Cambridge Quantum

# An Introduction to Quantum Cybersecurity

Published by Cambridge Quantum

Version 1.0, July 2021

Cambridge Quantum

# LEARN HOW QUANTUM COMPUTING WILL AFFECT THE SECURITY OF YOUR BUSINESS

Quantum computing will completely change the face of cybersecurity.

On the one hand, quantum computers will disrupt many of the systems we rely upon today, forcing a wholesale move to new solutions and algorithms. While on the other hand, quantum technology will allow us to achieve unprecedented levels of security in many aspects of cryptography.

In this whitepaper, we outline the challenges and opportunities that quantum computing brings to cybersecurity and the digital industry as a whole. In particular, we will explore some of the ways that quantum technology can strengthen cybersecurity solutions today.

# THE RISING THREAT OF NATION STATES

In recent years there's been an important shift in the way cyber attacks are being perpetrated. Gone are the "script kiddie" days, where hackers were typically youngsters armed with a limited toolset of exploits. Instead, we now see regular headlines about state-sponsored cybersecurity incidents, motivated by geopolitical ambitions. Studies show there's been a 100% increase in significant nation-state incidents between 2017 and 2020, with business and enterprise representing 35% of the victims in analyzed attacks.[1]

As more of our lives move online, cyber attacks are now a viable way to influence election results, disrupt major supply chains, steal intellectual property and generally disrupt a target nation. The victims of attacks are not always the intended targets – collateral damage is a common issue, especially when viruses are used to spread exploits indiscriminately.

"Gone are the script kiddie days."

Even nation states are not safe, as demonstrated in December 2020 when the United States government was attacked by a hacker group affiliated with Russian intelligence agencies.[2] A follow-on investigation in early 2020 of the now infamous SolarWinds hack revealed the true casualty figures: 18,000 government and private networks had been compromised and 250 U.S. federal agencies and businesses had been adversely affected.[3]

Although the SolarWinds hack was widely publicized, it is just the latest in a string of cyber attacks connected to nation states. Between January 2019 and April 2020, a staggering 38% of cyber attacks were associated with nation states.[4]

1 McGuire, Michael. *Nation States, Cyberconflict, and the Web of Profit.* HP Wolf Security. 2021.

2 Sanger, David, et al. *As Understanding of Russian Hacking Grows, So Does Alarm*. May 28, 2021.

3 Ibid.

4 ENISA *Threat Landscape 2020 –Cyber Espionage.* October 20, 2020.

In the past 24 months alone we've seen several notable attacks on businesses, NGOs and governments:

— Airbus, a European multinational aerospace firm, and its suppliers were targeted by state-sponsored hackers who stole the personal information of employees in their search for trade secrets.[5]

— Publicly traded German companies such as BASF, Henkel, and Siemens were victims of cyberattacks blamed on a Chinese-backed organization.[6]

— Ahead of EU elections, numerous European agencies were targeted by Kremlin-sponsored foreign hackers.[7]

South Korea's national defense ministry's computers were breached and data pertaining to national arms procurement was stolen.[8]

— Amnesty International Hong Kong, an NGO focused on human rights, was attacked by sophisticated state-sponsored cyber hackers.[9]

One consequence of this increase in nation-state-sponsored attacks is an increase in threat sophistication. Companies can no longer assume they won't be the target of a complex, persistent attack from a well-funded adversary.

CEOs, CISOs and CTOs must prepare and arm their organisations with a broad range of security measures, ensuring that every layer in their defence is as strong as it can possibly be. Weaknesses will be found and exploited, in this new age of sponsored cyber terror.

5 **France24.** *Airbus hit by series of cyber attacks on suppliers.* September 26, 2019.

6 **Reuters Staff.** *BASF, Siemens, Henkel, Roche target of cyber attacks.* Reuters. July 24, 2019.

7 **Palmer, Danny.** *Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections.* ZDNet. March 21, 2019.

8 **Cimpanu, Catalin.** *Hackers breach and steal data from South Korea's Defense Ministry.* ZDNet. January 16, 2019.

