5.2 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a secure communication technique that uses quantum mechanical concepts to construct a cryptographic protocol. It allows two people to generate a shared, randomly generated secret key that is only known to them. With this key, communications may be encrypted and decrypted. Since quantum key distribution is the most well-known example of a quantum cryptographic problem, it should not be mistaken for quantum cryptography. Instead of using mathematics to secure the data, QKD employs a quantum system that depends on fundamental principles of nature. This sets it apart from traditional key distribution.

What is Quantum Key Distribution (QKD)?

Quantum Key Distribution (QKD), A protected communication technique for sharing encryption keys. It exchanges cryptographic keys in a way that is verifiable and ensures security by using characteristics of quantum physics. Using QKD, two parties may generate and exchange a key for encrypting and decrypting communications. To be more precise, QKD is the process of sharing the key between participants.

Purpose of Quantum Key Distribution (QKD)

- To mollify the threat posed by the rapid advancements in Quantum Computing to the security of data being conveyed by many vital sectors across existing communication networks Quantum Key Distribution is needed.
- The technique might help several small and medium-sized businesses and start-ups in the quantum information space.
- It will make it possible for security services to design a proper quantum communication network with a backbone made of domestic technology.
- The way data is transported by photons is primarily responsible for the encryption's unbreakability.
- A photon is impossible to replicate exactly, and each measurement effort will cause it to fluctuate. This implies that whoever tries to intercept the data will be caught.

Types of Quantum Key Distribution (QKD)

Below are two types of Quantum Key Distribution

- **Entanglement-based protocols:** Protocols based on entanglement centre on quantum states, where two items are coupled to generate a single quantum state. According to the idea of entanglement, measuring one entity therefore influences the other. The other parties involved will be aware if an eavesdropper gains access to a previously trusted node and makes any modifications.
- **Prepare-and-measure protocols:** The goal of prepare-and-measure procedures is to measure unidentified quantum states. They may be used to identify possible data interceptions as well as instances of eavesdropping.

How Quantum Key Distribution (QKD) Works?

The process involves the following steps:

- Several light particles, or photons, are sent between parties via fibre optic cables in order for Quantum Key Distribution to function.
- The photons are transmitted in a stream of ones and zeros, with each photon having a random quantum state.
- A photon passes via a beam splitter on its way to the receiving end, which compels it to choose a random path into a photon collector.
- The sender receives information from the receiver about the photon sequence that was transmitted, which they compare with the photon sequence that the emitter would have sent.
- A certain bit sequence is all that remains after photons in the incorrect beam collector are eliminated.
- During an error repair phase and other post-processing procedures, any mistakes and data leaks are eliminated.

Quantum Key Distribution (QKD) Attack Methods

- QKD appears secure in principle, security might be jeopardised by shoddy QKD implementations. Real-world applications have shown methods for breaking into QKD systems.
- An eavesdropper backdoor was intended to be created via the phase remapping exploit. The attack exploits the requirement for one party member to permit signals to enter and depart their device.
- The photon number splitting attack is an additional attack technique. A perfect scenario would allow one user to communicate with another user by sending one photon at a time.
- Coherent attacks are those that are deemed to demonstrate the security of a QKD system in the scenario when the eavesdropper possesses infinite processing capacity..

Benifits of Quantum Key Distribution (QKD)

Below are some benifits of Quantum Key Distribution

- QKD system may be utilised for more secure key management of several military cryptography systems in an integrated Cypher Policy Committee (CPC) framework in India.
- Security services will be able to create a suitable quantum communication network with a homegrown technological backbone thanks to it.
- The technique might help a number of small and medium-sized businesses and start-ups in the quantum information space.
- It is anticipated to define standards and develop rules pertaining to crypto technology.

Challenges of Quantum Key Distribution (QKD)

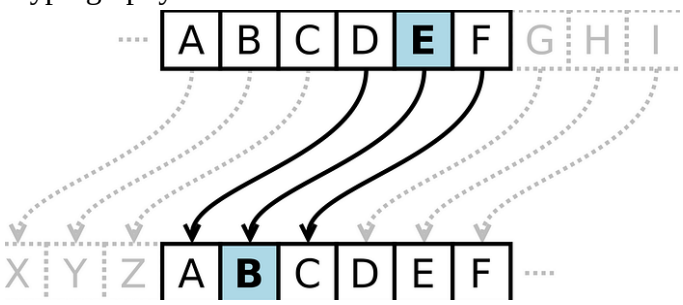
Below are some challenges of Quantum Key Distribution

- Establishing a classically authenticated communication route is necessary for quantum key distribution. This indicates that there was already enough security established because one of the involved users transferred a symmetric key in the first place.

