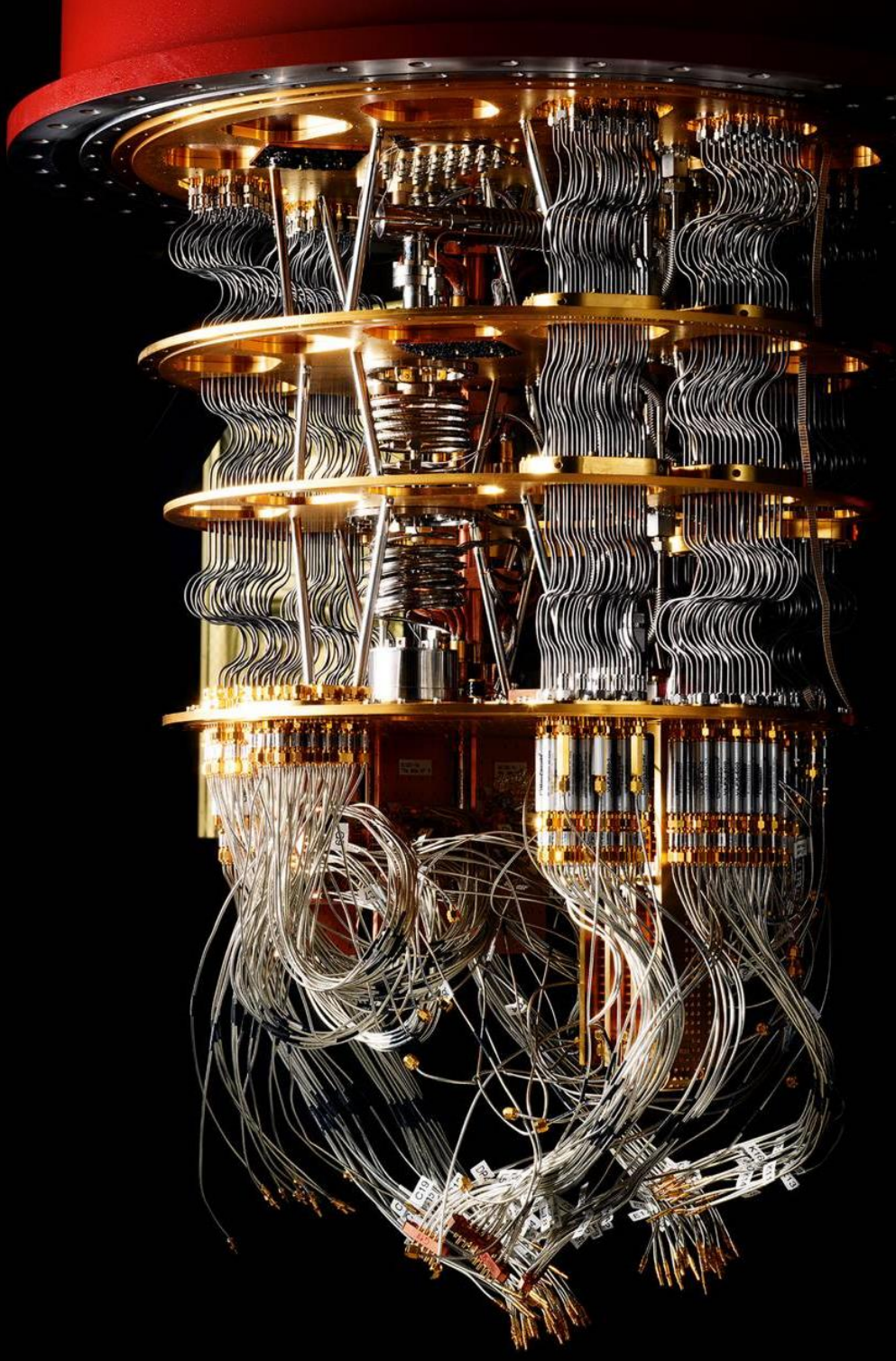
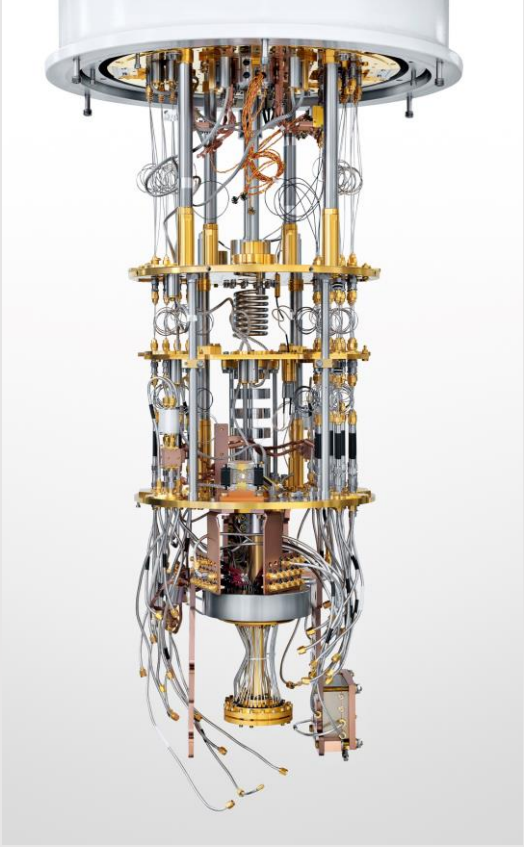


