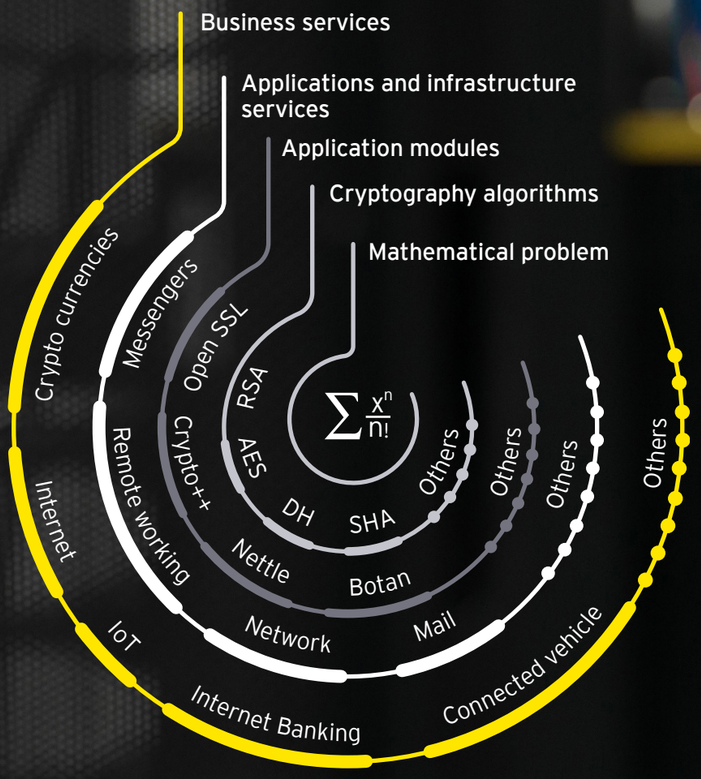
Can quantum technology secure data from theft?

EY
Building a better working world

Data security has never been more critical to businesses success

Confidentiality is a foundation of modern society. It is everyone's right to decide who should have access to their data, from medical records and financial data to even simple messages. In today's digital world, cryptography has proven to be an efficient way to provide confidentiality. It underpins almost every digital device and service we use.



Quantum computers pose a risk to classical cryptography algorithms but also allow us to build better security solutions. The impact of Quantum technology on cryptography is directed at the heart of security. The ramifications of this influence are enormous.

Quantum technology security solutions that might give business a boost

Information is the life-blood of every organisation. Its abuse with malicious intent can cause irreparable damage. Information security must therefore be at the heart of every organisation. The ability to effectively protect information is not only a regulatory requirement, but a competitive advantage.

Security enhancements through quantum technology can give businesses an advantage over adversaries.

1. Quantum Key Distribution

Quantum technology enables a new way of protecting data in transit. Also referred to as data in motion, data in transit is information that flows over communication networks.

Quantum Key Distribution (QKD) is a secure communication method where data is encrypted through principles of quantum mechanics – a branch of physics that deals with behaviour of matter at very small scales. Similar to traditional encryption, it enables two parties to produce a shared secret key known only to them, which can then be used to encrypt and decrypt messages.

Inherent limitations implied by the rules of physics defines the security basis for QKD cryptography protocols. Currently with encryption, security is enabled through the difficulty of solving mathematical problems using classical (non-quantum) computers.

In contrast to conventional key distribution algorithms, QKD offers forward security and is resilient to new attack algorithms and upcoming quantum computers.

2. Quantum Random Number Generators

Quantum technology can strengthen the existing encryption algorithms your organisation already uses today. For example, many cryptographic algorithms use a random number to begin encryption.

The strength of any security system lies in the quality of the "randomness" from the source used for generating cryptographic keys. Quantum Random Number Generators (QRNGs) generate numbers with a high degree of randomness using unique properties of quantum physics that have a high degree of "chaos" or entropy.