- Putting in place the perfect infrastructure for QKD is challenging. In principle, it is completely safe, but in reality, security flaws are caused by flaws in instruments like single photon detectors.
- The distance that may be covered by terrestrial quantum key distribution (QKD) is limited by optical losses that occur during signal transmission through fibre and repeaters.
- Low cost and resilience are essential characteristics combined with excellent performance for QKD systems to be deployed in real-world applications. Many directions are being investigated at the moment.

Quantum Key Distribution and BB84 Protocol

Quantum key distribution (QKD), very closely related to quantum cryptography, is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics. Before discussing quantum cryptography, let's talk about the basics of classical cryptography.



Simple classical cipher.

Classical Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Classical cryptography has two major branches: **secret or symmetric key cryptography** and **public or asymmetric key distribution.**

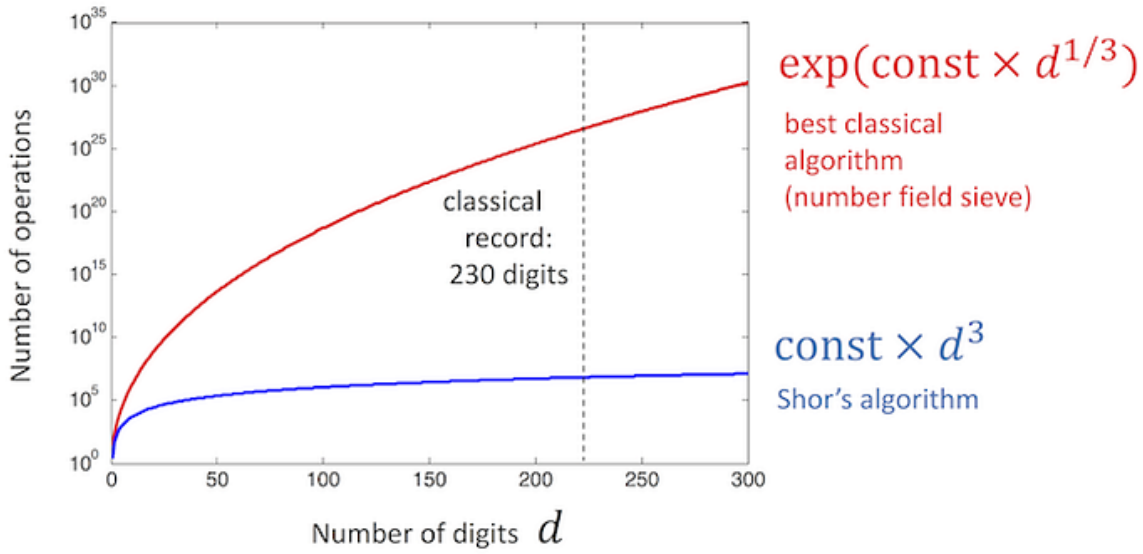
Secret Key Cryptography

Two parties encrypt and decrypt their messages using the same shared key in secret-key cryptography. The two parties must somehow share the key (physically, by email, or by letter) before using the key for secure communication. The downside is that you never know if someone stole the key while sharing it, which is a significant disadvantage of this cryptographic system.

Public Key Cryptography

In public-key cryptography, the key has two parts: public and secret. The data encrypted with the public key can only be decrypted with the private key, and the data encrypted with the private key can only be solved with the public key. The security of public-key cryptography is based on the unproven assumption about the difficulty of specific problems like integer factorization and the discrete logarithmic problem, which makes the system potentially vulnerable to improvements in computational power or the discovery of efficient algorithms. Indeed, there are algorithms to solve both integer factorization and discrete algorithm problems in polynomial time using quantum computers, like Shor's algorithm.

