Cambridge Quantum

PRESS RELEASE

Cambridge, United Kingdom
Tuesday, December 7 2021

CAMBRIDGE QUANTUM LAUNCHES QUANTUM ORIGIN

(origin)^{CQ}

Quantum Origin — A quantum-enhanced cryptographic key generation platform to protect data from advancing threats

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, December 7 2021

- Quantum Origin is the world's first commercial product built using quantum computers that delivers an outcome that classical computers could not achieve
- Quantum Origin is the first platform to derive cryptographic keys using the output of a quantum computer to ensure data is protected at foundational level against evolving attacks
- It provides immediate protection to enterprises and governments from current security issues, arising from the use of weaker random number generators (RNGs)
- Quantum Origin also helps protect against 'hack now, decrypt later' attacks, which are already happening and will have future implications
- The quantum-enhanced cryptographic keys generated by Quantum Origin are based on verifiable quantum randomness and can be integrated into existing systems. The protocol relies on "entanglement", a unique feature of quantum mechanics.
- Quantum Origin supports traditional algorithms, such as RSA or AES, as well as post-quantum cryptography algorithms currently being standardised by the National Institute for Standards and Technology (NIST)

Cambridge Quantum (CQ), the global leader in quantum software, and a wholly owned subsidiary of Quantinuum, the world's leading integrated quantum computing company, is pleased to announce that it is launching Quantum Origin – the world's first commercially available cryptographic key generation platform based on verifiable quantum randomness. It is the first commercial product built using a noisy, intermediate-scale quantum (NISQ) computer and has been built to secure the world's data from both current and advancing threats to current encryption.

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, December 7 2021

Randomness is critical to securing current security solutions as well as protecting systems from the future threat of quantum attacks. These attacks will further weaken deterministic methods of random number generation, as well as methods that are not verifiably random and from a quantum source.

Today's systems are protected by encryption standards such as RSA and AES. Their resilience is based on the inability to "break" a long string from a random number generator (RNG). Today's RNGs, however, lack true, verifiable randomness; the numbers being generated aren't as unpredictable as thought, and, as a result, such RNGs have been the point of failure in a growing number of cyber attacks. To add to this, the potential threat of quantum attacks is now raising the stakes further, incentivising criminals to steal encrypted data passing over the internet, with a view to decrypting it later using quantum computers. So-called "hack now, decrypt later" attacks.

Quantum Origin is a cloud-hosted platform that protects against these current and future threats. It uses the unpredictable nature of quantum mechanics to generate cryptographic keys seeded with verifiable quantum randomness from Quantinuum's H-Series quantum computers, Powered by Honeywell. It supports traditional algorithms, such as RSA or AES, as well as post-quantum cryptography algorithms currently being standardised by the National Institute for Standards and Technology (NIST).

"We have been working for a number of years now on a method to efficiently and effectively use the unique features of quantum computers in order to provide our customers with a defence against adversaries and criminals now and in the future once quantum computers are prevalent," said Ilyas Khan, CEO of Quantinuum and Founder of Cambridge Quantum. He added "Quantum Origin gives us the ability to be safe from the most sophisticated and powerful threats today as well as threats from quantum computers in the future."

Duncan Jones, head of cybersecurity at Cambridge Quantum, said: "When we talk about protecting systems using quantum-powered technologies, we're not just talking about protecting them from future threats. From large-scale takedowns of organisations, to nation state hackers and the worrying potential of 'hack now, decrypt later' attacks, the threats are very real today, and very much here to stay. Responsible enterprises need to deploy every defense possible to ensure maximum protection at the encryption level today and tomorrow."

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, December 7 2021

Quantum-enhanced keys on demand

With Quantum Origin, when an organisation requires quantum-enhanced keys to be generated, it can now make a call via an API. Quantum Origin generates the keys before encrypting them with a transport key and securely relaying them back to the organisation. To give organisations a high-level of assurance that their encryption keys are as unpredictable as possible, Quantum Origin tests the entire output from the quantum computers, ensuring that each key is seeded from verifiable quantum randomness.

These keys are then simple and easy to integrate within customers' existing systems because they're provided in a format that can be consumed by traditional cybersecurity systems and hardware. This end-to-end approach ensures key generation is on-demand and is capable of scaling with use, all while remaining secure.

Quantum Origin in practice

Quantum Origin keys should be used in any scenario where there is a need for strong cybersecurity. At launch, Cambridge Quantum will offer Quantum Origin to financial services companies and vendors of cybersecurity products before expanding into other high priority sectors, such as telecommunications, energy, manufacturing, defence and government.

The technology has already been used in a series of projects with launch partners. Axiom Space used Quantum Origin to conduct a test of post-quantum encrypted communication between the ISS and Earth – sending the message "Hello Quantum World" back to earth encrypted with post-quantum keys seeded from verifiable quantum randomness. Fujitsu integrated Quantum Origin into its software-defined wide area network (SDWAN) using quantum-enhanced keys alongside traditional algorithms.

More information is available on

— The partners use cases of Quantum Origin
— The Cambridge Quantum/Dimensional Research global leaders survey
— Quantum Origin product specifications

ABOUT CAMBRIDGE QUANTUM

Founded in 2014, Cambridge Quantum is a global leader in quantum software and quantum algorithms, enabling clients to achieve the most out of rapidly evolving quantum computing hardware. It is part of the newly formed Quantinuum, the world's largest, integrated quantum computing company. Cambridge Quantum has offices in Europe, USA, and Japan.

FOR MORE INFORMATION

CambridgeQuantum.com
LinkedIn
Access the source code for lambeq, TKET, Python bindings and utilities on GitHub