9 **Amnesty International** *State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack.* April 25, 2019.

# THE GROWING COST OF DATA BREACHES

Not only are attacks increasing in sophistication, but also the size and impact of data breaches are growing at a striking rate. The costs of a breach are not limited to technical remediation – companies must also deal with reputational damage, stock price dips, as well as increasingly serious fines.

Over 36 billion data records were stolen or exposed in the first half of 2020 alone, causing irreparable economic damage to individuals, companies, and governments alike.[10] According to an audit analytics report on cyber-breaches, these data breaches cost an average of $116 million for publicly traded companies.[11] Even smaller US companies face an average bill of $8.6 million.[12]

The surge in attacks has encouraged policymakers to rethink legislative requirements and impose substantial fines in an attempt to prioritise 'cyber alertness' amongst C-Suite. For instance, following the ransomware attack on Colonial Pipeline in May 2021, which disrupted oil supplies in the U.S. for 5 days, the EU's regulators drafted laws to augment cybersecurity measures in the energy sector and other critical infrastructure.[13][14] Similarly, the European Union installed a new joint cyber unit, a close collaboration with the European Union Agency for Cybersecurity (ENISA), to implement centralized response to large-scale cybersecurity crises and incidents.[15]

Following the introduction of the EU's General Data Protection Regulation in May 2018, fines have exceeded over $340 million cumulatively as of June 2021, with the broader media, telecoms, and broadcom industry accounting for approximately $160 million.[16] According to a popular GDPR fines database, the quantity of corporate fines has increased by a considerable 400% since January 2020.[17]

In recent history, companies that have paid large settlement sums include Equifax (2017; $575 million), British Airways (2018; $230 million), Uber (2016; $148 million), and Marriott International (2018; $124 million).[18] These occurrences are potent wakeup calls for management teams. To avoid the financial and operational distress following a crisis, organizations need to evaluate their existing systems for cyber-readiness and actively search for effective solutions.

10 RiskBased Security. *2020 Q3 Report - Data Breach QuickView*. 2020.

11 Nicodemus, Aaron. *Report: Average data breach costs public companies $116 million*. Compliance Week. June 9, 2020.

12 IBM Security. *Cost of a Data Breach Report 2020*. July 2020.

13 The Economist. *To stop the ransomware pandemic, start with the basics*. June 19, 2021.

14 Stupp, Catherine. *European Energy Sector Prepares for New Cybersecurity Rules*. The Wall Street Journal. June 8, 2021.

15 ENISA *EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit*. June 23, 2021.

16 Burgess, Matt. *What is GDPR? The summary guide to GDPR compliance in the UK*. WIRED. March 24, 2020.

17 CMS. *GDPR Enforcement Tracker: Fines Statistics*. Accessed June 25, 2021.

18 Johnson, Joseph. *Biggest data breach fines and settlements worldwide 2020*. Statista. January 25, 2021.

# THE QUANTUM THREAT

So far, we've been discussing the threat posed by today's state-sponsored cybercriminals. However, the situation will get worse in the near future when hackers have access to powerful quantum computers that can break our cybersecurity defences.

Today's public encryption schemes are heavily dependent on complex mathematical calculations, such as factoring large numbers. The ubiquitous RSA algorithm is a perfect example of such a scheme. However, as quantum computers and algorithms become more computationally advanced, these encryption standards will be broken. In 1994, Peter Shor, an applied mathematics professor at MIT, developed a quantum algorithm that would be able to crack RSA, and other algorithms, if run on a sufficiently powerful quantum computer.

Michele Mosca, co-founder of the Institute for Quantum Computing at the University of Waterloo, has stated there's a 1–in–7 chance that RSA–2048 will be broken by 2026 and 1–in–2 chance by 2031. Sundar Pichai, CEO of Google and Alphabet, has publicly claimed that in the next 5 – 10 years, existing public encryption algorithms will be broken by quantum computers, signalling to the wider business community to stay vigilant of the approaching threat.

> "There's a 1-in-7 chance that RSA-2048 will be broken by 2026."