Unleashing the power of Quantum Based Cryptography

White paper by QRDLab



Quantum chandelier
RIGETTI COMPUTING / JUSTIN FANTL

What's in a qubit?

Just as there were different transistor designs in the early days of computing, there are currently many ways to make qubits. Google and IBM both use a version of the leading method, a superconducting transmon qubit, of which the core component is a Josephson junction. This consists of a pair of superconducting metal strips separated by a gap just a nanometer wide; the quantum effects are a result of how electrons cross that gap.

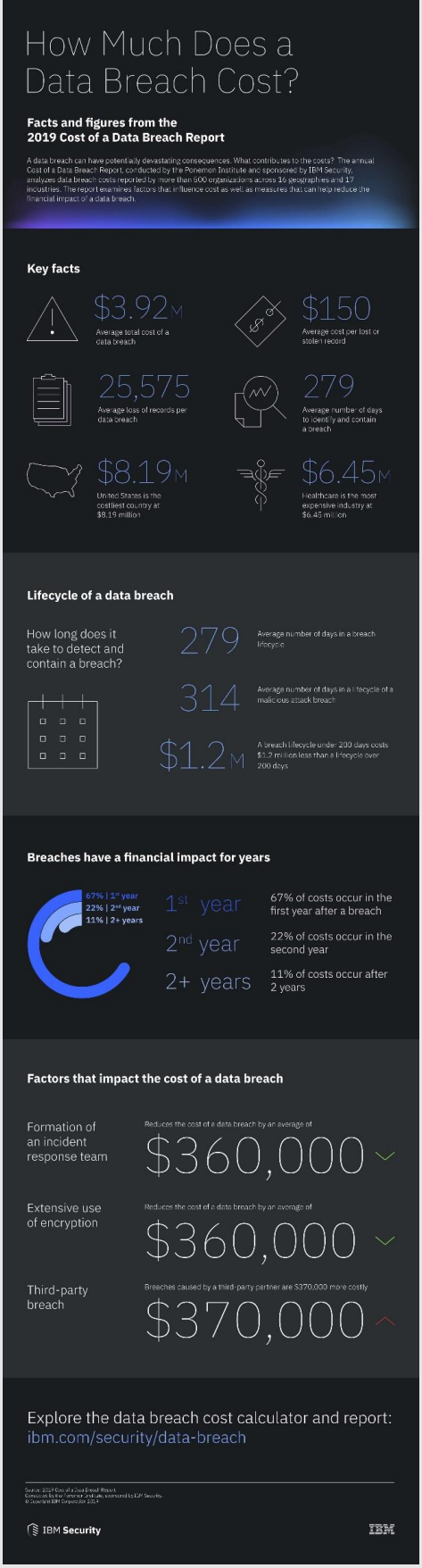
What is a Quantum Computer?

Quantum computers are exponentially more powerful than its classical counterpart, it outperforms the most advanced type of modern digital computers.

Quantum computers relies on the principles of Quantum mechanics and uses quantum bits (qubits) which are different from the classical bits, while classical bits hold values of either a 0 or a 1, qubits on the other hand can be in a superposition of 0 and 1 at the same instant of time.