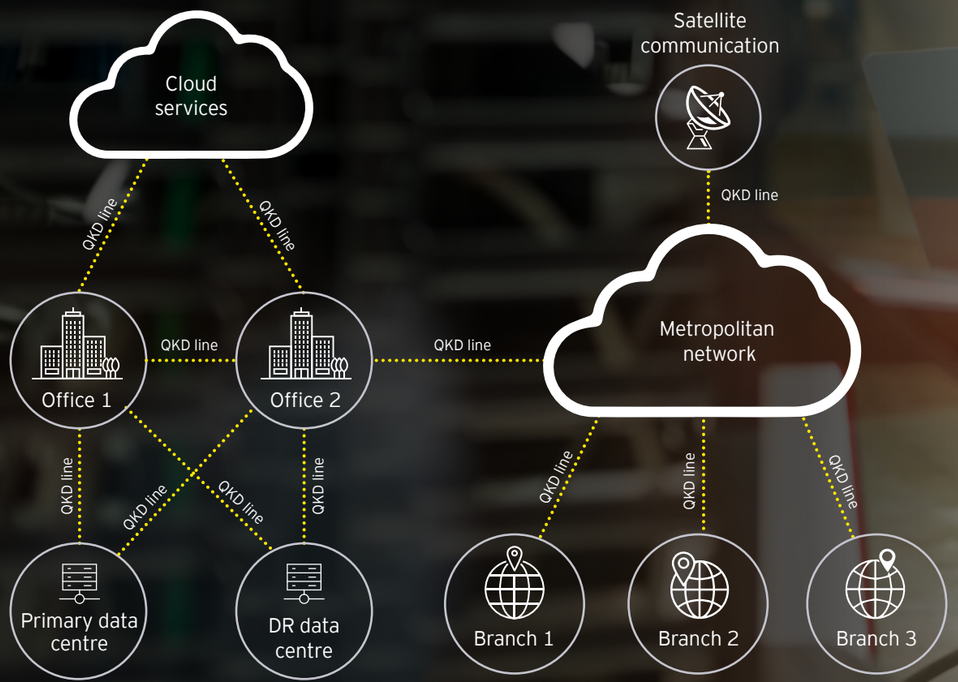
Today, we use systems such as Pseudo Random Number Generators (PRNGs) to generate randomness. These rely on deterministic, and thus predictable, algorithms and may not be secure. QRNGs may potentially be invulnerable to prediction or bias and provide true randomness.

Quantum Key Distribution applications

At the heart of data in transit security is the ability for the recipient and the sender to agree on a secret that no one else knows. Quantum Key Distribution (QKD) uses quantum mechanics to solve this challenge, but technology limitations require quantum technology to be enabled at both ends of the communication line.

QKD systems are best suited to secure:

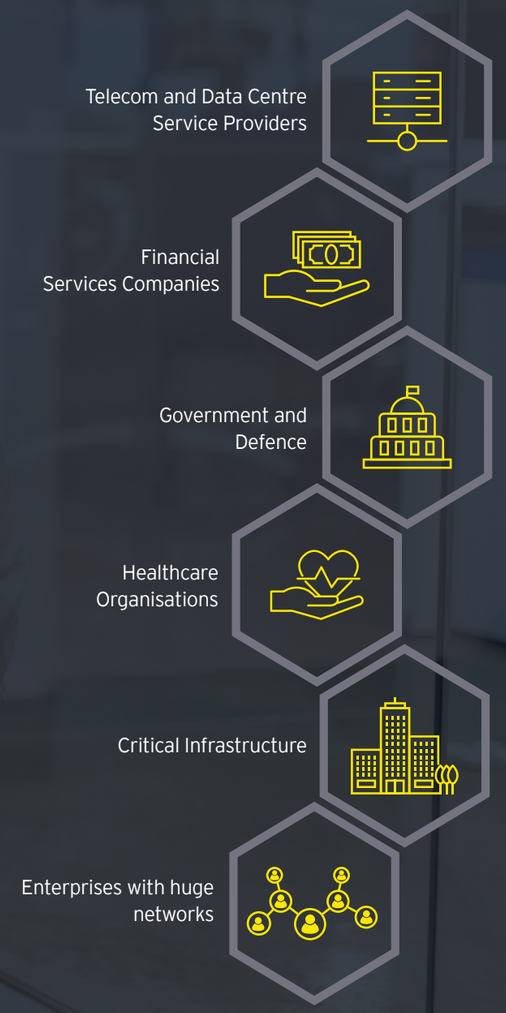
- Connection with the cloud
- Connection between business sites
- Data center interconnections
- Satellite communication
- Metropolitan backbone optical network
- Long-distance distribution network



