Case study

Enterprise Security
Quantum-safe Encryption

Confidential Compute: Quantum-safe Strategies for Hybrid Cloud

A strategic collaboration between Arqit and Intel focuses on advancing quantum-safe encryption solutions that secure AI, edge, and cloud computing environments.

At a glance:

- By placing Arqit's NetworkSecure Adaptor in a Trusted Execution Environment (TEE), enterprises can secure network connections between on-premises environments and the cloud, with robust isolation and secure communication.
- Working together, Intel and Arqit engineers transformed an idea for quantum-safe computing into a working demo in just two weeks.
- The combination of Arqit's lightweight software agent and Intel® Trust Domain Extensions (Intel® TDX) adds a post-quantum cryptography (PQC) solution to the network connections between TEEs that significantly reduces security vulnerabilities.

Challenge

Security threats are evolving at an unprecedented pace, which poses significant challenges to businesses across all sectors. As AI and generative AI (GenAI) become part of everyday workflows, companies need to be able to protect their data and custom AI models, both on-premises and in cloud deployments. Beyond the typical data breach, a larger concern looms: the threat posed by quantum computing. Quantum computers are believed to have the capability to crack traditional cryptographic technologies. "Harvest Now, Decrypt Later" (HNDL) is a real and present danger, where adversaries are actively stealing encrypted information with the intent to decipher it once Cryptographically Relevant Quantum Computers (CRQCs) become available. This underscores the urgent need for robust security measures that can withstand future technological advancements.

Arqit Quantum Inc. (Arqit) supplies a unique encryption software service which makes the communications links of any networked device or cloud machine secure against both current and future forms of attack on encryption - even from a quantum computer.

What is Quantum Computing and why could it be a threat?

Quantum computers can vastly outperform classical machines. Current estimates suggest that a fault-tolerant quantum computer with around 20 million qubits could factor a 2048-bit RSA key in about eight hours[1], a task that would take classical computers roughly one billion years. This means today's public-key cryptography would be broken almost instantly, exposing sensitive data, critical business assets, and national secrets.

Learn more by **watching this video**.

Solution

Arqit is a leading solution provider in post-quantum cryptography. Its cutting-edge technology delivered as a service is combined with a lightweight software agent that delivers a quantum-safe crypto key agreement system. The data channels between workloads, isolated with confidential computing, are protected by the deployed solution.

Arqit's Symmetric Key Agreement Platform (SKA-Platform)[2] establishes symmetric encryption keys[3] between endpoints, ultimately making these encrypted communications quantum-resistant. This provides protection against traditional man-in-the-middle attacks and HNDL spoofing attacks. Arqit's capability to provide quantum-resistant symmetric key agreements for VPN connections conforms to National Institute of Standards and Technology (NIST) standards and is compliant with the RFC-8784 specification defined by the Internet Engineering Task Force (IETF).

This protects data-in-transit, but data may still be vulnerable when in use on public cloud. Intel® Trust Domain Extensions (Intel® TDX) is a hardware-based security technology in modern Intel® Xeon® processors that enables Confidential Computing through Trusted Execution Environments (TEEs), also known as Trust Domains (TDs). Intel TDX isolates workloads from the underlying infrastructure—including the hypervisor and other system components—by encrypting data while it is in use.

This runtime protection helps prevent unauthorized access to sensitive data and applications, even in multi-tenant or public cloud environments. By ensuring that data remains encrypted during processing, Intel TDX reduces the risk of exposure to the infrastructure owner or other users on the same server.

Arqit's NetworkSecure Adaptor software agent is able to run within Intel TDX alongside a VPN client. Therefore data that enters or leaves the enclave is quantum-safe encrypted and is never visible to the cloud host. The solution can be deployed between Intel TDX or confidential VMs, or from a TEE in a public cloud environment to an on-prem environment, giving customers complete quantum-safe protection and privacy over their data even when it's outside their own infrastructure.

Intel TDX is designed for rapid "lift and shift" deployment of confidential virtual machines (VMs) in a highly secure environment. Arqit's integration of these technologies with its NetworkSecure Adaptor was seamless and the collaboration between Intel and Arqit quickly delivered a proof of concept. Intel engineers simply provided the Arqit team with details about Intel TDX and provided access to a software development environment.

> *"Our collaboration with Intel delivers a powerful, enhanced model for securing data in the cloud. By combining Intel TDX with Arqit's quantum-safe encryption, we're giving customers full control of their security, removing infrastructure providers from the trust equation entirely."*
>
> **– Andy Leaver, Chief Executive Officer, Arqit Quantum Inc.**

Arqit's PQC solution can be used in a variety of use cases, including the following:

- **Secure AI.** Enterprises developing AI solutions can ensure end-to-end protection by securing sensitive data during training and safeguarding proprietary models during use—preserving trust, maintaining compliance, and protecting competitive advantage.
- **Network as a service (NaaS) quantum-safe connectivity.** Global network service providers are exploring Arqit's PQC solution to deploy premium quantum-safe NaaS.[4]
- **Data Sovereignty.** Governments pursuing digital sovereignty can use Arqit's PQC solution to protect data in sovereign clouds and to secure communications between government entities.

> *"This solution is a significant step forward for digital sovereignty and confidential computing. It demonstrates how data can be both stronger and simpler. can be secured by design, no matter where it moves or who holds it."*
>
> **– Andy Leaver, Chief Executive Officer, Arqit Quantum Inc.**

A closer look at data sovereignty and Quantum-safe computing

Many regional data regulations require that governments keep their data within national borders and protect it from foreign entities. Intel® TDX helps protect data even when processed on third-party infrastructure, while Arqit's SKA platform helps prevent secure communications from being accessed in the future. Arqit's PQC solution is ideally suited for government workloads hosted in sovereign clouds, sensitive cross-border communications, and classified or sensitive public sector applications hosted in the public cloud.

Results

- Arqit helps deliver true end-to-end confidential compute, preventing any third party, including cloud providers, from accessing a customer's encryption keys, workloads, or data, even when distributed across multiple hosts.[5]
- Intel TDX encrypts memory in use and isolates workloads from cloud or on-prem infrastructure owners—including the hypervisor and system administrators—to protect sensitive data during processing.
- Intel and Arqit created a working proof of concept in under two weeks, benefitting from the "lift and shift" design of Intel TDX, supporting the rapid migration of VMs.

Solution Ingredients

- Intel® Trust Domain Extensions
- Intel® Xeon® 6 processors
- Arqit NetworkSecure Adaptor
- Data Sovereignty with Confidential Computing and Networking

Strengthen your cybersecurity today. Contact your Intel or Arqit representative to learn more.

intel. x ARQIT

[1] Sources: https://www.rsa.com/resources/blog/zero-trust/setting-the-record-straight-on-quantum-computing-and-rsa-encryption and https://www.btq.com/blog/how-far-away-is-the-quantum-threat

[2] For more information, read the solution brief.

[3] This is a different approach from asymmetric keys, also referred to as public/private keys.

[4] For more information, read the case study.

[5] "The security proofs for the design aspects of the key-establishment protocols used to enable symmetric key agreement over classical IP network infrastructures within Arqit SKA-Platform were independently assured in 2022." - Statement from the Surrey Centre for Cyber Security, at the University of Surrey in the UK.

Performance varies by use, configuration, and other factors. Learn more at www.Intel.com/PerformanceIndex.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details.
No product or component can be absolutely secure.
For workloads and configurations visit www.Intel.com/PerformanceIndex. Results may vary.
Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy. Your costs and results may vary.
Intel technologies may require enabled hardware, software or service activation.

0825/AC/CAT/PDF 366510-001EN