However, they won't wipe out conventional computers, though. As, using a classical machine will still be the easiest and most economical solution for tackling most problems. But quantum computers promise to power exciting advances in various fields, from materials science to pharmaceuticals research.

Companies are already experimenting with them to develop things like lighter and more powerful batteries for electric cars, and to help create novel drugs.



"Cybercrime represents big money for cybercriminals, and unfortunately that equates to significant losses for businesses," Wendi Whitmore, Global Lead for IBM X-Force Incident Response and Intelligence Services.

Why Cryptography?

Cryptography is the science of hiding information in plain sight, in order to conceal it from unauthorized access. It is a technique of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography makes web sites and electronic safe transmissions possible in a secured manner. Due to the large number of commercial transactions on the internet, cryptography is very key in ensuring the security of the transactions.

Cryptography allows you to have confidence in your electronic transactions. Without cryptography, hackers could get into our e-mail, listen in on our phone conversations, tap into cable companies ,acquire free cable service, or break into our bank/brokerage accounts. Time stamping is a cryptographic technique that can certify that a certain electronic document, communication existed or was delivered at a particular time.

In general, cryptography is an important way of achieving data confidentiality and data integrity.

QUANTUM-BREAKABLE

RSA encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman key exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic curve cryptography

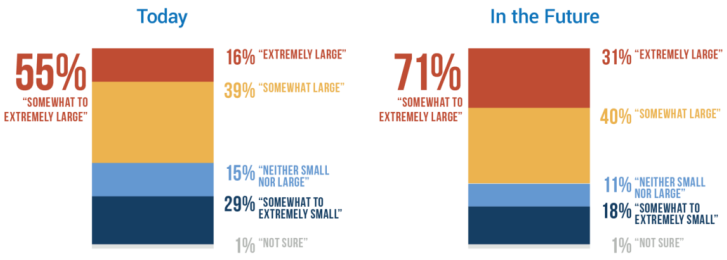
Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

"It is now clear that current Internet security measures and the cryptography behind them will not withstand the new computational capabilities that quantum computers will bring," NSA spokesperson Vanee' Vines stated in an email, confirming the change.

Are Quantum Computers a threat to Cryptography?

The development of quantum computers is both a boon and bane for modern technologies. No wonder in the fact that quantum computers have become the new front for both the business and government sector. But, as mentioned earlier quantum computers are both an opportunity and a threat, the biggest threat being the fact that quantum computers do threaten encryption. Which is by far one of the most sensitive parts of digital security as it provides privacy to our data, starting from banks to healthcare.

The standard encryption algorithms that are used in this modern technological era will soon be compromised by quantum computers. It has been surmised that a quantum computer with 4,000 qubits will be able to easily compromise encryption algorithms which are considered to be extremely strong.



Survey on Quantum Computing threat from DigiCert and ReRez Research that gathered data from IT staff at 400 enterprises in the US, Japan, and Germany.

Classical Encryption Algorithms

There are generally two types of encryption algorithms

- Symmetric Encryption – It uses one key commonly called the private key which is used both for encryption and decryption of data. Generally it is either block cipher or stream cipher. The most common symmetric encryption model that is widely used is AES (Advanced Encryption Standard).

- Asymmetric Encryption – It uses two keys, public key and private key, the private key is used for encryption and the public key is used for decryption of data. The most common asymmetric algorithm that is being widely used is RSA (Rivest, Shamir, Adleman) named after the inventors of this public-key encryption technology.

Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

Overview of Advanced Encryption Standard

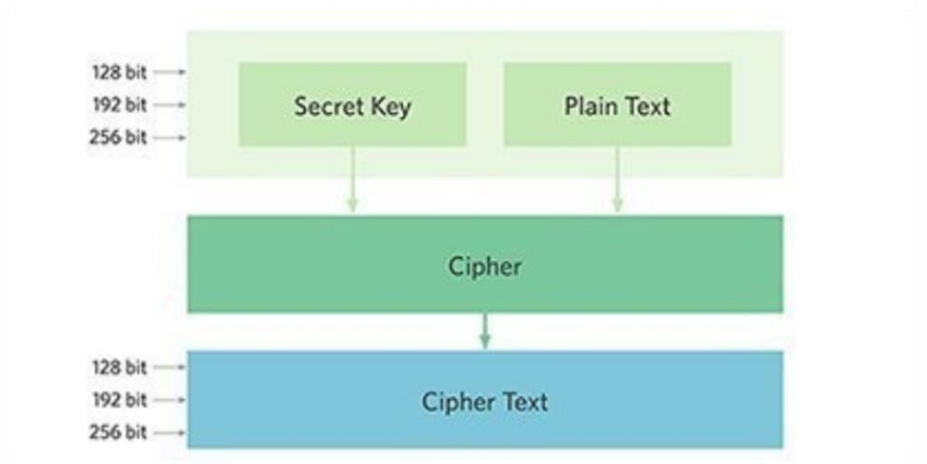
AES encryption was established by the United States National Institute of Standards and Technology (NIST) in 2001 and it aims to offer a specification for electronic data encryption. AES is characterized as being a symmetric block cipher, in other words it uses the same key for encryption and decryption.

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). AES performs all its computations on bytes rather than bits. However the number of rounds in AES is variable and depends on the length of the key. Each of which rounds uses a different 128-bit round key, which is calculated from the original AES key.

Types of AES encryption (Based on number of rounds) :

- 128 - Bit keys encryption - 10 rounds
- 192 - Bit keys encryption - 12 rounds
- 256 - Bit keys encryption - 14 rounds

The schematic representation of AES Encryption



More on Advanced Encryption Standard

The encryption process of AES comprises of four sub-rounds for each round, The four sub-rounds are depicted below namely,

Byte Substitution - Popularly known as Sub-Bytes, is a sequence of 16 input bytes that are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift Rows - Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of the row.

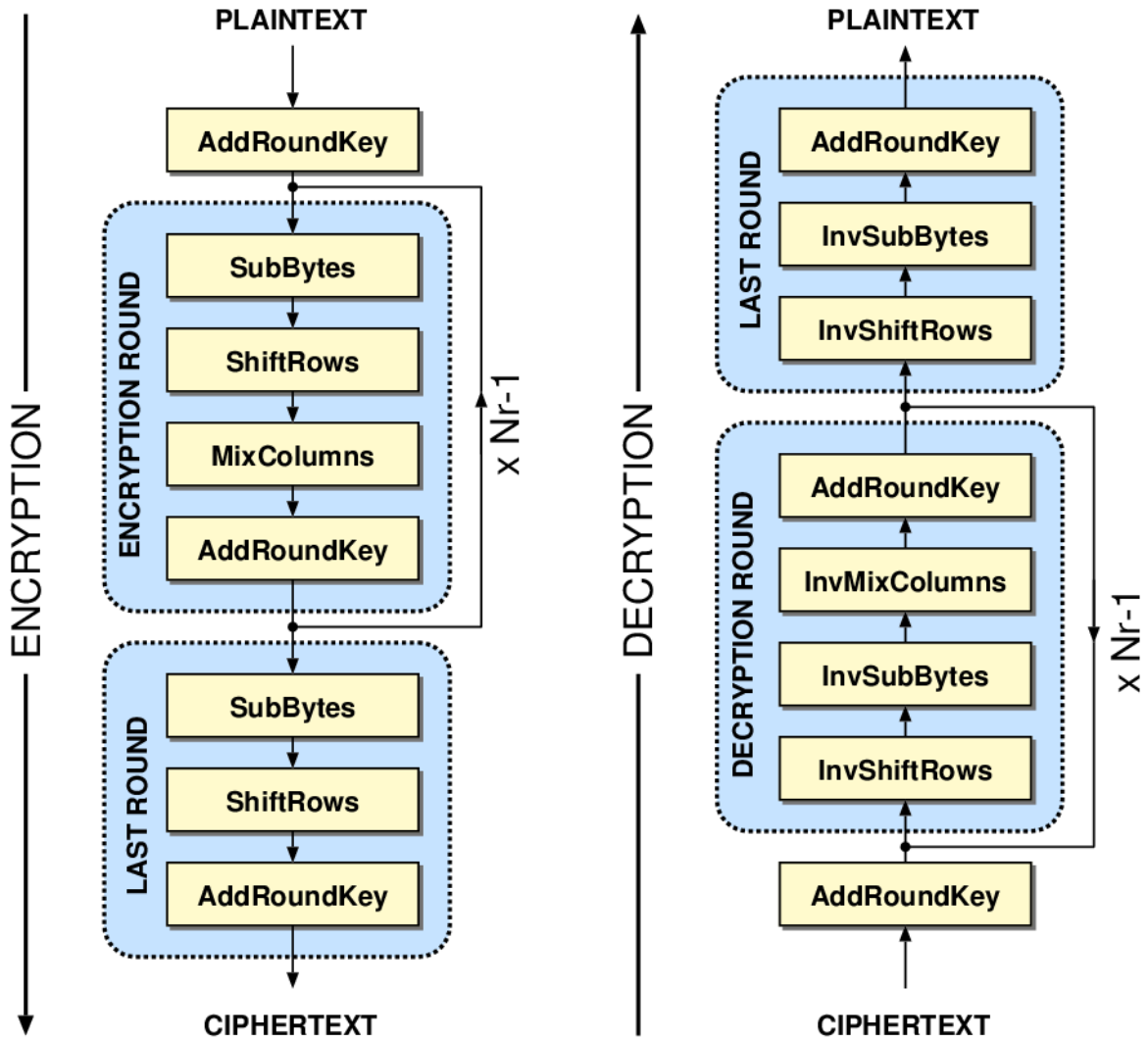
Mix Columns - Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes.

