marked a major influx of interest, with $1.1bn of investment in quantum companies. And that data doesn't include the massive investments made by established IT companies, including IBM, Amazon, Google and Honeywell.

Along with the opportunity come some major concerns. Perhaps the most pressing is the threat to current-day security practices. Armed with quantum computing, malicious actors would be able to forge digital signatures and crack current levels of cryptography and encryption, including the public key infrastructure that's now deeply embedded within the world's IT systems. Worse, even encrypted data that is currently protected might be stored for later decryption once practical quantum computing emerges. This is a problem that can't be deferred. The longer we wait, the more data we'll be creating that is at risk.

Figure 1: Investment in Quantum Computing Startups



Source: S&P Capital IQ Pro

The 451 Take

It's not possible to predict exactly when a quantum computer that can run Shor's algorithm effectively will become widely available such that a malicious actor could have access to it. So far, no IT vendor has provided a definite timeline for when quantum computing will meaningfully outperform classical computers. But rapid advances in technology over the past five years, along with the significant investments now in place, suggest that day will come, perhaps by the end of the decade. When it does, all the information currently protected by public key algorithms will be threatened with exposure. For government defense and intelligence agencies, and for cloud service providers and system vendors whose customers are in the regulated industries, the risk is already too high to ignore. Despite the false alarms of the past (think Y2K, when a widely used computer programming shortcut threatened to wreak havoc as the year changed from 1999 to 2000) and the unknowns of the future, one thing is clear: Danger from cyberattacks is a huge issue today, and the nature of threats and vulnerabilities is constantly evolving. Security policies need continuous review and update, and quantum-safe cryptographic technologies, alongside the implementation of crypto agility and a cryptographic inventory, are now a vital part of the equation.

Quantum-Resistant and Quantum-Safe Scenarios

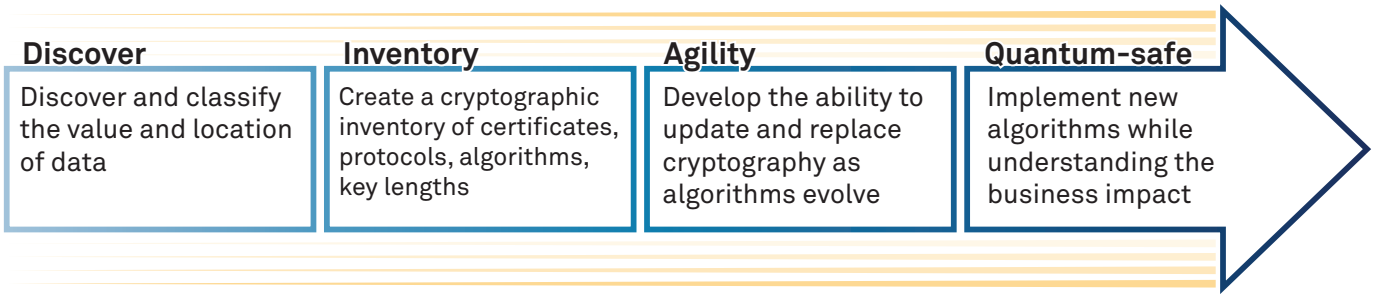
The problem is this: The current generation of widely used security algorithms is based on hard mathematical problems, too difficult for classical computers to break. But these problems could easily be solved by a quantum computer of sufficient power, a premise that's been widely accepted since 1994, when the American mathematician Peter Shor discovered the polynomial-time algorithm now known as Shor's algorithm. The first quantum computer was built three years later. Development of quantum-safe algorithms has been progressing well over the past decade. But conversion from the public key cryptography systems in widespread use today throughout government and industry to a new set of algorithms could take decades.

That's why organizations such as the National Institute of Standards and Technology (NIST) and the Department of Homeland Security in the US have been working on both the standardization process of the algorithms themselves, and on recommendations to help companies prepare for the transition to post-quantum cryptography. That work led to a White House memorandum in January mandating that government defense and intelligence services start making the switch.

Cracking open a 2,048-bit composite integer (by finding the prime factors) on the most powerful computers available today would take millions of years. On a quantum computer, that task could theoretically be completed in several hours. Current public key schemes broken by Shor's algorithm include the venerable RSA algorithm – now 45 years old but still used in almost all internet-based transactions – as well as Data Security Standard, the Paillier cryptosystem, elliptic curve digital signature algorithm, elliptic curve Diffie-Hellman and ElGamal encryption. A long list of standards established by NIST, ISO/IEC, ETSI and IETF are affected, which indicates that the problem is an international one: The Chinese SM2 digital signature algorithm and SM9 national cryptography standard are also broken.

The NIST standards process, which started in 2016 with a call for proposals, has identified a new set of quantum-resistant candidates. After three rounds of evaluation and analysis, NIST has selected the first algorithms it will standardize as a result of the post-quantum cryptography (PQC) standardization process. The public-key-encapsulation mechanism (KEM) that will be standardized is CRYSTALS–KYBER. The digital signatures that will be standardized are CRYSTALS-Dilithium, FALCON and SPHINCS+. While there are multiple signature algorithms selected, NIST recommends CRYSTALS-Dilithium as the primary algorithm to be implemented. The PQC standardization process is continuing into a fourth round with the following KEMs still under consideration: BIKE, Classic McEliece and HQC. NIST is requesting additional digital signature proposals to be considered in the PQC standardization process. Round four started in 2022 and will be completed by the end of 2024.