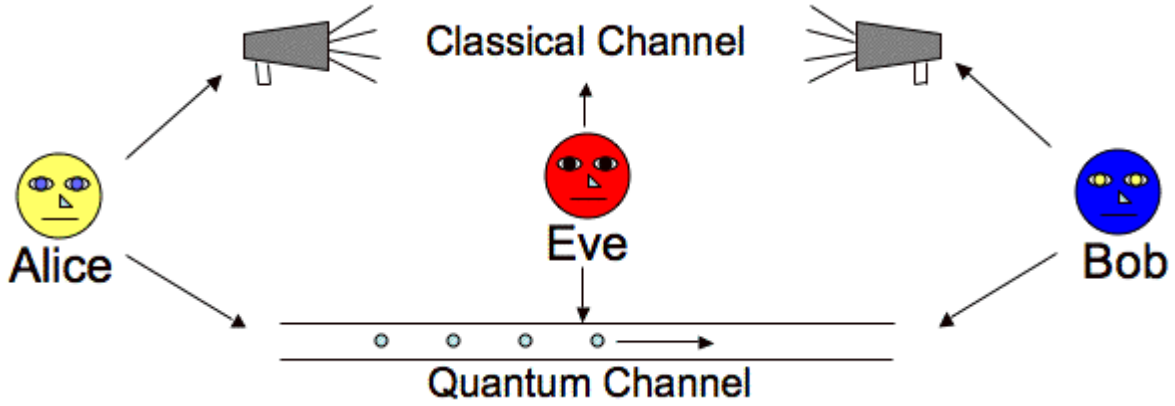
Performance of Shor's algorithm against the best classical factorizing algorithm
Press enter or click to view image in full size



Performance of Shor's algorithm against the best classical factorizing algorithm

Quantum Cryptography

In contrast to classical cryptography, quantum key distribution and other protocols use quantum mechanics principles to provide an unconditionally secured public-key cryptosystem. These protocols can even detect the presence of an eavesdropper in the system who is attempting to learn the key.



Basic QKD Model. Image by Mart Haitjema.

The basic model of QKD consists of two parties, referred to as Alice and Bob, having access to both a quantum communication channel (which is private) that involves sharing a secret key by exchanging quantum particles and a classical communication channel (which is public) that involves basis reconciliation, error correction, and privacy amplification protocols. We assume that an eavesdropper, called Eve, can access both channels.

1. Heisenberg's Uncertainty Principle: This principle states that in a quantum system, only one property of a pair of conjugate properties like position and momentum can be known with certainty (a plausible measurement of a particle's position will disturb its speed). Quantum cryptography takes advantage of this by using the polarization of photons (as photons can be exchanged over fiber optic links) on different bases as the conjugate properties.

2. No Cloning Theorem: Indirectly following the last principle states that it is impossible to create identical copies of an unknown quantum state. Due to this, it is possible to find out if someone interrupted the quantum channel during the vital transmission.

3. Quantum Entanglement: Regardless of the distance, two quantum particles can entangle. When a particular property is measured in a particle, a correlated state of the property will appear on the other particle. Quantum teleportation uses entanglement for communication via a classical information channel. Entangled states are used as the basis of **Eckert's protocol**, which we will talk about later.



Fictional representation of entanglement

The BB84 Protocol

In 1984, Charles Bennett and Gilles Brassard published a protocol based on Heisenberg's uncertainty principle. The protocol is named BB84 after the authors' names and the year it was published. It is one of the most prominent quantum protocols. All the other protocols based on HUP are considered variants of BB84.

In the BB84 protocol, Alice can transmit a random secret key to Bob by sending a string of photons with the private key encoded in their polarization. The no-cloning theorem guarantees that Eve cannot measure these photons and transmit them to Bob without disturbing the photon's state in a detectable way.

The above is true, considering no error on the quantum channel. If the track is prone to error, Alice and Bob will not detect Eve's presence all the time.

Photons as Qubits

Photons have quantum properties and can be transmitted through fiber optics and, therefore, can be used to encode the secret key. Let's discuss how photons act as qubits and how we can operate them.

Photons are qubits for their state of polarization. Now, what is polarization? Before that, we must know what a lightwave is? A light wave is an electromagnetic wave where the plane occupied by the electric

field is perpendicular to the plane occupied by the magnetic field. And the direction of propagation of the wave is orthogonal to these two planes.