Add Round Key - The 16 bytes of the matrix are then considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and another similar round begins.

The Decryption process of AES is just the reversed order of the encryption and the sub-rounds of the rounds are, Add Round Key followed by Mix columns followed by Shift Rows and the last sub round being Byte Substitution.

More on Advanced Encryption Standard (Cont.)

The Schematic of AES Encryption model and Decryption model is shown below:



So is AES under threat by Quantum Computers?

In short yes as well as no.

Firstly, asymmetric encryption algorithms like RSA and Diffie - Hellman have been mathematically proven to be impacted and be broken by quantum computers using Shor's algorithm.

However, that's not the case for symmetric encryption algorithm mostly talking about AES (AES-256 to be precise). As unlike asymmetric encryption algorithms, symmetric encryption algorithms don't rely on prime factorization which was once believed to be extremely safe as factorizing is a really tedious, time taking and extremely complex problem to be tackled by a classical computer and could take up to a 1000 years or more, but, with the help of quantum computers and quantum computational algorithms like Shor's algorithm it can speed up the whole process exponentially, It has been surmised that a quantum computer with 4,000 qubits will be able to easily compromise encryption algorithms under minutes which are considered to be extremely strong and would take several years for a classical computer. And, in case of symmetric algorithms there exists no explicit quantum computing algorithm that could give an exponential speed-up. However, the best possible known approach to compromise the AES algorithm is brute-forcing which is nothing but searching through the possible key streams, and there exists a vey well known quantum computational algorithm that could speed up the whole process of searching quadratically, Grover's algorithm. Now, Grover's algorithm can reduce the brute force attack time to its square root. So for AES-128 the attack time becomes reduced to 2^{64} which is considered to be not secure) while, AES-256 becomes reduced to 2^{128} which is considered to be extremely secured according to the current norms.

So, It can be concluded that AES-256 is not quantum-breakable, but..

But, there exists a problem!!

Now, the reason behind the fact that it is not completely secured from the hands of the era of quantum computation is because most of the classical encryption algorithms use random numbers for their key generation.

However, random numbers can be classified into two types

- Pseudo Random Number
- True Random Number

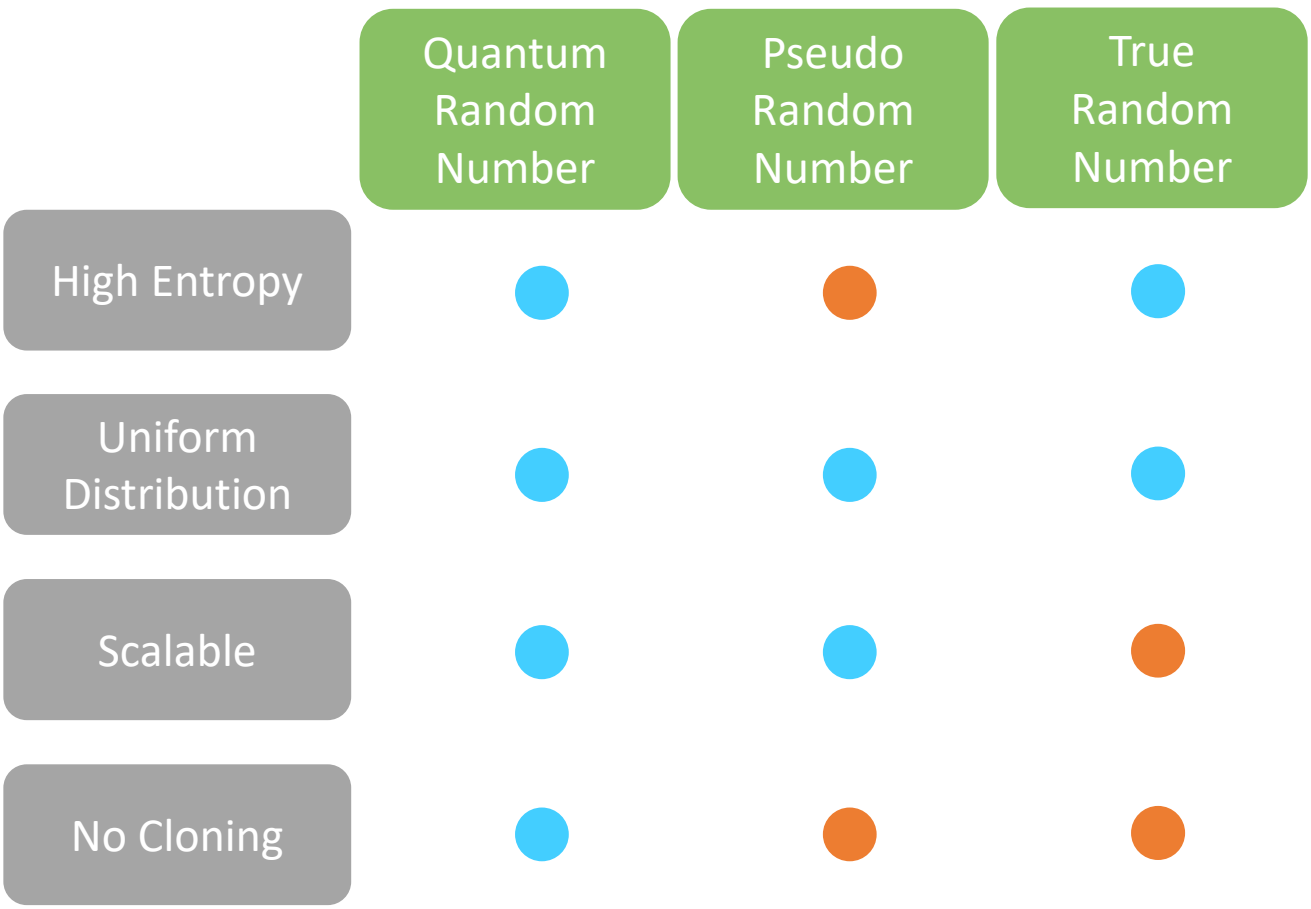
Now the real problem exists in the fact that the random numbers that are being used are mostly pseudo random numbers, or in other words generated using software methods, which means that the 256-bit keys derived from passwords actually can have less than 256-bits of entropy because of which an attacker could try deriving keys from likely passwords which would be next to impossible for random 256-bit numbers.

And, a quantum machine learning algorithm could exists which could speed up the whole process to find out the bit stream due to lack of randomness in the system. However, the use of a classical system based true random number generator is slow, expensive and less efficient to use.

However, there exists a solution to solve the problem, Quantum Random Number generators, since Quantum Computing is a probabilistic approach of computing and offers unprecedented growth in computing through parallelism. Quantum phenomena is inherently random which results in generation of true random bits, which eventually will be free from any non-uniformity or biasedness resulting in negligible statistical error and correctness in research conclusions unlike pseudo random number generators.