Not only will quantum computers break algorithms, but they will also break cryptographic keys. Quantum computers will be able to simulate and model very complex systems, including the methods currently used to generate cryptographic keys. Using a quantum computer, attackers may be able to predict some or all of the bits used to construct a cryptographic key. Once this is known, the attacker can decrypt data at will.

Given the above facts, a natural question would be: when will quantum computers be powerful enough to break these algorithms and keys? While the answer to this is unknown, the more important question to ask is:

## When should we act?[19]

Attackers are assumed to have begun recording encrypted transmissions sent today, knowing they can be decrypted in the future. This means sensitive data sent today may be exposed to the world in as little as 5-10 years' time. The fear of this data exposure is rightly driving many companies to explore the early adoption of quantum-proof algorithms.

Organizations such as the National Institute of Standards and Technology (NIST), have crafted roadmaps outlining the implementation of quantum-safe algorithms to combat cybersecurity threats. NIST began the search process for a new set of quantum-safe algorithms in early 2016 and expects to conclude its evaluation by 2023, with standards issued by 2024. This implies that time is of the essence for organizations, who must act quickly to become familiar with these new algorithms.

19 Comandar, Lucian et al. *Ensuring Online Security in a Quantum Future.* Boston Consulting Group. March 30, 2021.

# KEYS: THE LAST LINE OF DEFENCE

The core of any security infrastructure is the cryptographic keys that encrypt sensitive data. These keys are all that stand between the hackers and our most valuable secrets, whether that is customer data, medical data, financial records or intellectual property, to name a few examples.

Given the threats we've outlined above, the two questions companies need to ask about their keys are:

— Would they withstand attack from a nation-state?
— Are they quantum-proof and ready for the near future?

A recent study from KeyFactor showed that 1 in 172 certificates are so fundamentally weak, they can easily be broken by today's computers.[20] This may sound like a positive statistic for cybersecurity until you consider how many certificates the average company uses in this digital age. (Hint: it's measured in the tens of thousands).

These sorts of weaknesses arise because traditional approaches to key generation can fail silently without warning. Cryptographic keys are generated from random data, which must be perfectly unpredictable in order to be truly secure. Unfortunately, it is impossible to create perfectly random data using solutions in the market today.[†]

To keep data safe from advanced attacks, we need keys that are:

— Completely unpredictable and perfectly random
— Certified as completely random – we cannot rely on assumptions
— Generated using methods that a quantum computer cannot simulate.

Fortunately, such an approach now exists, and it ironically uses quantum computing to solve the problem.

20 JD Kilgallin. *Securing RSA Keys & Certificates for IoT Devices*, accessed June 2021.

† With the exception of the Ironbridge platform, outline in later sections.

# A NEW QUANTUM APPROACH

To generate a perfect, unhackable cryptographic key, you need perfect randomness. Until recently, this has been impossible to generate in the real world.

Commonly-used "true random number generators", which use chaotic physical processes to produce randomness, fall short of achieving perfection. This leaves a crucial weakness in each key that may be exploited by nation-state attackers, as well as quantum-powered attackers in the future.

Even the first generation of so-called "quantum random number generators" (QRNGs) failed to deliver on their promise. Despite measuring quantum-based effects in nature, they were unable to do so in a way that preserves or guarantees the randomness of their outputs. Consequently, some have been shown to fail advanced statistical tests, which highlights how their output isn't really random.[21]

The correct solution to this problem is using a truly non-deterministic method of key generation. This means using an approach that is inherently random and cannot fail. Such approaches are also impossible to simulate accurately, even by a powerful quantum attacker.

By tapping into the heart of quantum mechanics, it is possible to access the true randomness that powers our Universe. Quantum computers provide the tools we need to access this provably perfect source of randomness and perfectly solve the problems listed above. This is the only non-deterministic randomness humans have discovered, and it's only recently become possible to use it thanks to the advances in quantum technology.

For the first time ever, we can finally generate perfectly strong cryptographic keys. Not only that, but it's possible to prove the keys are perfect.