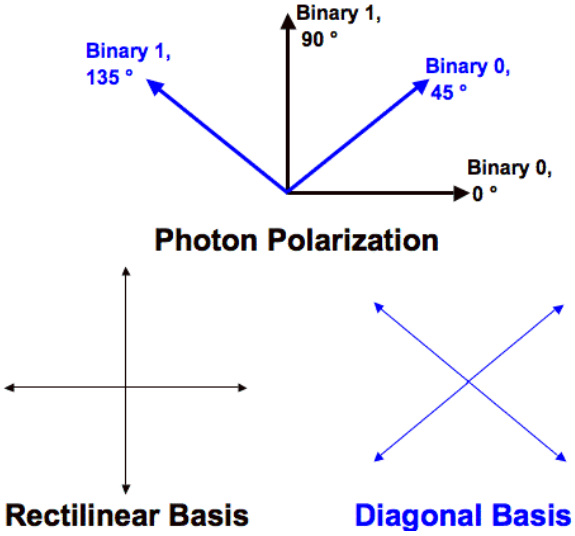
When a light wave is polarized, it oscillates on a single plane. We can use polarizers and wave plates like half-wave plates and quarter-wave plates to polarize light.

There are two types of polarization: **linear** and **elliptical**. We don't need to know about elliptical polarization here. Linear polarization has two states: **rectilinear** and **diagonal**. Again Rectilinear polarization is of two types: **horizontal** and **vertical.** And Diagonal polarization is also of two kinds: **diagonal** and **anti-diagonal.**

It is pretty easy to see that we have a two-level system in photon polarization. Thus, we can use one as $|0\rangle$ and another as $|1\rangle$. The two states of rectilinear polarization, horizontal and vertical, are represented as $|H\rangle$ and $|V\rangle$. The two states of diagonal polarization, diagonal and anti-diagonal, are described as $|D\rangle$ and $|A\rangle$. Now, we can consider $|H\rangle$ and $|V\rangle$ as $|0\rangle$ and $|1\rangle$ on the **Z-axis** and $|D\rangle$ and $|A\rangle$ as $|+\rangle$ and $|-\rangle$ along the **X-axis**.

Back to BB84

For the BB84 protocol, we define polarization of 0° on the rectilinear basis or 45° on the diagonal basis as binary 0. Similarly, a binary 1 can be 90° on a rectilinear basis and 135° on a diagonal basis.



Bits are encoded in the polarization state of a photon. In the first step, Alice and Bob communicate over a Quantum Channel. Alice randomly selects a string of bits and a string of bases (rectilinear or diagonal) of equal length. Then she transmits a photon for each bit with the corresponding polarization through an optical fiber (or other channels that allows sending photons) to Bob.

Bob randomly chooses a basis for each photon to measure its polarization. If Bob selects the same basis as Alice for a particular photon, he will correctly find the bit Alice wanted to share as he measured the same polarization. If he doesn't guess correctly, he will get a random bit.

Alice and Bob communicate over a classical public channel in the second step. Bob tells Alice the bases he used to measure each photon. Alice informs Bob of the bases he guessed correctly to measure the encoded bits. After that, Alice and Bob remove the encoded and measured bits on different bases. Now, Alice and Bob have an identical bit-string, the **shifted key**.

Alice's bit-string	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	+	×	×	+	×	+	+	+	+	+
Alice's polarization	V	D	D	V	A	H	H	H	H	H
Bob's measurement basis	+	+	×	+	+	×	+	+	+	×
Bob's polarization	V	V	D	V	H	A	H	H	H	D
Shifted Key	1	1	1	1	0	1	0	0	0	0

BB84 protocol up to this point

To check the presence of Eve, Alice and Bob can share a few bits from the shifted key, which are supposed to be the same. Any disagreement in the compared bits will expose the presence of Eve. Let's look at an example where Eve managed to intercept some of the photons used in the quantum channel.

Alice's bit-string	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	+	×	×	+	×	+	+	+	+	+
Alice's polarization	V	D	D	V	A	H	H	H	H	H
Eve's measurement basis	×	×	+	×	+	+	×	+	×	+
Eve's polarization	D	D	V	A	V	H	D	H	A	V
Bob's measurement basis	+	+	×	+	+	×	+	+	+	×
Bob's polarization	H	H	A	H	V	D	H	H	V	D
Shifted Key	0	1	1	0	1	0	0	0	1	0

BB84 protocol when Eve interferes with some photons

Due to the presence of Eve, despite having six identical bases, only one of Alice's and Bob's bits match. Which revealed the presence of Eve in the channel. In this case, Alice and Bob will have to transmit the photons again using another Quantum Channel.