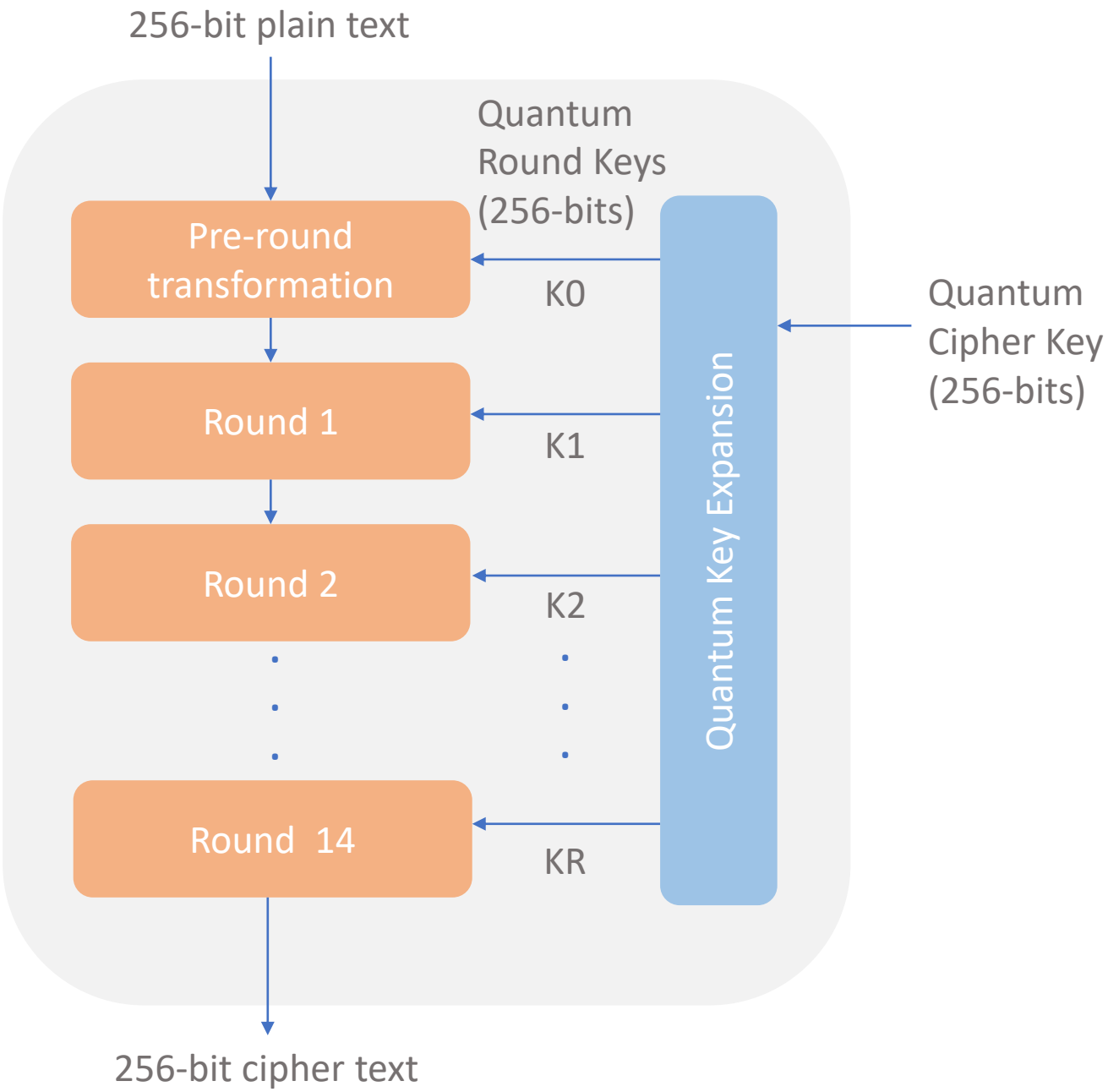
How QRNGs compare to other RNGs?

The comparison chart is shown below



Architecture of our solution

The proposed architecture of the model is shown below



Here the Quantum Cipher Key is generated from a Quantum Random Number Generator which ensures true randomness and makes it secured from best possible known attacks.

