Time to time technological advancement has surprised us and disrupted the market. Each time we found a way to adapt and use those advancements for the betterment of people, product and business. Development of personal computers, mobile phones, smart phones and app based ecosystems, machine learning, AI and now more advancement in AI with large language models like ChatGPT etc. are primary examples of such advancements.

In current time, apart from ChatGPT another major advancement is happening in a field which I believe will have more impact in our day to day life. This advancement is based on a principle of physics on which once even Einstein was doubtful.

Yes, you guessed it right, I am talking about Quantum computing. While on one hand the community is excited about the promise technology is showing in the field of computational advancement (which will really be helpful to solve some of the problems which are nightmare even for the existing supercomputers), but on the other hand the same computational advancement can break almost all the secure systems we have today. Quantum computers will be able to break existing encryption and will be in a position to expose all the critical data.

To understand this idea we need to know few basic things:

1. How security work in our current system today
2. How Quantum computer can effectively break existing secure systems
3. Post quantum cryptography and
4. Preparedness to create quantum safe systems
5. Example PQC implementation

**Security in existing computer systems:**

When you visit a secure website (https), do online shopping or banking, data is transferred in a way that no one else can access private information.

As most of you have studied, the RSA algorithm is the most widely used encryption algorithm for data transmission. This is how it works:

* Two very large distinct prime number are chosen and
* Their product along with algorithmically calculated two exponents are used to create public and private key.
* Public key is used to encrypt the message
* Private key is used to decrypt the message

This encryption system relies on the fact that calculating the prime factor from the public key and figuring out the factors that made the private key is computational intensive and there is no algorithm that can do this in polynomial time.

**How Quantum computer can break security algorithms:**

One of the most popular and promising use cases for Quantum computers was Shor’s algorithm. Developed in 1994 by Peter Shor, this algorithm finds the prime factor of an integer and provides strong proof that quantum computers can be superpolynomial faster than current computers.

With a sufficient number of qubits and with no quantum noise and decoherence (described qubit, quantum noise and decoherence later) Shor’s algorithm can be used to break public-key cryptography schema such as RSA.

RSA is based on the assumption that factoring large numbers is computationally impossible. None of the existing classical algorithms can find out factors in polynomial time. On a perfect quantum computer, Shor’s algorithm shows that factoring integers is polynomial and efficient.

Due to the possibility of breaking RSA using quantum computers, a new field of research emerged in cryptography, **post quantum cryptography -** How will you secure your data once quantum computers will be available?

**Post Quantum cryptography**

As of today quantum computers lack processing power to break any encryption but researchers are preparing for the day when quantum computers will be fully functional and perfect to break. As per the analysis all current forms of asymmetric key exchange standardized for use in TLS and all of the digital signature and public key algorithms standardized for authentication in TLS, are vulnerable.

Researchers wanted to be safe from the concept of harvest now decryption later.

Main challenge of this problem is to implement quantum safe algorithms in the existing system.

**National Institute of Standard and Technology (NIST)** has created a program and competition - Post-Quantum Cryptography standardization. It was announced in 2016 and in August 13, 2024, NIST has released the first three post quantum crypto standards:

Federal Information Processing Standard (FIPS) 203, FIPS 204, FIPS 205.

**FIPS-203**  Primary standard for the general encryption.Small encryption key and speed of operation is its advantage. This standard is based on Crystals-Kyber algorithm which is renamed as Module-Lattice based Key Encapsulation Mechanism (ML-KEM)

**FIPS-204** Primary intention is to protect digital signature.The standard uses Crystal-Dilithium algorithm renamed as Module Lattice based Digital signature Algorithm (ML-DSA).

**FIPS-205 :** Also for digital signature. Standard uses Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) created for backup in case ML-DSA will be vulnerable.

**Preparedness to create quantum safe systems**

To prepare for PQC migration any organization can follow below steps:

* **Assess current security landscape**

1. Identify all systems and applications which use cryptography within org.
2. Analyse current algorithm and analyse which are vulnerable to quantum computers
3. Prioritize the fix based on data and impact.

* **Establish a team**

Setup a cross functional team of security experts, different project leads and developers.

* **Identify and evaluate PQC algorithms**

1. Follow NIST page for latest algos and
2. Evaluate different PQC algorithms for performance, compatibility etc.

* **Develop a migration plan**
* **POC and implementation**
* **Monitor and adapt for any further changes**

**Example PQC implementation:**

Bouncy Castle java library supports NIST standardized algorithms, making them to be used in java applications.

An example code to show post quantum hybrid encryption using java is uploaded for reference.

PQC is an interesting topic and needs careful planning in the organization to guard against future cyber attacks.