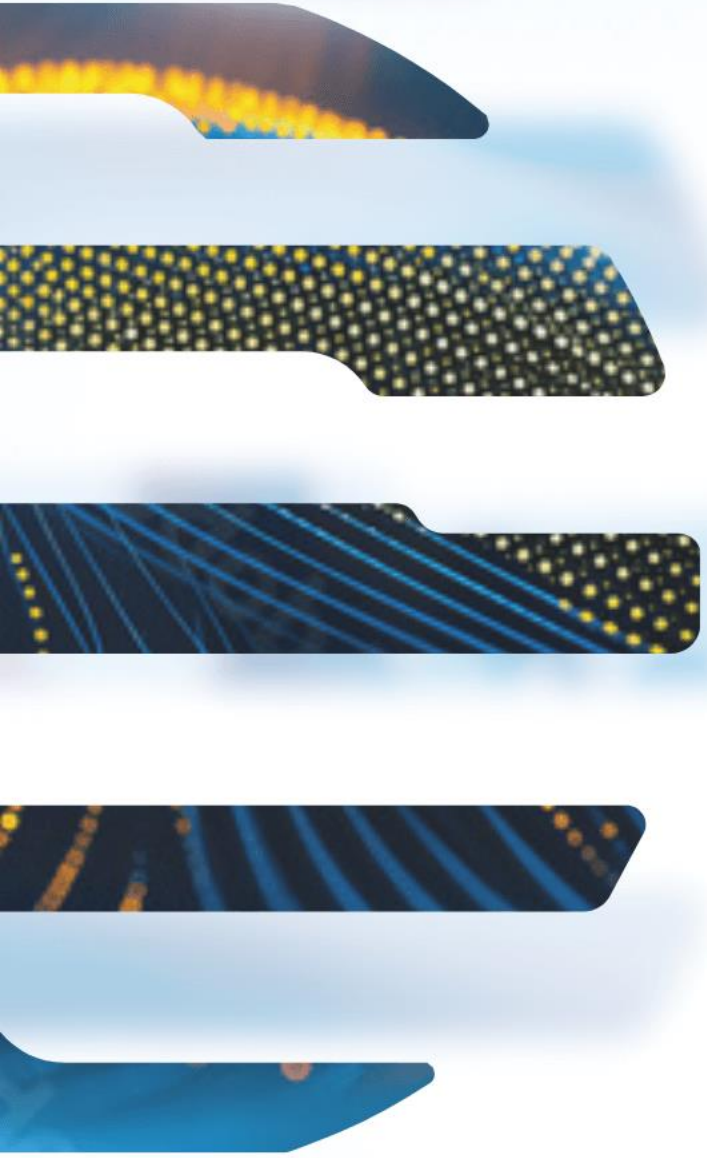


IDC Innovators: Post-Quantum Cryptography, 2024

THIS IDC INNOVATORS EXCERPT FEATURES ARQIT

Heather West, PhD

September 2024

IDC #US52524924e

In this Excerpt

The content for this excerpt was taken directly from IDC Innovators: IDC Innovators: Post-Quantum Cryptography, 2024 (Doc # US52524924).

Synopsis

This IDC Innovator presentation identifies five emerging post-quantum cryptographic (PQC) vendors that are providing transformative solutions enterprises can use to protect classical data and infrastructure with a long shelf value from the risk of a potential quantum cyberattack. However, the migration process can be overwhelming. Until recently, there was very little guidance as to which PQC algorithms and technology would be most effective for certain situations. In August 2024, the U.S. Department of Commerce's National Institute of Standards and Technologies (NIST) released the final FIPS standards for three PQC algorithms. Now, enterprises have the necessary guidance they need to begin the migration process. This IDC Innovator presentation provides a summary of some of the PQC offerings available from a select group of emerging vendors.

"The advent of quantum computing is a double-edged sword, offering unparalleled compute power while posing unprecedented cybersecurity challenges. The transition to post-quantum cryptography may seem daunting, but with the right resources, strategic planning, and trusted partnerships, enterprises can ensure the protection of sensitive data against future quantum cyberattacks."

