Cambridge Quantum

BENEFIT FROM ENCRYPTION

Backed by quantum, today.

(ironbridge)^{CQ}

Version 1.0, November 2021

The data disaster

Every year, more than 7.9 billion data records are stolen or exposed by hackers. For public companies, the cost of a data breach has now reached an eye-watering $116M. Nation-states are becoming routinely involved in sophisticated attacks, and companies have found themselves under attack, simply as a route through to another valuable target.

Regulations are increasing

Regulators and privacy bodies now impose heavy fines on companies that lose personal data. Regulations like GDPR are starting to bite, and in the last few years, we have seen multiple $100M fines issued around the world.

Companies can no longer afford to be the subject of a mega-breach. Between the cost of the fines and the technical remediation, breaches are now existential threats.

Existing keys are weak

Cybersecurity relies on layers of defence to defeat attackers. The foundations of your security are the cryptographic keys that encrypt your most sensitive information.

Randomness is at the heart of key generation, as keys must be completely unguessable to an attacker. Today, companies use randomness generation that is not truly random. Researchers have uncovered nearly half a million certificates in active use that are completely broken due to poor randomness.

The quantum threat

In 5 to 10 years, quantum computers will break the encryption systems we use today, according to Google CEO Sundar Pichai. Unfortunately, these attacks work retrospectively, as data sent today can be decrypted in the future.

We cannot rely on today's methods of key generation any longer. We need to be designing quantum-proof cybersecurity approaches such that we're prepared for **the future.**

JEREMY FLEMING
Head of Government Communications Headquarters, April 2021

Technology and science are at the forefront of quantum computing, and these unprecedented capabilities must be leveraged to create a safe and resilient cyber nation.

Dr. Krysta Svore of Microsoft Research states that the RSA-2048 problem would take 1 billion years to solve with a classical computer, a quantum computer can do it in 100 seconds.

Nature's perfect randomness

Cambridge Quantum's cybersecurity keys ensure verifiable quantum randomness and can help defend against threats today and into the future.

The answer is quantum

Cambridge Quantum has addressed these threats head-on with our IronBridge quantum key generation platform. We use modern-day quantum computers, from any vendor, to produce strong cryptographic keys.

IronBridge harnesses the power of quantum mechanics to generate verifiable random data, which no one can predict.

Zero trust approach

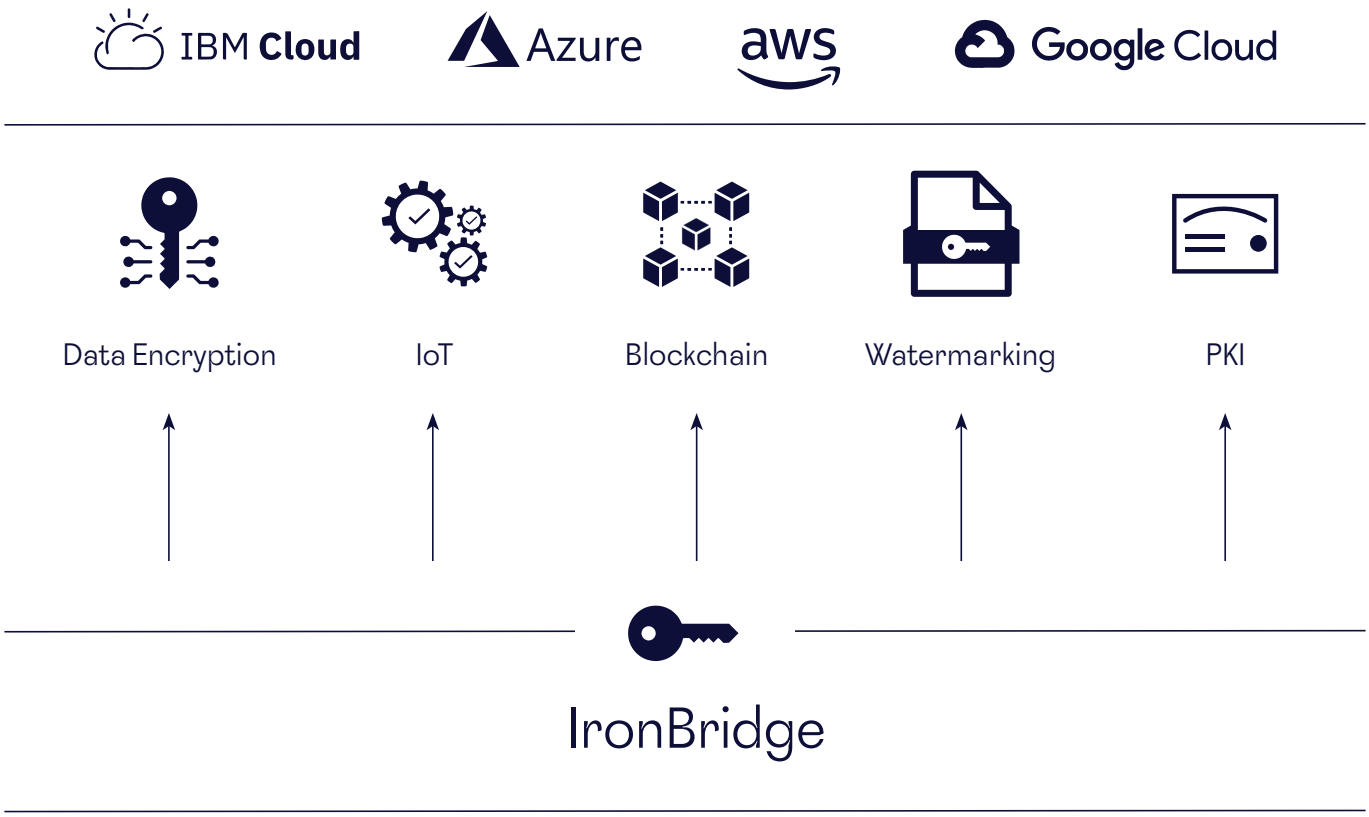
IronBridge is the only key generation platform that generates cryptographic keys seeded from verifiable quantum randomness. Moreover, we continually verify the randomness we generate from quantum computers.

Secure today, secure tomorrow

IronBridge can withstand today's threats, as well as tomorrow's, even when attackers have access to powerful quantum computers. IronBridge keys remain completely unpredictable and offer a secure solution, although we publish the details of how our algorithms work.

That's true security. We don't rely on secret methods or clever tricks, just quantum randomness.

(ironbridge)^CQ



(ironbridge)^{CQ}

Easy integration

IronBridge is a cloud-hosted platform that integrates easily with existing cryptographic systems. In most cases, you won't need to adjust your application to work with our quantum-derived keys.

IronBridge can generate standard cryptographic keys, such as those used in AES or RSA, as well as those utilised in post-quantum algorithms. This means our platform can integrate today without any difficulty. We can also support your transition to quantum-proof algorithms over time.

Use cases

IronBridge keys can be integrated into any cryptographic use case with little or no modification to the existing application.

BLOCKCHAIN

Secure transactions between users with quantum-proof history.

IDENTITY AND ACCESS

Prevent impersonation and unauthorised access.

DATA WATERMARKING

Seal data with quantum-proof signatures.

IoT

Bring devices to life with strong identity keys.

WHY NOT GET STARTED WITH IRONBRIDGE TODAY?

CONTACT US

Please contact our team at
Email: support@cambridgequantum.com

Cambridge Quantum

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