21 *https://kar.kent.ac.uk/81957/11/Quantum_Leap_TOPS_Submission_FINAL.pdf*

# THE IMPORTANCE OF DEVICE INDEPENDENCE

One of the cornerstones of this new quantum approach to randomness is device independence.

Device independence is a characteristic of a security protocol, or algorithm. In a device-independent protocol, no assumptions are made about the physical device that executes the protocol. Instead, the device is treated as a black box, and the protocol simply provides inputs and interrogates the output from the device.

Until now, all approaches to randomness generation have been device-dependent. This means they make assumptions about the construction and operation of the hardware in order to function correctly. First-generation QRNGs, for example, rely upon the perfect construction of angled mirrors and photon detectors. If these are not in fact perfect, the results from the box cannot be fully trusted.

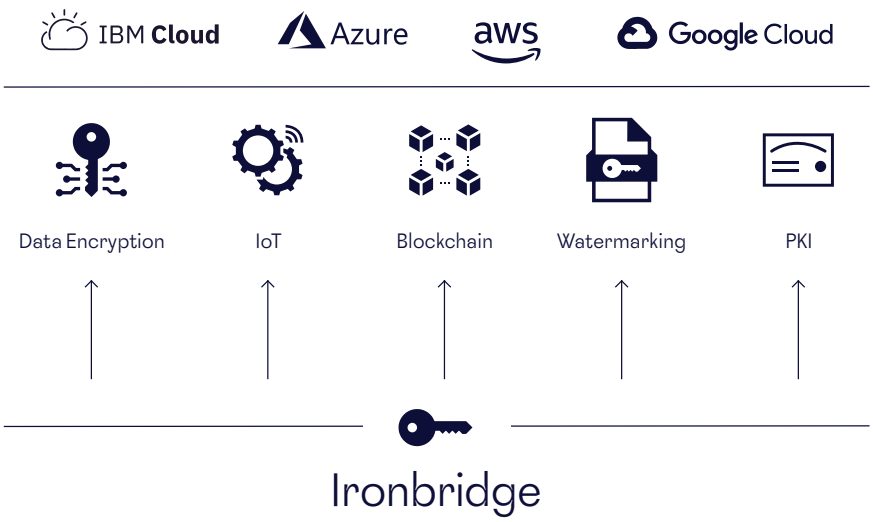
By contrast, the new approach Cambridge Quantum is pioneering is based on a fully device-independent protocol. This means that any failures or imperfections in the quantum devices we use cannot negatively affect the output. As a result, the randomness generated is guaranteed to be perfect.

# IRONBRIDGE: PERFECT QUANTUM-BASED KEYS

22 https://csrc.nist.gov/Projects/post-quantum-cryptography

Ironbridge is a key generation platform that uses quantum computers to generate provably perfect cryptographic keys. This is the only solution available in the market that uses verifiably quantum entropy.

The keys generated by the platform can be classical algorithms (such as RSA or AES) or post-quantum algorithms from the NIST post-quantum cryptography competition.[22] All of the keys are seeded from quantum entropy.




Ironbridge is a software-as-a-service platform, delivering encrypted keys to wherever they are needed within an organisation. Use cases such as data encryption, PKI, blockchain and IoT all benefit from using strong cryptographic keys.

Unlike other solutions in the market, Ironbridge is based on verifiably perfect quantum randomness. This means that the keys generated are always completely unpredictable to present-day threats as well as future quantum attacks.

Integration with existing cybersecurity solutions is easy, thanks to the existing standards for accessing keys and hardware security modules. Ironbridge delivers keys wherever they are needed and existing applications can continue working exactly as they did before.

Cambridge Quantum

# ABOUT CAMBRIDGE QUANTUM COMPUTING

Founded in 2014 and backed by some of the world's leading quantum computing companies, 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. Cambridge Quantum has offices in the United Kingdom, Japan and United States.

## CONTACT

Duncan Jones
Head of Quantum Cybersecurity
duncan.jones@cambridgequantum.com
+44 (0) 7789 424392

## FOR MORE INFORMATION

LinkedIn
GitHub
CambridgeQuantum.com