Use cases of Quantum aided Encryption

Use Case 1: Online Payments

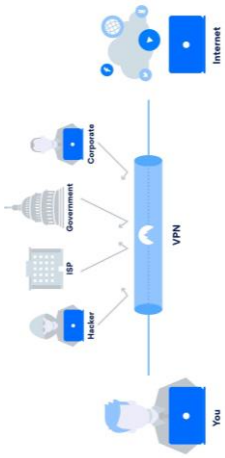
One of the most sensitive areas where encryption is used is in online payment. Even PCI-DSS standards mandate payment card data (stored as well as in-transit forms) to be encrypted using algorithms such as AES-256. However as mentioned before with upcoming quantum computing era such algorithms will not aid in securing our data any longer. However, quantum computing aided cryptographic algorithm helps in such cases and makes it quantum safe.

Use Case 2: Databases

Database is another sensitive area handling all of our confidential data (from transaction passwords to health data) making encryption a must have. Encrypting databases help to restrict external hackers as well as insiders from seeing specific organizational data. Transparent database encryption (TDE) is a popular database encryption technique that helps to encrypt all “data at rest” in one go. Making it quantum safe in the quantum era is a must.

Use Case 3: VPN

VPNs OR Virtual Private Networks are extremely useful and are used by many people for their business, personal data transaction, online payment and is also used by governments.



- Many businesses use this so that their remote employees can connect to the office and connect to file servers email servers and other services without having to make them directly available over the internet and hence creating a secured environment. For own Data privacy like sharing sensitive information over internet, online transactions and many more
  While using a public wireless network where it is really unsecure to surf the web
- By governments for sharing secretive and confidential information and requires a secured environment for data transfer

However VPNs rely on encryption algorithms however most VPNs rely on algorithms which are not quantum safe and is susceptible to quantum

intervention. Here a quantum computing aided Encryption algorithm will help in boosting security.

Use Case 4: SSL

An SSL certificate (or TLS certificate) is a digital certificate that binds a cryptographic key to your organization's details. Secure Sockets Layer (SSL) are cryptographic protocols designed to encrypt communication between a server and a web browser. Encryption data reduces the cybersecurity risk of man-in-the-middle attacks or many other forms form of cyber attack. Traditionally, SSL has been used to secure credit card information on e-commerce sites, personal data transfer and to secure social media sites. However a quantum computing aided encryption algorithm would make the whole protocol quantum safe

Use Case 5: Data in the cloud

In public and hybrid cloud models, sensitive data resides at a third-party data center. Any attack on co-tenants can result in that data getting exposed too. Encrypting your data in the cloud prevents hackers from being able to read it correctly.
Quantum safe encryption algorithm helps in securing the data in the cloud.

Use Case 6: Emails

Email encryption helps to protect sensitive information sent through email channels. Public key encryption methods along with digital certificates are usually the methods used for securing email communications. Most email providers rely on quantum breakable algorithms making it susceptible to hacks. However, quantum computing aided cryptographic algorithm makes it quantum safe and much more secured.

References

- Peter W. Shor (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing. **26** (5): 1484–1509. arXiv:quant-ph/9508027. Bibcode:1995quant.ph..8027S. doi:10.1137/S0097539795293172.
- *"Cryptographers Take On Quantum Computers". IEEE Spectrum. 2009-01-01.*
- "Advanced Encryption Standard (AES)" (PDF). Federal Information Processing Standards. 26 November 2001. doi:10.6028/NIST.FIPS.197. 197.
- Quantum Security Analysis of AES, Xavier Bonnetain , María Naya-Plasencia and André Schrottenloher,
- Breaking Symmetric Cryptosystems using Quantum Period Finding, Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia
- M. Siswanto and B. Rudiyanto, "Designing of quantum random number generator (QRNG) for security application," 2017 3rd International Conference on Science in Information Technology (ICSITech), Bandung, 2017, pp. 273-277, doi: 10.1109/ICSITech.2017.8257124.
- A. Narayanan, "Quantum computing for beginners," Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406), Washington, DC, USA, 1999, pp. 2231-2238 Vol. 3, doi: 10.1109/CEC.1999.785552.

Authors & Contributors

Subham Dasgupta, QRDLab
Nivedita Dey, QRDLab, University of Calcutta
Mrityunjay Ghosh, QRDLab, University of Calcutta
Prof. (Dr.) Amlan Chakrabarti, QRDLab, University of Calcutta