Eve's Escape Probability

Eve has no way to know the bases Alice used to encode the bits before Alice reveals her coding bases in the classical channel. So, Eve needs to guess the bases to measure the photons. If she measures incorrectly, information encoded on the other bases will be lost. Again Eve cannot replicate the states of the intercepted photons before sending them to Bob. Based on probability, if Eve eavesdrops on **n** bits, she will go undetected **(3/4)^n** times. In our case of 10 bits, Eve's escape probability is 0.0563, which is very small.

BB84 Protocol Variants

SSP99 Protocol: The six-state protocol was proposed by Pasquinucci and Gisin in 1999. Instead of two orthogonal bases, it uses six orthogonal bases to encode the bits, which results in a lower escape probability for Eve.

Eckert91 Protocol: Eckert used a single photon source in this protocol that produces entangled photons. One of the photons from each entangled pair goes to Alice and the other one to Bob. Alice and Bob randomly select bases to measure the photons. They will get correlated results for each measurement, where they chose the same basis. After removing the photons measured on different bases, they will have a bit-string binary correlated to each other. Knowing if the entangled states were inversely or directly related, Alice and Bob can convert their key to the shifted key. They can measure a photon (they measured on a different basis) on a third basis, and with that result, they can test Bell's Inequality to check Eve's presence. If the inequality contains, someone may have eavesdropped on the quantum channel.

B92 Protocol: In 1992, Charles Bennett developed a simplified version of the BB84 protocol where only two states are used in encoding bits in photons. Binary 0 is encoded as 0° on a rectilinear basis, and binary 1 as 45° on a diagonal basis. Here the bits themselves dictate the bases Alice must choose to encode them. Bob still selects bases randomly to measure the polarized photons. If he chooses the wrong basis, he will not get any measurement this time.

Weaknesses of Quantum Cryptography

Quantum cryptography is unconditionally secured because no assumptions are made about Eve's inability to compute complex mathematical problems but rather about her failure to violate the principles of quantum mechanics. However, these protocols are vulnerable to a man-in-the-middle attack where Eve pretends to be Bob or Alice. The man-in-the-middle attack cannot prevent such attacks without Alice and Bob authenticating each other first. Moreover, quantum cryptography is not perfectly secured when used with faulty equipment and in a noisy environment (which may lead to bit-flip, phase errors, or measurement errors). In an error-prone quantum channel, i**nformation reconciliation** and **privacy amplification** can be used to develop a secured key.

Information reconciliation is carried out in the classical channel to ensure both the shifted keys are identical. It is conducted so Eve cannot intercept much information about each key. The most common protocol used for information reconciliation is the **cascade protocol** which operates in several rounds. During each round, both the keys are divided into small blocks, and **parities** of those blocks are compared. If there is any difference in inequality, a **binary search** is performed to find and correct the error.

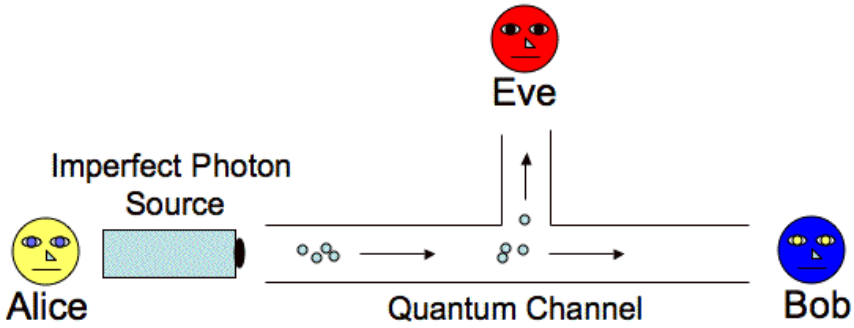
If the parity of a former round was correct but had an error, the error can be found in the next round and can be corrected as before. And the whole process is repeated recursively. After one round, Alice and Bob again reorder their key and start another round. After multiple rounds, Alice and Bob get an identical key with high probability.

Privacy amplification is followed by information reconciliation, where the partial information about the key that Eve might have collected from the quantum or the classical channel is reduced. In Privacy amplification, a shorter key is produced using Alice and Bob's key so that Eve has negligible information about the new key. Privacy amplification uses a publicly known set of functions that take the old key as input and outputs a new key of short length. The shortening of the new key depends on how much information Eve has gained about the old key.