Figure 2: Maturity Milestones Toward Quantum Safety



Source: 451 Research

The Road to Quantum-Safe Cryptography

What actions should organizations be taking now to prepare for the incorporation of quantum-safe cryptography in their information security architectures over the next decade? The first step, already underway, is to participate in the standardization process. It's important for any organization with a stake in preventing fraudulent authentication, protecting encryption integrity and avoiding compromise of digital signature to take an active part to ensure their requirements are met by the approved list of final algorithms, processors and tools. Despite good progress from the standardization bodies, it's an ongoing task: More algorithms will be required. Beyond that, the following maturity milestones lead to quantum safety.

- **Data discovery and classification:** Take an inventory of critical data. Which has the highest value? Where is data located? What are the compliance requirements? This understanding is critical because many organizations won't be fully aware of what they have or its value. Without this knowledge, they can't identify their most serious vulnerabilities. They must create and manage a data inventory with defined ownership.
- **Crypto inventory:** A cryptography inventory details where and how vulnerable public key cryptography is being used, and it contains details such as certificates, encryption protocols, algorithms and key lengths. The inventory must be managed to cover the full lifecycle of certificates and encryption keys.
- **Crypto agility**: Within their plans and transition processes, organizations need to consider crypto agility so they can make adjustments with less pain as technology evolves and circumstances change. They should design and implant processes so they can update or replace current-generation cryptography – and then test it – more easily within well-defined lead times.
- **Quantum-safe**: Organizations must implement new algorithms with an awareness of the potential performance impact of quantum-safe crypto on the business.

Every organization is different, and not all organizations will be in a position (or of a mindset) to change everything, for example due to expense or the problems of lifecycle management. But designing in the ability to update or replace security protocols is crucial both in the shorter and longer term. Because it's closely related to the system infrastructure, achieving crypto agility will require the cooperation of system designers, application developers and security experts. There is currently a lack of tools available to help with this process.

Organizations will use a variety of factors to prioritize quantum-safe cryptographic replacement: the value of assets protected; the vulnerability of what's being protected (i.e., key stores and passwords); which connected systems could be affected (i.e., information sharing with outside entities, including federal agencies); and how long data needs to be protected. Hybrid schemes, combining classical and quantum-safe algorithms, will be necessary during the lengthy transition period.

Implementation, Motivation and Drivers

System vendors and the large cloud service providers whose equipment and infrastructure hosts mission-critical enterprise workloads don't have the luxury of waiting for the quantum-safe cryptography standards to be fully completed. They have been working on this problem for several years and have contributed to the choice of algorithms and protocols that are front-runners to make the finalized standards list in 2024. A number of cloud-based key management services already support round two and round three algorithms. Customers are starting to use these services to measure potential performance impacts on their applications from likely additional overhead on bandwidth utilization and latency, and also to mitigate likely connection failures at the Transport Level Security proxy layers. But everyone agrees that the transition to quantum-safe will be a multi-year journey as the standards and technology evolve, and that the journey begins by securing core infrastructure.

In the systems world, mainframes are still in widespread use as highly available and secure core infrastructure for the largest banks, insurance companies, telecommunications, retail and transportation businesses – a position they've maintained for over half a century. The newest generation of mainframes will come equipped with hardware security modules that are quantum-safe, working in conjunction with updated operating system components, key management APIs and support for a suite of the emerging quantum-resistant algorithms. Quantum-safe secure boot technology with a hardware root-of-trust will be used to protect system boot firmware integrity, and quantum-safe mechanisms for the secure exchange of cryptographic keys with business partners will be provided through application programming interfaces.

Cloud service providers and vendors must play a significant role in helping their customers make the switch to quantum-safe cryptography. Regulatory pronouncements on their own are not enough, partly because they are typically not prescriptive enough to provide clear guidelines for user organizations without significant expertise of their own. Vendors already at the center of mission-critical infrastructure can make the process easier by providing core business system protection without additional system-level changes for enablement. They can also provide much-needed discovery tools for crypto-application analysis. Organizations responsible for data need to ensure that their data is protected across its lifecycle – for today and in the future – because data encrypted using classical algorithms today might be decrypted by an advanced quantum computer in the future. If that data must be secured for 20 years, then that takes us well into the 2040s. Even skeptics who believe that practical quantum computing is still many years away must acknowledge that, given the current rate of progress, the likelihood will have significantly increased by then.

Conclusions

The business case for quantum computing is strong – a fully realized quantum computer would enable opportunities for advancement in chemistry, machine learning, finance, transportation, healthcare and beyond. Quantum computers would exponentially accelerate the processing of equations that are impractical to run on the classical, deterministic computers in use today.

On the flip side is the effect quantum computing could have on the already growing threat to data protection and privacy from cyberattack. As the business value of data increases, so does the scale and cost of data protection requirements. And because the value of data is long-lasting, the increasing likelihood that quantum computing will become a practical reality in the foreseeable future must be taken into account. Acting sooner rather than later would result in a safer, more controlled evolution toward quantum-safe core infrastructure, the implementation of tools able to discover current application-layer vulnerabilities, the protection of key exchange systems used across organizations, and the continued protection of long-lasting secrets held in the data.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence