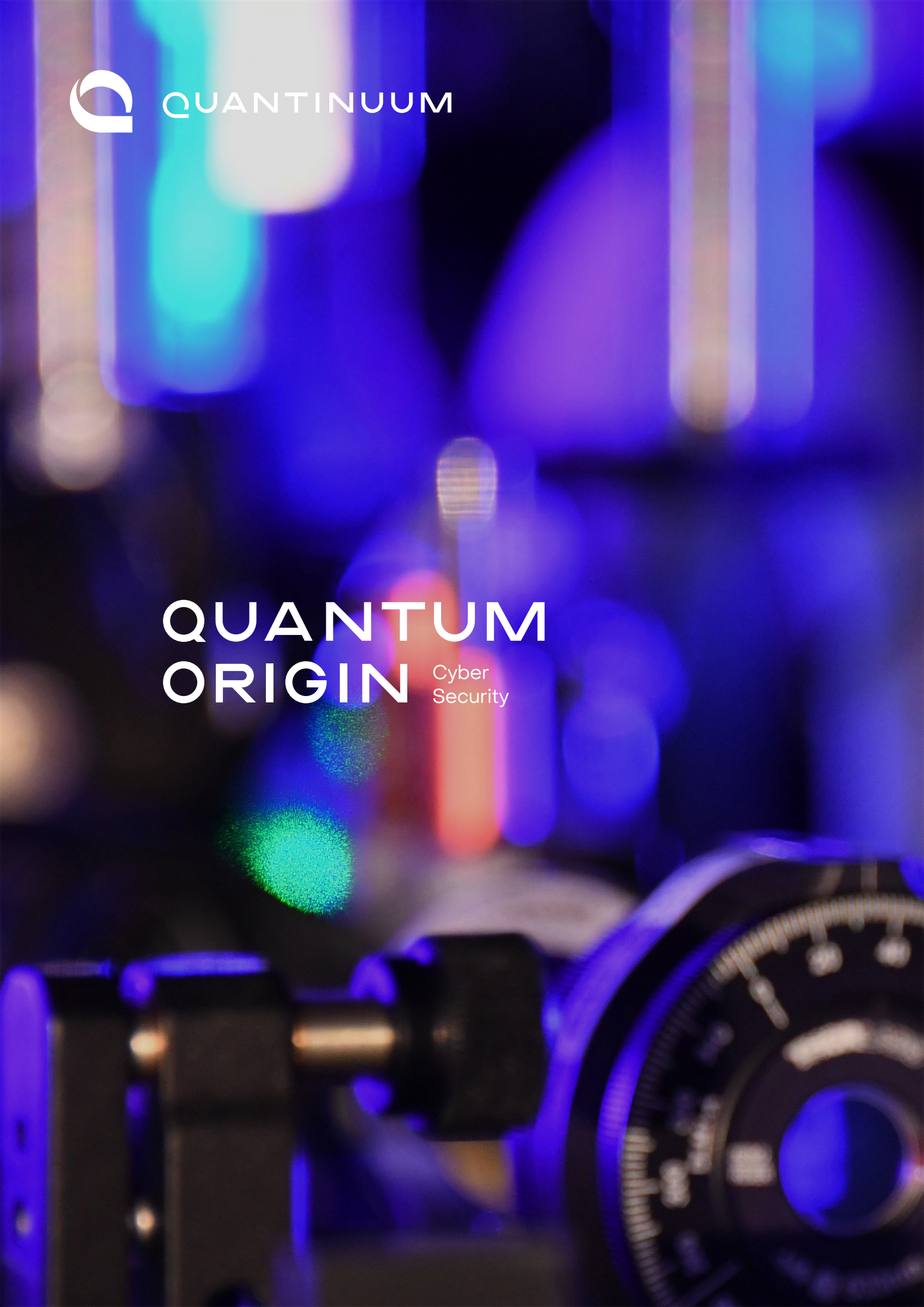

QUANTINUUM
QUANTUM
ORIGIN
Cyber
Security

SECURE TODAY, SECURE TOMORROW

QUANTUM ORIGIN AT A GLANCE

Quantum Origin is the world's first cryptographic key generation platform based on verifiable quantum randomness. It is designed to secure the world's data from both current and advancing threats to today's encryption.

Quantum Origin is a cloud-hosted platform that uses the unpredictable nature of quantum mechanics to generate superior cryptographic keys. Each key is seeded with verifiable quantum randomness drawn from quantum computers. The platform supports traditional cryptographic algorithms, such as RSA or AES, as well as post-quantum algorithms currently being standardised by the National Institute of Standards and Technology (NIST).

THREATS TO MODERN ENCRYPTION

Cyber security relies on multiple layers of defence to defeat attackers. The foundation of these layers is the cryptographic keys that encrypt sensitive information.

Strong cryptographic keys must be completely unguessable to an attacker. This means the creation of high quality randomness is at the heart of key generation. Today, companies use cryptographic keys that are not truly random. In one recent study, researchers uncovered nearly half a million certificates in active use that are so fundamentally weak, they can easily be broken by today's computers.[1]

The problem is caused by existing RNGs, which cannot generate verifiable randomness. The numbers they generate are not fundamentally unpredictable, and so the resulting cryptographic keys are not suitably strong. As a result, such RNGs have been the point of failure in a growing number of cyber attacks.

[1] Kilgallin et al *Factoring RSA Keys in the IoT Era*, First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, 2021

HACK NOW, DECRYPT LATER

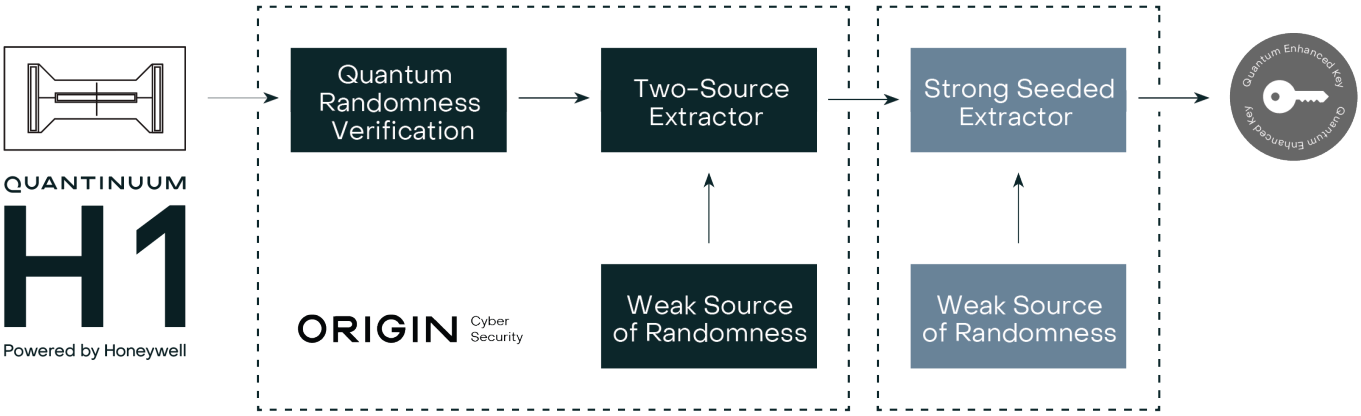
In the future, quantum computers will be able to break many of the encryption systems we rely upon today. Because a powerful quantum computer doesn't exist yet, many companies mistakenly believe the data they exchange today is completely safe, provided it's encrypted.

A "hack now, decrypt later" attack involves intercepting and recording encrypted data as it passes through public networks. When a powerful quantum computer arrives, which may only be 5–10 years away, according to Google's CEO[2], the attacker can retrospectively break the encryption used to protect the data.

To defend against this attack, companies can move towards using quantum-safe encryption algorithms, such as those being standardised by the NIST post-quantum cryptography process[3]. Quantum Origin has been designed to support those algorithms from launch, helping customers to transition towards solutions that are resistant to quantum attack.

[2] Hannah Boland, *Quantum computing could end encryption within five years, says Google Boss,* The Telegraph, 2021

[3] NIST, *https://csrc.nist.gov/projects/post-quantum-cryptography,* 2020



QUANTUM ORIGIN, A UNIQUE APPROACH

Every key generated by Quantum Origin is seeded[4] from verifiable quantum randomness. The word "verifiable" is crucial because it's the reason Quantum Origin delivers superior security guarantees compared with other solutions in the market.

Quantum Origin's random number generation leverages nature's intrinsic randomness. According to the laws of quantum mechanics, qubits can be prepared and measured in such a way as to produce an outcome of "0" or "1" with exactly 50% probability. Unlike other solutions on the market, Quantum Origin is able to isolate this randomness from deterministic classical noise without relying on strict modelling of the device. The result is mathematically-proven, near-perfect randomness, which is used to generate superior cryptographic keys.

Other solutions may claim to generate exceptional randomness, however those claims are rooted in unfair assumptions about how those devices are constructed and how they operate. Because the Quantum Origin approach is based on a device independent protocol, we can verify our randomness is as good as we claim it is.

The Quantum Origin platform uses a quantum computer to generate quantum-enhanced randomness. Using entangled qubits and the Bell Test, we verify the level of randomness present and further refine the output using multiple randomness extraction operations. This ensures a near-perfect set of randomness is available for cryptographic key generation.

[4] The term "seeded by" means the key generation process is kick-started by our randomness. Anyone who could predict this seed would be able to guess the key, hence the unpredictability of this seed is critical.

EASY INTEGRATION, SECURING SYSTEMS TODAY AND TOMORROW

As Quantum Origin is a cloud-hosted platform it integrates easily with existing cryptographic systems such as virtual private networks, hardware security modules, public key infrastructure, or any cryptographic system where keys are consumed.

Quantum Origin customers request new cryptographic keys by calling a web API. The response is an encrypted key, which can be securely imported into existing cyber security systems.

Quantum Origin generates standard cryptographic keys, such as those used in AES or RSA, as well as those used in post-quantum algorithms. This means the platform can help increase the security of today's systems, while being future-proofed for the pending transition to post-quantum algorithms.

By using Quantum Origin, companies can help reduce the risk of data breaches caused by weak or inferior keys across a wide range of use cases, see on the right side.


Hybrid Encryption


Data Watermarking


Data at Rest


Identity & Access Management


Blockchain


Data in Transit


Secure Messaging


Internet of Things


Raw Randomness

THE RESEARCH BEHIND QUANTUM ORIGIN

The Quantum Origin team is supported by a research group with a long history of academic success. The researchers conduct ongoing fundamental research into novel cyber security applications for quantum technology. Alongside this, time is devoted to solving the practical challenge of building real world quantum cyber security technology.

Many of the researchers have worked directly on topics related to building Quantum Origin during their years in academia. This has resulted in combined expertise across the domains of cyber security, classical and quantum cryptography, information security, pure mathematics, experimental quantum optics and quantum information.

PATENTS

The technology underpinning Quantum Origin is patented. Further implementation-specific patents are pending.

SECURE TODAY, SECURE TOMORROW

Quantinuum's cyber security keys ensure verifiable quantum randomness and can help defend against threats today and into the future.

CONTACT US

Please contact our experts by email
quantumorigin@cambridgequantum.com

Visit quantinuum.com