Due to hardware limitations, we cannot implement the protocol perfectly. In a natural system, as we cannot produce and detect single photons properly, we often use a laser to make a small amount of coherent light, which creates the chance of a PNS (Photon Number Splitting) attack where Eve splits off a small number of photons from each bit-transmission for measurement and allows the rest to pass on to Bob. PNS attacks let Eve measure the photons without disturbing Bob's photon measurement.

To prevent this, we use the **decoy-state technique.** Here, Alice transmits each qubit using a random intensity. After transmission, Alice announces publicly the intensity level she used to send each qubit.

A PNS attack will reduce the power of the qubits at Bob's end. Bob can detect the PNS attack by monitoring the **bit error rate** associated with each intensity level.



PNS attack depiction.

Post-quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC), also known as Quantum Safe Cryptography (QSC), refers to cryptographic algorithms designed to withstand attacks by quantum computers.

Quantum computers will eventually become powerful enough to break public key-based cryptography, also known as asymmetric cryptography. Public key-based cryptography is used to protect everything from your online communications to your financial transactions.

Quantum computing represents a major security threat and action is needed now to secure applications and infrastructure using Post-Quantum/Quantum Safe Cryptography.

This blog explains everything you need to know about the new algorithms designed to protect against quantum computer attacks.

What is quantum computing?

Quantum computing utilizes quantum mechanics to solve certain classes of complex problems faster than is possible on classic computers. Problems that currently take the most powerful supercomputer several years could potentially be solved in days.

As such, quantum computers have the potential to deliver the computational power that could take applications like AI to a whole new level. Powerful quantum computers will become a reality in the not-so-distant future, and while they offer many benefits, they also present a major security threat.

Why are quantum computers a security threat?

Once sufficiently powerful quantum computers exist, traditional asymmetric cryptographic methods for key exchange and digital signatures will be broken. Leveraging Shor's algorithm, quantum computers will be capable of reducing the security of discrete logarithm-based schemes like Elliptic Curve Cryptography (ECC) and factorization-based schemes like RSA (Rivest-Shamir-Adleman) so much that no reasonable key size would suffice to keep data secure. ECC and RSA are the algorithms used to protect everything from our bank accounts to our medical records.

Governments, researchers, and tech leaders the world over have recognized this quantum threat and the difficulty in securing critical infrastructure against attacks from quantum computers.

"A quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world.

When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, May 2022

What is Post-Quantum Cryptography (PQC)?

New digital signatures and key encapsulation mechanisms (KEMs) are needed to protect data and hardware from quantum attacks. Many initiatives have been launched throughout the world to develop and deploy new cryptographic algorithms that can replace RSA and ECC while being highly resistant to both classic and quantum attacks. Post-Quantum Cryptography (PQC) refers to these cryptographic algorithms designed to withstand attacks by quantum computers.

Is Quantum Safe Cryptography the same as Post-Quantum Cryptography (PQC)?

Yes, Quantum Safe Cryptography is another term for Post-Quantum Cryptography. Both refer to cryptographic algorithms designed to withstand attacks by quantum computers. Other terms that you may come across include Quantum Proof Cryptography or Quantum Resistant Cryptography.

Why do we need to act now if quantum computers are still a way off?

While quantum computers powerful enough to break public key encryption may still be a way off, data harvesting is happening now. Malicious actors are already said to be collecting encrypted data and

storing it for the time when future quantum computers will be capable of breaking our current encryption methods. This is known as a "harvest now, decrypt later" strategy.

Further because the shelf life of confidential or private information can span years or decades, there is a rapidly growing need to protect such data today to future proof it from quantum attack. Additionally, for many devices such as chips, the development cycle is a long one. Given that it can take years for security testing, certification and then deployment into the existing infrastructure, the earlier the transition to Quantum Safe Cryptography begins, the better.

What progress has been made to develop new PQC algorithms?

The biggest public initiative to develop and standardize new PQC algorithms was launched by The U.S. Department of Commerce's National Institute of Standards and Technology (NIST). International teams of cryptographers submitted algorithm proposals, reviewed the proposals, broke some, and gained confidence in the security of others.

