QUANTUM CRYPTOGRAPHY

AUTHORS

VARALAKSHMI.K
DIVYA NANDINI.R
LATSHANA. PR

INTRODUCTION

In a world where data privacy and security are paramount, quantum cryptography presents itself as a fascinating and innovative solution.Quantum cryptography is a method of encryption that uses the properties of quantum physics to secure and transmit data so that the sent information cannot be hacked.In this white paper,let’s acknowledge the importance of quantum cryptography over cryptography.When public or private entities in a city or region that manage critical infrastructures, for example hospitals, electrical plants, or public transportation, use the internet to send important information between their headquarters and operation sites, how can they guarantee that they are not being hacked, or that nobody is trying to steal the information that is transmitted? In most cases, today we send information through the internet where the security of the net relies on different methods , one of them called public-key cryptography.

Public Key Cryptography

Here, two keys are generated : a public-key that is sent to one party, and a private key that remains with the other party. The message is encrypted using the public-key and opened with the private key. The security of this method relies on that the private key is secret, and only the party receiving the message has access to it. The public and private keys are created using different mathematical algorithms. The most famous is based on the factorization of a large number into prime numbers, and it is known as RSA.Anyone can see the message but they can't read it without the key. This is what Queen Mary of Scots used to try to assassinate queen Elizabeth.

How it differs from crytography?

What makes it so powerful is that instead of math it relies on the laws of physics. Two laws in particular: the Heisenberg uncertainty principle and the principle of photon polarization. It says that you can't know absolutely everything about the state of a quantum particle. It's not because you're not smart enough or your equipment isn't good enough, it's just because nature keeps some things hidden. The Heisenberg Uncertainty principle states that, “Measuring the quantum state of any system without distributing that system is impossible”. The principle of photon polarization states that, “an unknown qubits can be copied by the eavesdropper” that is unknown quantum states, due to no-cloning theorem.

Future-Proof Technology

- Quantum cryptography is considered a future-proof technology, as it is immune to advancements in computing power. With the rise of quantum computers, traditional encryption methods may become obsolete, making quantum cryptography an essential tool for long-term security.
- By adopting quantum cryptography now, organizations can stay ahead of the curve and ensure that their data remains secure in the face of evolving threats.

BENEFITS OVER TRADITIONAL CRYPTOGRAPHY

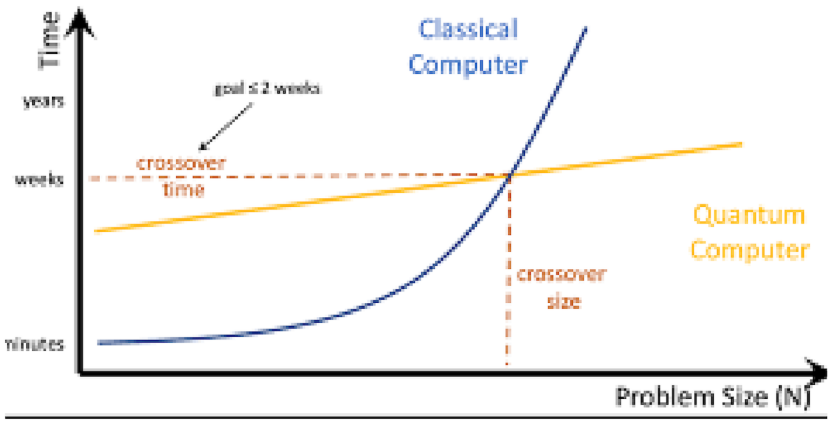
- Secure Communication
  - Quantum cryptography ensures secure communication by leveraging the principles of quantum mechanics to encrypt messages.
- Financial Transactions
  - Protecting financial transactions from eavesdropping and tampering is crucial, making quantum cryptography an ideal solution.
- Government and Military
  - Government agencies and military organizations rely on quantum cryptography to safeguard classified information.

Securing IoT Ecosystems

- In the era of the Internet of Things (IoT), billions of devices are interconnected, posing security challenges.

- Quantum cryptography can provide a robust security framework for IoT ecosystems, safeguarding sensitive data transmissions.

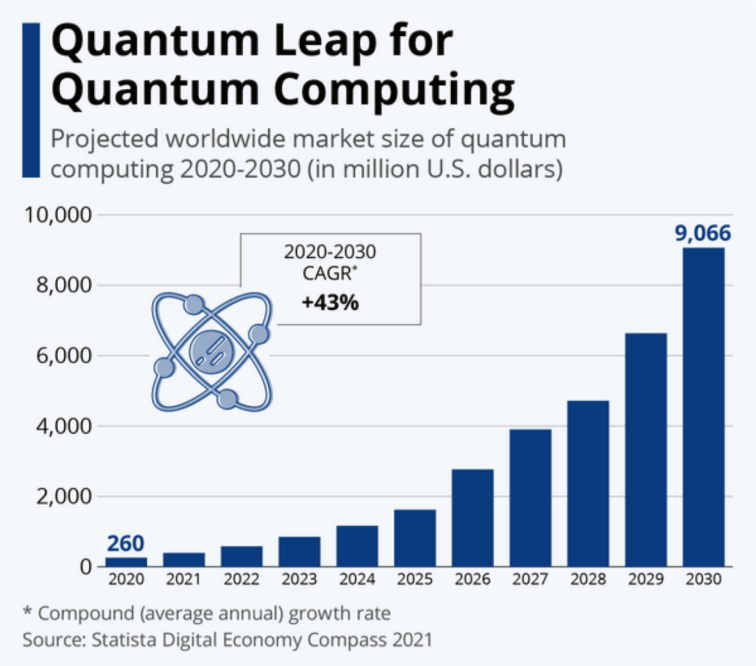
- By implementing quantum secure communication protocols, IoT devices can communicate securely without compromising data integrity.



The graph showcases the resilience of quantum cryptography against quantum computing attacks, which pose a significant threat to traditional encryption methods.

Growth of Quantum Cryptography Research Publications

- This statistical graph showcases the exponential growth of research publications in the field of quantum cryptography over the past decade.
- The steep upward trend reflects the increasing interest and investment in this ground-breaking technology.
- Researchers and institutions from around the world contribute to the expansion of knowledge in quantum cryptography, as evidenced by the diverse sources represented in the graph.



CONCLUSION

- Amidst the challenges faced by quantum cryptography, its applications offer a glimpse into a secure and resilient future where data privacy is prioritized. Embracing the advancements in quantum technology is essential to stay ahead of cyber threats. Let's exploring the possibilities of quantum cryptography to enhance data security and privacy.

- By understanding challenges and applications of quantum cryptography, we pave the way for a safer digital environment where trust and privacy are not compromised. Let's embrace this innovative technology secure our communication channels from potential threats.

REFERENCES

- Shahid, F., Khan, A. and Jeon, G., 2020. Post-quantum distributed ledger for internet of things. Computers & Electrical Engineering
- Post-Quantum Cryptography, URL: https://csrc.nist.gov/projects/post-quantum-cryptography [Last Accessed on 21/04/2021].
- Agilepq Q3 2019 Report, A Guide to Post-Quantum Security for IoT Devices, URL: https://agilepq.com/wp-content/uploads/2020/02/Post_Quantum_IoT_WP.pdf [Last Accessed on 24 April, 2021] 2. Fernández-Caramés, T.M., 2019.