Markets

Quantum Key Distribution (QKD) technology has a variety of applications. It provides enhanced security over classical cryptography schemes. With the development of quantum computers, classical cryptography suites lose their ability to be safe. QKD, in turn, is entirely free of this disadvantage and can withstand an attack performed with the help of a quantum computer.

This makes QKD technology most relevant for those organizations that process and transmit highly-sensitive information requiring protection due to regulatory requirements with a long lifespan.



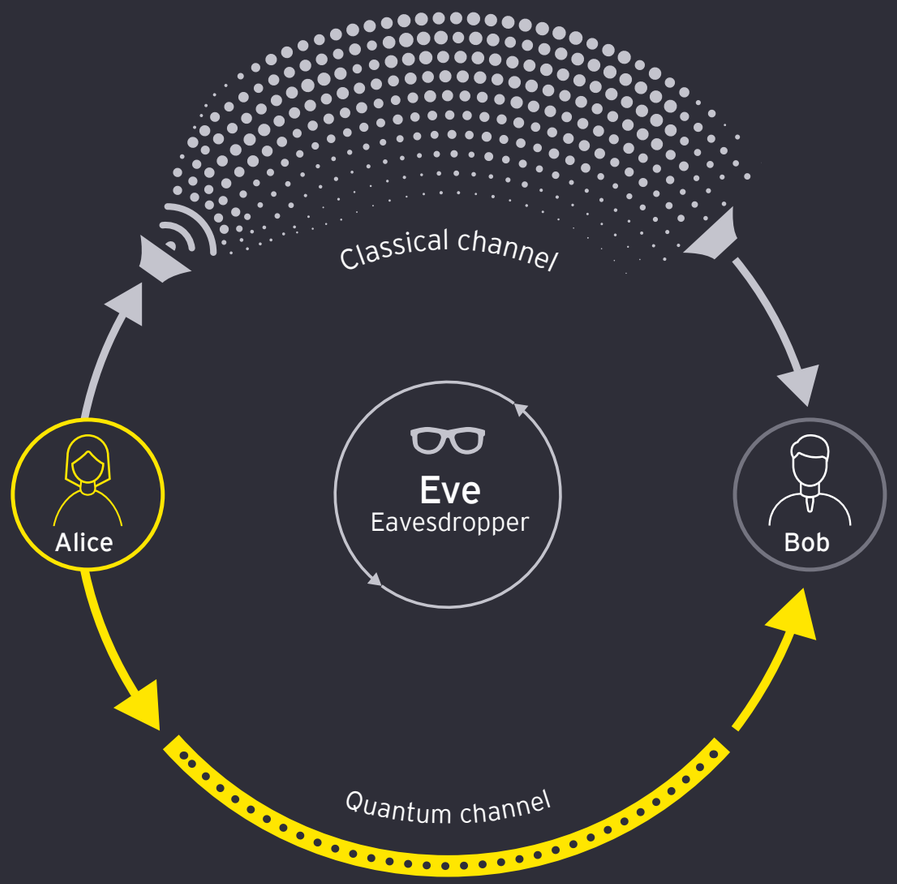
QKD superiority over classical cryptography

The sender (Alice) and the receiver (Bob) want to exchange information so that no one but them can read it. To do this, they must agree on a secret that no one (Eve) knows. The data is encrypted using this secret.

The challenge is in agreeing on a key without meeting each other in-person. This needs to happen quickly and over open (insecure) channels.

Alice and Bob might use existing classical algorithms, but as quantum computers evolve, they become insecure. Quantum Key Distribution scheme does the same job but remains resistant to a quantum computer attack.

It allows Alice to generate a secret and send it to Bob in a way that no one can intercept it.



Suppose Alice and Bob decide to use existing Key Exchange schemes (e.g., Public Key Cryptography). In that case, the security of their transmission ultimately relies on mathematical problems that are difficult for classical computers. A breakthrough in technology may render conventional ciphers vulnerable. A sufficiently powerful quantum computer, for example, could solve previously unfeasible mathematical problems and break modern cryptography protocols.

Researchers are working on so-called Post-Quantum Cryptography[1] – methods that will continue to be effective after quantum computers are powerful enough to break existing key exchange methods. However, these are all based on the **assertion that certain numerical algorithms are difficult to reverse**.

Quantum Key Distribution (QKD) is the only known method for transmitting a secret key that is proven to be **secure as per the laws of quantum physics**.

In contrast to conventional key distribution algorithms, QKD is the cryptographic technique which offers forward security – resilience against new attack algorithms and upcoming quantum computers.

QKD systems are "provably secure", but this is not the same as "unhackable", "unbreakable", or "unconditionally secure". "Provably secure" has a specific quantitative technical definition relating to the probability of eavesdropping in a nominally successful round of communication.

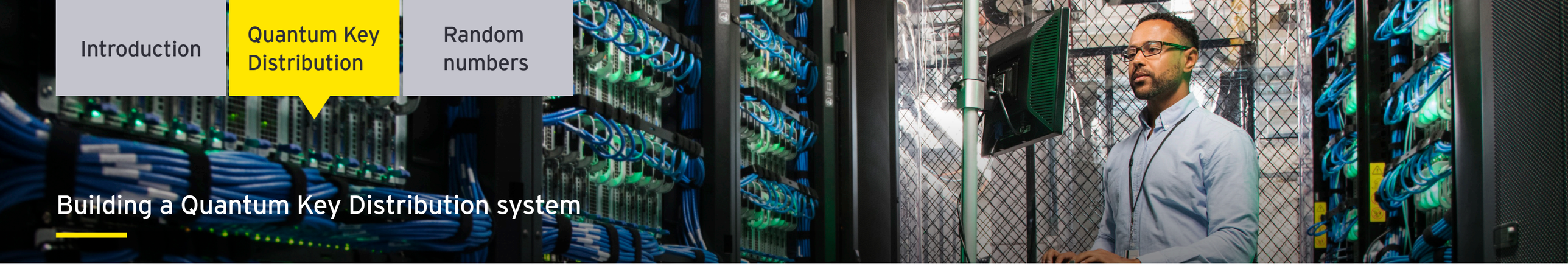
While it is worth noting that quantum physics may provide nature-based security through QKD algorithms, the physical implementation of the system is still subject to threats. More broadly, systems that implement QKD algorithms will also need to be protected from threats, and there is a subfield dedicated to attacks on quantum systems.[2]

QKD works by using light particles (photons) to transfer a secret between Alice and Bob. Even though Eve can intercept some of the photons, Alice and Bob will know exactly which photons have been intercepted. It is impossible to hijack a photon without Alice and Bob knowing about it.

Alice and Bob will leave only photons that certainly no one has seen, and the intercepted ones simply will not be used. As a result, they will have a secret no one know about.

QKD may become a cornerstone of network security for high-value data.

(1) https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
(2) https://www.nature.com/articles/s41598-018-22700-3



Building a Quantum Key Distribution system

Risk assessment

- Identify the security risks presented by vulnerabilities and threat actors, and their impact to the business. QKD is aimed at tackling network and communications-related risks.

Threat modelling

- Identify threat actors. Who are you protecting against?
- Develop threat scenarios specific to an organisation.

Determine if you need a QKD System

- Identify risks that are poorly covered by the existing network architecture and encryption solutions.
- Assess the impact of QKD systems on identified risks.
- Use a detailed network architecture review and network traffic analysis to enable a more granular impact analysis of QKD.
- Prepare a business case for QKD, including risk and benefit analysis.

Vendor selection

- Consider the solutions in the market using selection criteria such as: cost, ease of use, level of risk mitigation, resilience, availability, integration with other devices and management protocols, throughput capacity and regulatory requirements.
- Assess vendors against these selected criteria.