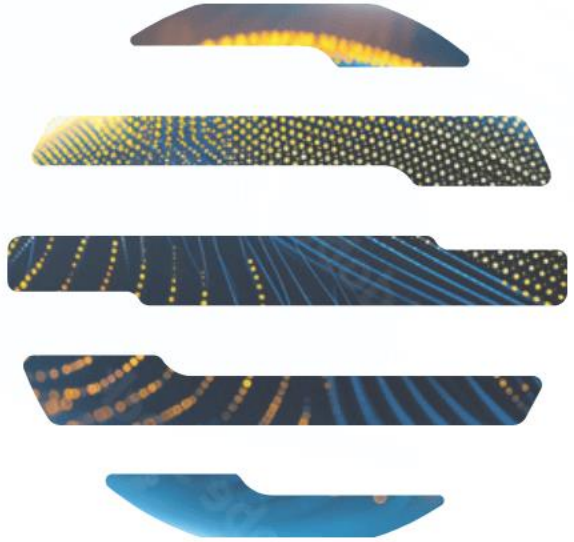
Heather West, PhD
Research Manager, Quantum Computing Research Lead
IDC Information Systems, Platforms, and Technologies Group

Executive Summary

Currently, classical computing encryption used to protect sensitive data stored, transferred, and accessed via cloud computing and classical infrastructure is made possible with classical algorithms. Using classical computing technology, hacking these algorithms can be nearly impossible, depending on the algorithm used. Comparatively, the quantum properties of qubits, specifically superpositioning and entanglement, will provide the exponential compute power needed to solve complex mathematical problems, including those that make up current classical encryption algorithms. As a result, quantum computing technology will enhance a hacker's ability to crack a classical encryption algorithm in fewer tries. As a result, classical encryption protocols will not easily withstand cyberattacks launched using quantum technology.

For years, it was thought that at least 1 million high-quality qubits would be needed to solve some of the intractable problems that are beyond the scope of classical compute infrastructure. Yet recent advancements in quantum computing hardware and software, as well as error mitigation and suppression techniques, suggest that the quantum era might be approaching faster than expected. In fact, some quantum hardware vendors suggest that these, and future, advancements will enable quantum systems made up of less than 1 million qubits to deliver smaller-scale, near-term advantage. By 2030, it is possible that the world will be introduced to a quantum-centric supercomputer made up of 100,000 qubits. These systems are expected to be capable of solving complex algebraic math problems such as those that are used to protect today's classical data stored on classical compute infrastructure.

It is speculated that some cybercriminals are stealing data with a long-shelf value today to decrypt tomorrow. Whether or not an organization is investing in quantum computing, the risks that quantum computing poses for data encryption should be top of mind. To protect against these and other unknown threats, enterprises must start investing and implementing quantum-resilient solutions to protect their sensitive data. This IDC Innovator presentation identifies five emerging vendors that offer solutions and services to assist with this transition.



VENDOR PROFILE

Arqit

Vendor Profile: Arqit

IDC Innovator® | Arqit

Founded
2017

Number of Employees
80

Headquarters
London, England

Founders
David Williams
David Bestwick
Barry Childe

Product/Service Description
Symmetric Key Agreement Platform
NetworkSecure
TradeSecure

Funding
Nasdaq listed (ARQQ; ARQQW0) in September 2021 after a SPAC merger
$158 million in capital investments total resulting from both Series A and SPAC

Source: IDC, 2024

Why Arqit Was Chosen as an IDC Innovator

Established in 2017, Arqit has developed the Symmetric Key Agreement Platform (SKA) that allows enterprises the ability to control network access and manage permissions across endpoints and users. To ensure the security of a network, all endpoints or devices must be registered or provisioned with a bootstrap key using a combination of multiple post-quantum algorithms over the air or through manual key delivery for ultra-high security scenarios. Only then can the endpoint authenticate with the SKA Platform. During this process, Arqit's proprietary ratcheting is employed to ensure forward secrecy. When multiple devices want to create a symmetric key, each device must authenticate and establish a quantum-safe tunnel with the SKA Platform. This tunnel leverages additional key material exchanged over non-quantum-safe channels in a split trust model to further enhance security. As a result, the key is never stored or known. In addition to the SKA Platform, Arqit has released TradeSecure and NetworkSecure Adaptor. TradeSecure generates and distributes digital trade finance instrument as a means of protecting finance supply chains against quantum cyberattacks that may cause disruption. Arqit's NetworkSecure Adaptor software application integrates with existing infrastructure to protect VPN communications from quantum attacks.

Vendor Profile: Arqit

Innovator Assessment

1

Compliance with Standards

Arqit places a strong emphasis on adhering to established standards. Arqit's solutions are built on well-known, standardized cryptographic primitives like hash functions and AES-256 block ciphers. This approach ensures that their security properties are well understood and trusted.

2

Market Readiness

Arqit's quantum-resilient cryptographic solution is already at general availability as the vendor is already actively selling these solutions through channel partners. Arqit's solution is designed to be integrated with existing hardware and software solutions, making it practical and easily consumable by end users without requiring them to manage or understand the underlying quantum-resistant algorithms.