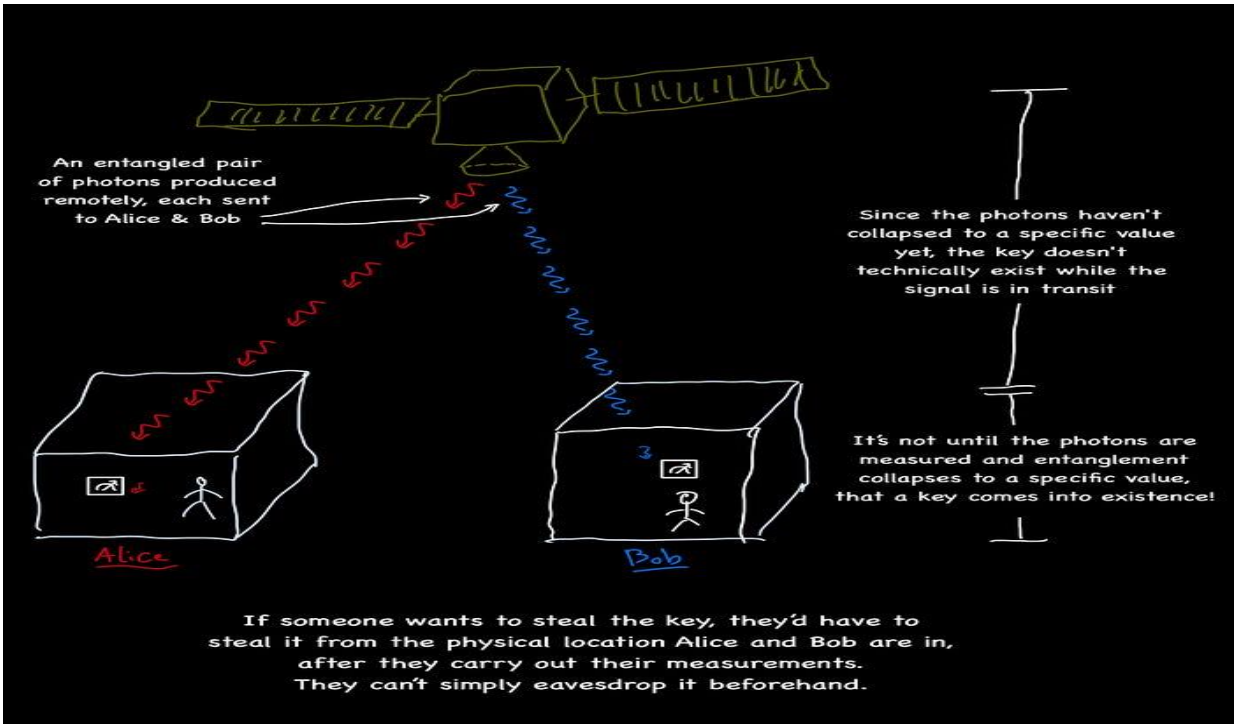
After multiple rounds of evaluations, on July 5th, 2022, NIST announced the first PQC algorithms selected for standardization. CRYSTALS-Kyber was selected as a Key Encapsulation Mechanism (KEM) and CRYSTALS-Dilithium, FALCON, and SPHINCS+ were selected as digital signature algorithms.

Quantum Key Distribution — E91 protocol

The E-91 protocol for Quantum Key Distribution, describes how to securely distribute an encryption key while taking advantage of quantum properties to prevent eavesdropping.

The key can then be used to encrypt and decrypt messages using classical encryption algorithms.

This protocol is known as E-91, after physicist Artur Ekert who proposed it in 1991.



This protocol does not require a Quantum Computer, all that's needed is a photon emitter and receiver. There's no need to run qubits through logic gates of any sort.

It distribute a key to two remote parties, while guaranteeing no eavesdropping during transmission.

At **the heart of this protocol** is the knowledge gained from **Bell's inequality.** Which proved that measuring the states of two entangled particles differs from measuring the states of two independent (separable) particles.

Bell's inequality states if the photons measured by both parties are still entangled at time of measurement.

The steps can be broken down into the following parts:

1. **Transmission:** Send a bunch of entangled pair of photons to two parties, let's name them Alice and Bob.
2. **Measurement:** Each party measures its photon using one of three polarizers (either a vertical, a horizontal or a diagonal one), while randomly and independently changing which polarizer to use for each photon. Through chance, in some cases they'd choose the same orientation and in other cases they won't.
   — **NOTE:** Because the particles are entangled, when Alice and Bob use the same polarizer orientation to measure a pair of photons, they are guaranteed to get the exact result.