Deployment and implementation

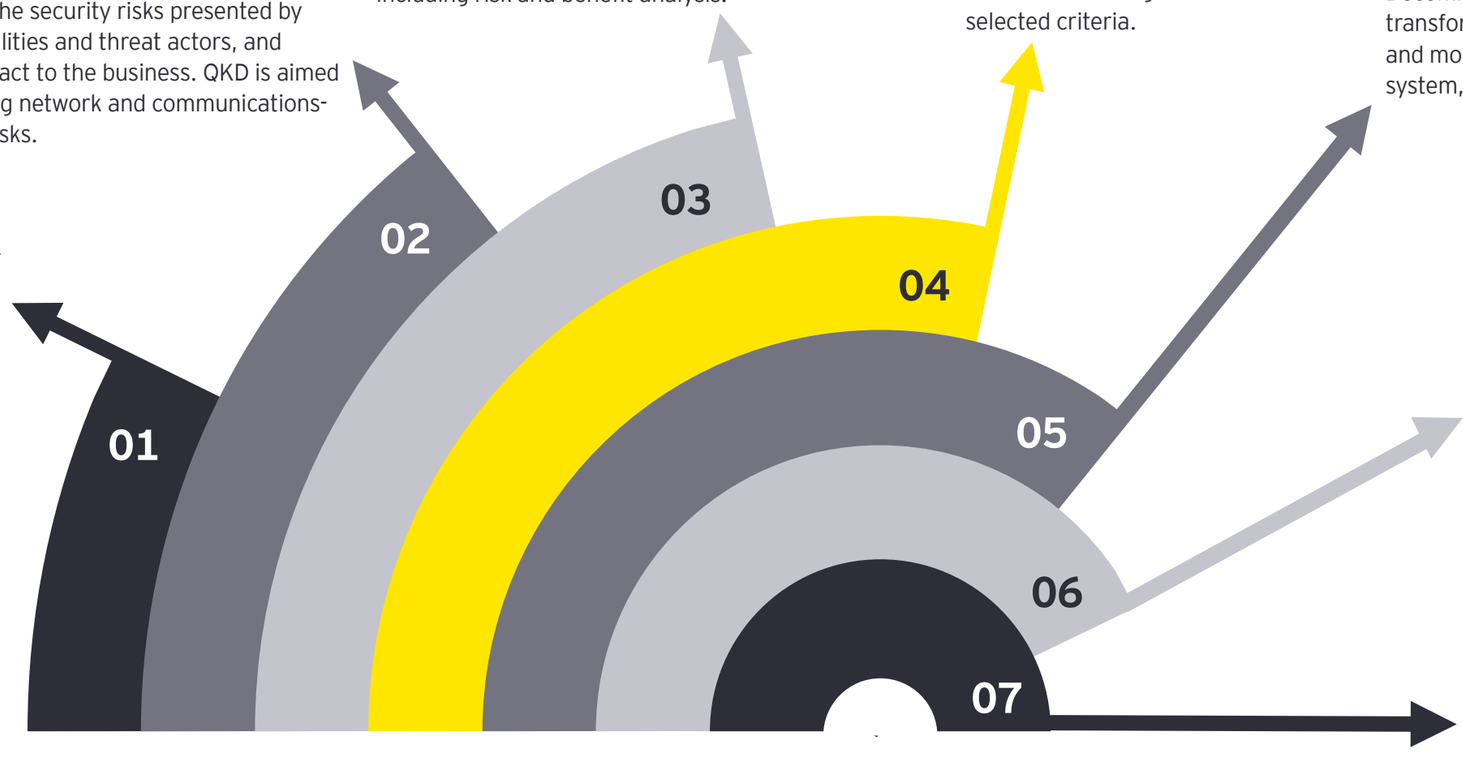
- With the assistance of vendors and subject matter experts, implement, configure and test the QKD system.
- Decommission "legacy" systems, transform existing infrastructure, and modify the network management system, if required.