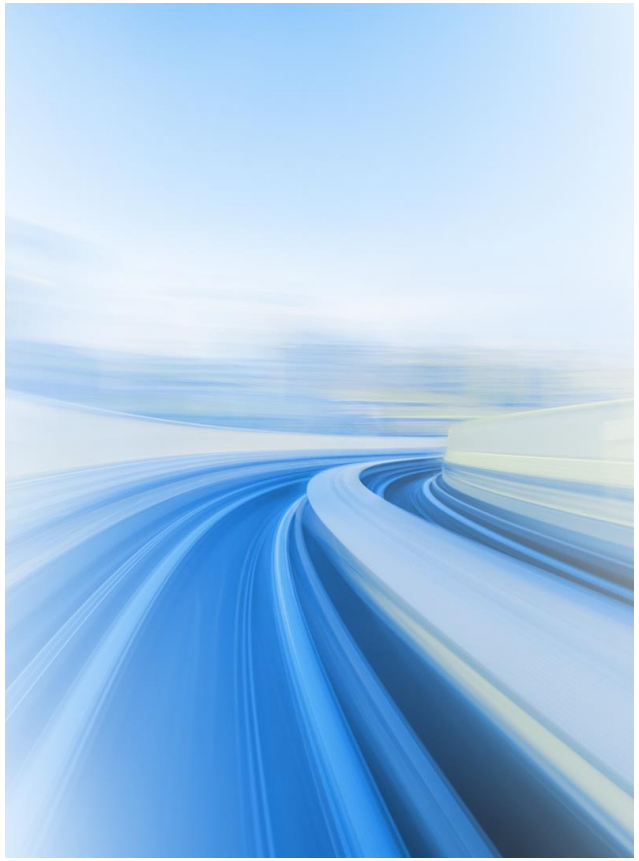
3

Promote Cryptographic Agility

Arqit employs a hybrid cryptography model, mixing several post-quantum algorithms with classical algorithms like Diffie-Hellman. This approach is adaptable and ensures that Arqit's solutions can evolve with the cryptographic landscape, particularly as standards around post-quantum cryptography solidify. Further, the technology is designed to be agnostic to the underlying algorithms, allowing for easy updates or changes to cryptographic methods as needed. This is crucial for maintaining security against future threats.

Vendor Profile: Arqit

Key Differentiators



Focus on Practicality and Usability

Arqit's solutions are designed to be practical and easily integrated into existing systems. Arqit's solutions avoid the complexity often associated with quantum-safe technologies, such as the need for customers to choose between different post-quantum algorithms.

Partnerships with OEMs

Arqit's go-to-market strategy involves integrating the company's technology with the products of OEM partners like Fortinet, Juniper, Cisco, Hewlett Packard Enterprise (HPE), and Intel. This integration makes quantum safety more accessible and eliminates the need for end users to manage or understand the underlying quantum-resistant algorithms.

Third-Party Accreditations and Evaluations

Arqit's quantum-resilient cryptographic solutions have undergone evaluations and received accreditations from reputable third parties, including a Tamarin proof of their protocols by the University of Surrey. In addition, Arqit has demonstrated compliance with the National Security Agency's (NSA's) Commercial Solutions for Classified Program's Symmetric Key Requirements Management Annex v2.1.

