Cambridge Quantum

An Introduction to Quantum Cybersecurity

(origin)^{CQ}

Version 1.0, December 2021

Quantum 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. 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 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 has 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 has been a 100% increase in significant nation-state incidents between 2017 and 2020, with business and enterprise representing 35% of the victims in analysed 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 US federal agencies and businesses had been adversely affected.[3]

Although the SolarWinds hack was widely publicised, 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 organisation.[6]

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

— South Korea's national defence 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 which have been 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 US 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 centralised 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)[18] and Marriott International (2018; $124 million). These occurrences are potent wakeup calls for management teams. To avoid the financial and operational distress following a crisis, organisations need to evaluate their existing systems for cyber-readiness and actively search for effective solutions.

10 Risk Based Security
2020 Q 3 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
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-key encryption schemes rely on the difficulty of performing certain 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, many of 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.

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

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 a 1-in-2 chance by 2031. Sundar Pichai, CEO of Google and Alphabet, has publicly claimed that in the next 5 to 10 years, existing public-key encryption algorithms will be broken by quantum computers, signalling to the wider business community to stay vigilant of the approaching threat.

Given the above facts, a natural question would be: when will quantum computers be powerful enough to break existing cryptography? 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 post-quantum algorithms.

Organisations such as the National Institute of Standards and Technology (NIST), have crafted roadmaps outlining the implementation of post-quantum algorithms to combat cybersecurity threats. NIST began the search process for a new set of post-quantum 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 organisations, which 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

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

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 are difficult to identify in real world systems before it's too late. This is because cryptographic keys are generated from random data, which must be unpredictable in order to be truly secure. Unfortunately, current solutions to randomness generation cannot provide strong guarantees on the quality of their output. When this is combined with the risk of implementation errors, it's easy to see why weak keys are being found in the wild.

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

- Seeded from highly unpredictable randomness that was generated using a verifiable process
- Generated using methods that even a powerful quantum computer cannot predict

Fortunately, such an approach now exists, and it ironically uses quantum computers to solve the problem. But before we get on to that, we must discuss the important distinction between "deterministic" and "nondeterministic" systems, which has a significant impact on cryptographic keys.

DETERMINISTIC VS NONDETERMINISTIC

Consider what happens when you toss a coin. To the human eye, the result is quite random: we cannot predict whether the coin will land on heads or tails. But is this process really random?

The answer to this is no. The process that unfolds when you toss a coin is fundamentally deterministic in nature. If you know enough information about the system state, such as the height above the ground, the air pressure and the velocity of the toss, you can predict what happens next. Even if you don't know the entire system state, with a powerful enough computer, you could simulate various outcomes and likely have a better than 50% chance of guessing the results.

This same problem applies to any solution that relies on classical physics to generate randomness. The process appears random, and yet it isn't. We are relying on our ignorance of the system state and our inability to perform complex calculations to keep this randomness unpredictable to some degree.

Unfortunately, as quantum computers become more powerful, it will be increasingly easy to simulate large complex systems. This makes it harder to rationalise that this randomness is unpredictable.

Fortunately, quantum mechanics provides the answer to this dilemma. Unlike classical physics, quantum mechanics is non-deterministic in nature. This means even with unbounded computational power, it is not possible to predict how some quantum processes will behave.

This is the reason why cryptography must move towards quantum sources of randomness to ensure that keys remain unpredictable even as computing power increases exponentially. However, it is not as simple as just introducing some quantum processes into the mix. We need to do so in a way that delivers a measurable benefit.

This brings us to the next topic: measuring randomness.

HOW DO YOU MEASURE RANDOMNESS?

Creating strong cryptographic keys requires excellent randomness. But how do we measure randomness?

From an academic perspective, the goal is to quantify the probability someone can distinguish between the randomness you're producing and a theoretically perfect stream of randomness. An excellent source of randomness would have an unbelievably small number for this probability, something like 2^{-128}. To give some sense of how small this probability is, it would be like winning the lottery five times in a row. We can never say a source of randomness is perfect, but this is as close to perfect as we can ever get.

Unfortunately, we cannot calculate this probability using standard statistical test suites, such as DIEHARD[21]. While these tests can detect obvious signs of bias, they cannot measure the quality of the randomness. Passing well-known statistical tests is relatively easy and many software functions and simple approaches to randomness generation can do that. This includes "pseudo random number generators" (PRNGs), which are software functions that expand a random seed into a stream of random-looking data. This data might pass statistical tests, but it is far from the levels of near-perfection we describe above.

To calculate the real probability, we need to shift from examining the output to examining the process that created the output. If we can correctly model and assess the process used, we can quantify the quality of the randomness. However, this is easier said than done.

The challenge with this approach is making a reasonable set of assumptions about the underlying device and how it's built. On paper, it's easy to argue a chaotic electrical circuit will operate in a certain way, or that firing photons at a beam splitter will have unpredictable results. But in the real world, devices don't operate perfectly. Manufacturing processes have errors, so the physical device will differ from the theoretical model. It is also difficult to separate the random effects you are measuring from the surrounding environment noise. Finally, devices change behaviour as they age, or if they are attacked, and this will also affect the output of the device.

Because of this, there is no rigorous way to measure the quality of most random number generators, including "true random number

21 Brown, Robert G
Dieharder: A Random Number Test Suite
2004

22 Hurley-Smith et al
Quantum Leap and Crash: Searching and Finding Bias in Quantum Random Number Generators
Boston Consulting Group
March 30, 2021

generators" and almost every "quantum random number generator" on the market. The security arguments these devices make are too closely linked to how the devices work internally, and they tend to make unreasonable assumptions that cannot be verified during operation. Consequently, some have even been shown to fail advanced statistical tests.

Fortunately, there is a solution to this issue, which is to move towards "device-independent" approaches to randomness generation.

THE IMPORTANCE OF DEVICE INDEPENDENCE

Device independence is a characteristic of a security protocol or algorithm. In a fully device-independent (DI) protocol, only minimal 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.

Because a DI protocol makes minimal assumptions about the device, it doesn't fall victim to the problems highlighted earlier. There are no unreasonable assumptions about manufacturing quality. Device ageing is not a problem because they are measured by challenges and responses. If the device no longer operates correctly, whether due to ageing or attack, the responses will begin to be affected and will be detected by the protocol.

In practice, building fully DI systems is very difficult and such systems only exist on lab-top benches at the moment. A related category of protocols, known as semi-device-independent (SDI) protocols, fall in between DI protocols and the typical "trust everything" approach taken to date. In an SDI protocol, some components of the device are treated as a black box, while the rest are trusted in the traditional sense.

SDI protocols represent a complete spectrum, ranging from the ideal case of only making one assumption about a device, all the way through to trusting everything in the device except one component. The state-of-the-art practical systems are those on the SDI spectrum.

In the next section, we'll explore how Cambridge Quantum has combined non-deterministic quantum randomness with a device-independent mindset to create the strongest cryptographic keys in the world.

QUANTUM ORIGIN — GENERATING THE STRONGEST CRYPTOGRAPHIC KEYS IN THE WORLD

Quantum Origin is the world's first commercial 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).

Every key generated by Quantum Origin is seeded[23] 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. Unlike other available solutions, 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

23 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.

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 cybersecurity applications for quantum technology. Alongside this, time is devoted to solving the practical challenge of building real world quantum cybersecurity 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 cybersecurity, classical and quantum cryptography, information security, pure mathematics, experimental quantum optics and quantum information.

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.

CONTACT

Please contact our experts by email
quantumorigin@cambridgequantum.com

FOR MORE INFORMATION

LinkedIn
CambridgeQuantum.com