Operational uplift

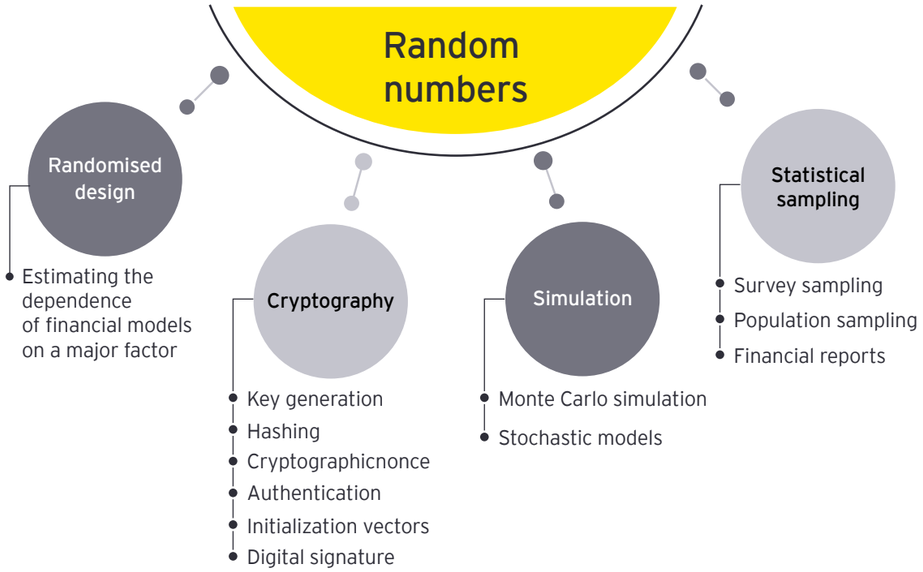
Update internal processes and documentation to reflect the change in infrastructure, and to ensure key employees have the information needed to perform their roles. Documentation may include a risk profile, network/ cryptography policies and standards, and training material for the upskill of resources.

Ongoing assurance

- Perform an independent review of the QKD system configuration to confirm that it is working as intended.
- Update an organisation's risk profile with emerging cyber threats.



Quantum Random Number Generators give pure randomness – true entropy



Random numbers are everywhere. The quality of their "randomness" affects a system or an algorithm build upon them. Random numbers should have a high degree of entropy; they must be as close to truly random as possible.

Many cryptography protocols, like the ones that secure credit card transactions or confidential documents, rely on long strings of random numbers. These numbers are used to begin the encryption process. The less guessable the number, the higher the security.

Traditional deterministic random number generators (Pseudo Random Number Generators) may not have sufficient "randomness" to remain secure.

- Some devices encrypt information using algorithm-generated numbers – which means that if you possess the algorithm, the numbers are entirely predictable.
- Other random number generators might convert electrical noise, like small fluctuations in voltage, into strings of numbers. But over time, these generators deteriorate and end up producing numbers that exhibit patterns.

Any discernible pattern is a security risk.

Quantum Random Number Generators (QRNG) provide encryption keys with high entropy; they are derived from a quantum source which is unpredictable by nature. Integrating QRNG into your security architecture is an essential first step to building quantum safety.

(1) https://eprint.iacr.org/2012/064.pdf

What can go wrong if random numbers could be predicted?

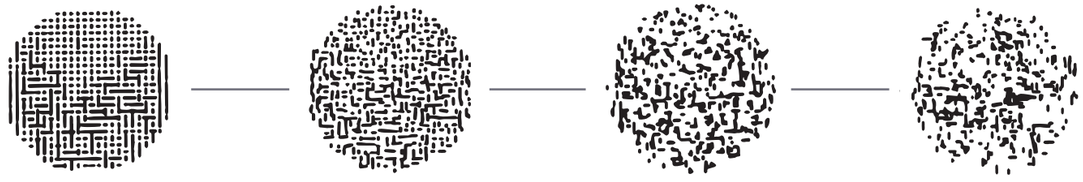
Data leak because of poor random numbers

If random number generators could be secretly modified to have less "randomness" entropy than stated, the encryption based on these random numbers may be susceptible to attack.

For example, spy agencies such as the NSA and GCHQ used this technique to demonstrate the capability to break HTTPS encryption.[2] By knowing the random number patterns, agencies were able to efficiently guess passwords.