Vendor Profile: Arqit

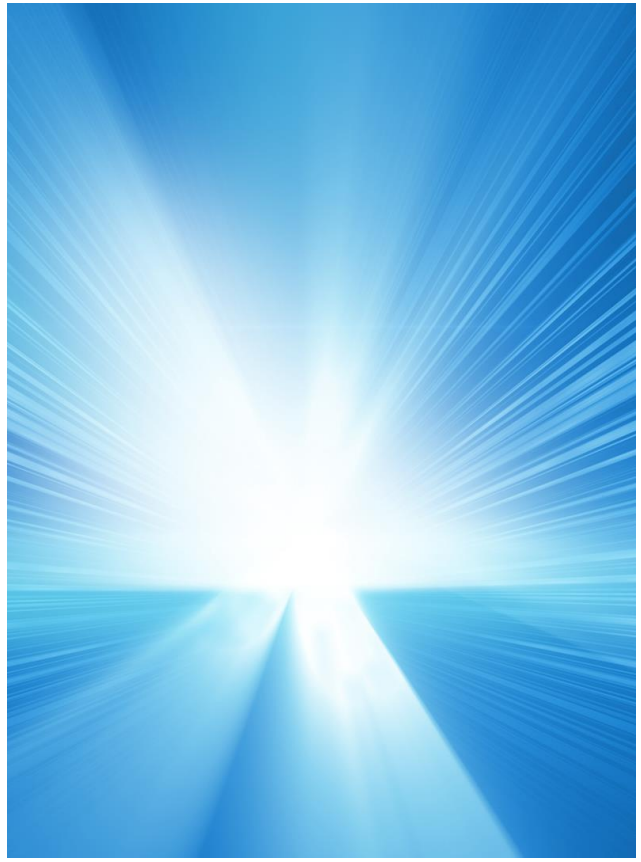
Challenges

Maintaining Relevancy in a Slowly Maturing Market

Like all new technology markets, the quantum-resilient cybersecurity market is made up of several established and start-up vendors. Maintaining relevancy in the quantum-resilient cybersecurity market will be particularly challenging. Many organizations delayed their adoption of quantum-resilient cryptographic solutions until the release of NIST's final PQC recommendations. With this release, enterprises now find themselves with several options from multiple vendors. To stay relevant, it is important that Arqit continues to develop industry partnerships that will help promote and integrate the SKA Platform, as well as grow and evolve the company's product and service offerings.

Lack of a Publicly Available Developmental/Product Road Map

With quantum computing being a nascent technology, there are many uncertainties surrounding the technology. One such uncertainty is whether today's quantum-resilient cryptographic solutions will remain relevant as quantum computing technology continues to advance. Because of this, many potential customers rely on developmental or product-related road maps to determine if a particular solution will be suitable for both current and future needs. Currently, such a road map does not appear to be available, or easily accessible, for Arqit's SKA Platform.



Technology Definition

Post-Quantum Cryptography

Post-quantum cryptography includes cryptographic algorithms designed to be quantum-resilient — that is protect high-risk data with a long-shelf life, as well as the infrastructure on which these data are stored, processed, or transferred, against a cybersecurity breach powered by a quantum computer.

Quantum Random Number Generation/Entropy Seeds

The quantum random number generation (QRNG)/entropy seeds market segment includes technologies capable of generating random numbers and entropy seeds using quantum computers. Because these numbers and seed are truly random, they can never be replicated. QRNG and entropy seeds can be used to encrypt data that is transmitted across a communication network.

Quantum Key Distribution

Quantum key distribution (QKD) differs from post-quantum cryptography and quantum random number generation in that it is being developed to protect quantum data transferred across a quantum network. Specifically, QKD will allow for data to be encoded into the quantum states of photons. If eavesdropping were to occur, the instance would be easily identified given the final state of photon at the end of the transmission.

To learn more, see *IDC's Worldwide Quantum Computing Taxonomy, 2024* (IDC #US51684624, March 2024).

IDC Innovators Inclusion Criteria

An "IDC Innovators" document recognizes emerging vendors chosen by an IDC analyst because they offer an innovative new technology or a groundbreaking business model, or both, and were approved by the IDC Innovators Review Panel. It is not an exhaustive evaluation of all companies in a segment or a comparative ranking of the companies.

An IDC Innovators document highlights vendors that meet the following criteria:

- In IDC's opinion, the company exhibits innovative technology or a new business model.
- The company's annual revenue is under $100 million at the time of selection.
- Customers are currently using the company's products and services (i.e., the products and services are not conceptual or in the process of being released).
- The product, service, or business model must solve or help alleviate an IT buyer challenge.

In addition, vendors in the process of being acquired by a larger company may be included provided the acquisition is not finalized at the time of publication of the document. Vendors funded by venture capital firms may also be included even if the venture capital firm has a financial stake in the vendor's company.

Related Research

Document Title	IDC Document Number	Publication Date
NIST's Post-Quantum Cryptographic Standards Revealed	lcUS52523724	August 2024
Quantum-Safe Telco Networks: An Overview	EUR152400724	July 2024
IDC's Worldwide Quantum Computing Taxonomy, 2024	US51684624	March 2024
Apple PQ3: Quantum-Resilient iMessaging Data Security	lcUS51909524	February 2024
IDC FutureScape: Worldwide Emerging Technologies 2024 Predictions	US51082023	December 2023
Understanding the New NIST Post-Quantum Cryptography Algorithms to Enhance Data Trust	US51236223	September 2023
NIST Releases Draft FIPS Standards for Post-Quantum Cryptographic Algorithms	lcUS51190823	August 2023
IDC TechBrief: Applying Post-Quantum Cryptography to Data Protection to Enhance Digital Trust	US50789923	June 2023

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, IT benchmarking and sourcing, 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.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
508-872-8200
https://x.com/idc
https://blogs.idc.com
https://www.idc.com

Thank You

IDC.com

linkedin.com/company/idc

x.com/idc

blogs.idc.com