QUANTUM ORIGIN
HSM Solution Brief

\((\text{origin})^{cQ}\)
The secrecy of cryptographic keys is the foundation of all cryptographic security processes. Care must be taken to maintain the confidentiality of keys from bad actors within high-risk environments – even from insiders within the same organization, so that they are only available for authorized activities. A common way to secure these keys is to deploy them within hardware security modules (HSMs), which can be thought of as a cryptographic library wrapped in a physical appliance. This appliance is resistant to attempts to tamper with it and will respond to these attempts by clearing all sensitive data once detected.

These HSMs include a random number generator (RNG) that generates their own cryptographic keys using a pseudo-random process with input from external sources. However, by utilizing Cambridge Quantum’s new Quantum Origin cloud platform the HSM can utilize the best source of randomness, a provably random quantum source, strengthen keys, and add another layer of security.
Introduction

Organizations will typically use deterministic or ‘pseudo random’ generation methods (PRNG) to create randomness, such as those used to generate keys for public-key cryptography. As the name implies, these deterministic methods are not truly random - but generated from an algorithm with input extracted from an initial seed. An algorithm by itself cannot produce truly random values, but is a process that only appears to be random. If an algorithm is initialized with duplicate values, this algorithm will always provide the exact same result.

Using a hardware random number generator (HRNG) or a true random number generator (TRNG), is not a viable substitute. These devices, while an improvement over a PRNG, and used within higher security environments, still use deterministic physical processes to generate a seed for a PRNG that can in principle be modelled. This introduces a predictable bias that could be determined by an organization with enough classical or quantum computational resources.

And similarly a traditional QRNG is not the solution. While these devices use non-deterministic quantum processes to generate their randomness, it can introduce classical noise which cannot be separated from the random output. This requires organizations to trust that the QRNG has been perfectly built and cannot be weakened over its operational lifetime.

The Benefit of Quantum Origin

Quantum Origin on the other hand, leverages the advantages that quantum computing brings to generate near-perfect private random data and keys from a provably random source. Quantum mechanics states that a quantum bit (or qubit) prepared in a suitable way will be read with an exact 50% chance of being a ‘0’ or a ‘1’ and forms the basis of Quantum Origin’s random number generation.

Quantum Origin has undergone evaluation in the quality of randomness generated using industry-recognized statistical tests including Diehard, ENT, TestU01, and the NIST Statistical Test Suite. But Quantum Origin goes a step further, in addition to these tests, by using quantum entanglement to certify the level of randomness generated from a quantum source. Reading the information from the quantum computer will introduce noise with the output, but as opposed to a traditional RNG, our entanglement-based verification is used to compute a bound on the generated randomness. Using a randomness extractor, this randomness is then refined to provide a near-perfect output. What remains is a near-perfect quantum seed for generating the best possible cryptographic keys.
How Quantum Origin Strengthens HSMs

An HSM is responsible for maintaining the confidentiality and integrity of cleartext cryptographic keys, performing encryption or signing operations without exposing keys externally, enforcing security policies including dual custody, and controlling what users and applications are able to use the keys. Since the HSM is a tamper resistant/responsive device, any attempt to breach the HSM’s physical protections will result in immediate erasure of all cryptographic keys before they can be exposed.

Historically HSMs were deployed within heavily regulated financial organizations or within government agencies. However, due to the rise of malicious actors including nation state supported attackers, cybersecurity best practices have tightened and organizations around the world use HSMs to secure their operations such as their corporate certificate authority private keys, authentication channels including HTTPS/TLS and VPN deployments, and databases.

However, if the keys used within the HSM are not random and can be predicted and modelled, or compromised via quantum computers when using classical algorithms, armed with Shor’s Algorithm, the secrecy of all data encrypted by the HSM can be exposed. Quantum Origin generates the best possible cryptographic keys from verifiable randomness from a quantum process. These keys can be made available to all existing application in line with existing application workflows and APIs such as PKCS#11 without modifying existing applications.

SHOR’S ALGORITHM

In 1994, American mathematician Peter Shor devised a quantum algorithm capable of calculating prime factors of large numbers. Security experts immediately recognized the threat Shor’s Algorithm posed to public-key cryptography such as RSA, which relies on the difficulty in efficiently factoring large numbers as the basis of its security. It is trivial for classical computers to calculate the product of two numbers, but extremely difficult to efficiently reverse this operation and find the prime factors that could produce the product of a similar calculation.

If run on a quantum computer with enough qubits, Shor’s Algorithm could render the prime factorization challenge insignificant, reducing an operation that would take hundreds or thousands of years on today’s classical computers to minutes on a sufficient quantum computer. However, it’s important to understand that it’s not just the threat to the public-key algorithm, but the ways the cryptographic keys themselves are generated must also be strengthened.
Get started with Origin today by using Quantum Origin

The Quantum Origin platform is designed to easily integrate into existing cryptographic systems, including HSMs and key management systems. Quantum Origin is a secure cloud-hosted platform, accessible over an encrypted REST API, and delivering key material wherever there is a routable TCP/IP connection. Enterprise-wide applications that rely on cryptographic keys can consume keys no matter their location, including the primary datacentre, branch office, or other geographically separate location.

Using Quantum Origin’s near-perfect keys, organizations can increase the security of existing processes. Quantum Origin generates keys from verifiable quantum randomness instead of deterministic sources such as TRNG/HRNGs or traditional QRNG platforms which rely on assumptions and complete trust being placed on the source. Rather, Quantum Origin is based on a device independent approach using randomness verification to ensure a near-perfect result.

And as the threat landscape changes, Quantum Origin will be there to support it. The “Harvest Now, Decrypt Later” threat, where bad actors stockpile encrypted messages with the intent to decrypt them later using a quantum computer, can be mitigated by deploying post-quantum algorithms. Quantum Origin supports all current NIST candidate algorithms and can be used by applications transitioning away from classical algorithms or for use with hybrid algorithms for crypto agility.

CONTACT US

Please contact our experts by email quantumorigin@cambridgequantum.com
We set out our vision to positively transform the world using the power of quantum computing back in 2014. Today, we are recognised as one of the foremost quantum computing companies, delivering science-led, enterprise-driven solutions to tackle hard problems across a diverse range of industries.

Cambridge Quantum designs, engineers and deploys algorithms and enterprise application libraries, translating cutting-edge research into industry-leading technologies through a product-centric focus. TKET, our hardware-agnostic software development platform, and other technologies are currently utilised by an expansive and ever-growing user base.

The team at Cambridge Quantum has been developing the theoretical foundations of quantum computing for over 25 years, forging ahead with breakthroughs in the fields of quantum chemistry, quantum artificial intelligence, quantum cybersecurity and quantum algorithms.

At present, we have the deepest roster of researchers, developers and engineers working to democratise quantum computation and realise the benefits for the greatest possible number of people.

FOR MORE INFORMATION

LinkedIn
CambridgeQuantum.com