3. **Comparison:** The two parties communicate over open classical channel (open, meaning unsecured and an eavesdropper can listen in) to check the value of their measurements, without giving it away, and a key is thus generated. This check looks as follows:
   — Alice and Bob will go through the list of photons they've received and share how they measured them one by one.
   — At **NO POINT** will they mention the value of their measurement, but only state what type of polarizer they used to measure, either a vertical a horizontal or the diagonal one.
   — **They will keep the measurement values for the photons that went through polarizers of the same orientation.** *This will be the key!*

4. **Verification:** Alice and Bob will use the measurement values of the remaining photons, that were measured through different polarizers, and use the knowledge gained from Bell's inequality to determine if the photons were entangled or not.
   — If they determine that the photons **were not entangled**, then they can assume there was an **eavesdropper** measuring one of the photons before it got to either of them and retransmitting a random photon in its place. In this case, they will discard the key and restart their work from the beginning.
   — If they determine that the photons **were entangled**, then they can confidently know with 100% certainty that there **was no eavesdropper** and no one but them knows the exact composition of the key they just produced.

This key can then be used to encrypt and decrypt messages, and send them over open channels.

Quantum Security Concepts

Quantum computing will break the cryptography that protects nearly everything we do online — from banking transactions to national security communications. The question is no longer whether, but when. And the migration to quantum-resistant cryptography is already the largest cryptographic overhaul in the history of information technology.

Quantum security is the discipline of protecting digital systems, data, and cryptographic infrastructure against threats from quantum computing, while also harnessing quantum technologies for defense.

It encompasses three interconnected domains: defending against quantum attacks through post-quantum cryptography (PQC), using quantum physics itself as a security tool through methods like quantum key distribution (QKD), and securing quantum computing systems from classical threats.

quantum computers will eventually break the public-key cryptography that protects virtually all digital communications, and the migration to quantum-resistant alternatives is a multi-year program that regulators, standards bodies, and major technology vendors are already forcing into action.

The Quantum Threat to Cryptography

The threat is specific and well-understood. A sufficiently powerful quantum computer running Shor's algorithm can break RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange — the three families of public-key cryptography that underpin TLS, digital signatures, VPNs, code signing, PKI, and essentially every secure digital transaction on the planet. This is not speculation. The mathematics has been proven since 1994. What remains uncertain is when a quantum computer capable of executing this attack will exist.

In 2021, the best published estimate for breaking RSA-2048 required approximately 20 million physical qubits. By May 2025, Craig Gidney's updated analysis brought that figure below one million physical qubits — a 20× reduction achieved purely through algorithmic and error correction improvements, not hardware breakthroughs. In early 2026, the Pinnacle architecture proposal pushed the theoretical floor below 100,000 qubits under certain assumptions. And in March 2026, Google's quantum team published research showing that ECC-256 could potentially be broken with fewer than 500,000 superconducting qubits in under nine minutes.

No one has built a machine with anywhere near these capabilities today. The largest gate-based quantum computers operate in the low thousands of physical qubits, with error rates still far above what cryptanalysis requires. But the trajectory is moving in one direction, and the gap is closing faster than most security planners expected even two years ago.

Grover's algorithm poses a separate, less severe quantum threat to symmetric cryptography: it effectively halves key lengths, meaning AES-256 would offer roughly AES-128 equivalent security against a quantum attacker. This is significant but manageable – doubling symmetric key lengths is a well-understood mitigation. The existential threat is to public-key systems, and that is where the urgency lies.

Beyond Encryption: The Full Scope of Quantum Security

Quantum security extends beyond the cryptographic threat. The field also encompasses the security of quantum computing systems themselves. As quantum computers become operational infrastructure — accessible through cloud services, integrated into hybrid classical-quantum workflows, and processing sensitive data — they introduce a new attack surface at the quantum-classical interface that security teams will need to defend.

Quantum sensing presents both opportunities and risks for security. Quantum magnetometers, gravimeters, and timing systems have applications in defense, navigation, and surveillance that fall outside traditional cybersecurity but within the broader security landscape.