Data leak because of poor random numbers

In 2010, a U.S. lottery draw was rigged by a man who surreptitiously installed backdoor malware on the Random Number Generator used to generate the lottery outcome. A total amount of $16,500,000 was won by predicting the numbers correctly a few times in year.[3]



(2) https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
(3) https://www.thedailybeast.com/inside-the-biggest-lottery-scam-ever

What should be considered when implementing Quantum Random Number Generators?

1. **Include QRNG into your strategy**
   - QRNG implementation is not an overnight change.
2. **List IT assets, including vendor-owned**
   - List IT assets where random numbers are of paramount importance.
   - Every organisation consumes vendor developed software with limited control and visibility of underlying technology.
3. **Consider building Entropy as a Service**
   - Equip your environment with high entropy random numbers. This is becoming increasingly important as the Internet of Things (IoT) grows.
4. **Implement QRNG for critical assets**
   - Where quality of randomness is critical to protect sensitive assets, consider the early implementation of dedicated hardware Quantum Random Number Generators.

Who is investing right now?

Business cases

China

China has established a quantum network between Beijing and Shanghai and an extension including the Hubei and Hefei provinces. The network is augmented with satellite-based quantum key distribution using the Micius satellite.[1]

Huishang Bank has transitioned to quantum encryption between its main and back-up data centres. Quantum encryption is also in place for the transmission of digital certificates between its branches and the certificate authority.[2]

Switzerland

Services Industriels de Genève (SIG), Geneva's utility company, secured their data centres with a quantum encrypted interconnect.[3]

The 2007 Switzerland elections used quantum encryption to protect the line from ballot counting centres in Geneva to the centralised data repository. This is still in use annually for Geneva elections.[4]

Japan

A collaboration between various Japanese and Australian companies and educational institutions has implemented the Tokyo QKD network for communications research and development.[5]

United Kingdom

A quantum link was established between Suffolk and Cambridge via nodes provided by British Telecom (BT). This forms a part of the future UK quantum network.[6]

QKD Roadmaps

US

In July 2020, officials and scientists from the University of Chicago and the Department of Energy unveiled plans and a blueprint strategy to build a "quantum internet".[7]

UK

In September 2015, the United Kingdom released a quantum roadmap for stimulation of application and market opportunities as well as building a strong technology foundation.[8]

Russia

In August 2020, Russia, within a broader Digital Economy program, approved the quantum technology development roadmap. The roadmap covers the development of secure communication lines and quantum computing.[9]

Australia

In May 2020, Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO) released a roadmap for quantum development, outlining Australia's position for quantum opportunities.[10]

(1) https://www.chinadaily.com.cn/a/201811/15/WS5bed3644a310eff303288f4b.html
(2) https://www.digfingroup.com/huishang/
(3) https://www.idquantique.com/services-industriels-de-geneve-collaborates-with-adva-and-id-quantique-to-secure-their-links-between-datacenters-with-leading-edge-quantum-cryptography-for-the-first-time/
(4) https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/
(5) http://www.uqcc.org/QKDnetwork/
(6) https://newsroom.bt.com/testing-begins-on-uks-ultra-secure-quantum-network-link-ukqntel-between-research-and-industry/
(7) https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet
(8) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470243/InnovateUK_QuantumTech_CO004_final.pdf
(9) https://www.tadviser.ru/index.php/Статья:Сквозные_технологии_цифровой_экономики
(10) https://www.csiro.au/en/Showcase/quantum

Contacts

Anthony Robinson
EY Oceania Cybersecurity Leader

Phone: +61 2 9248 5975
Email: anthony.robinson@au.ey.com

Jacqueline Kernot
EY Cyber Security Partner

Phone: +61 2 9248 5290
Email: jacqueline.kernot@au.ey.com

Alexey Bocharnikov
EY Cyber Security Senior Manager

Phone: +61 2 9248 5613
Email: alexey.bocharnikov@au.ey.com

We acknowledge the assistance of Vikram Sharma from QuintessenceLabs in the preparation and review of this article.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. OC00000595

BMC Agency
GA 1018647

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/mfg