

## DEFINITION

# quantum key distribution (QKD)

Posted by: [Margaret Rouse](#) [WhatIs.com](#)



Contributor(s): [Alexander Gillis](#) and Kris Gabor

Quantum key distribution (QKD) is a secure communication method for exchanging encryption keys only known between shared parties. The communication method uses properties found in quantum physics to exchange cryptographic keys in such a way that is provable and guarantees security. QKD is a form of [quantum cryptography](#).

This process enables two parties to produce and share a key that is then used to [encrypt](#) and decrypt messages. Specifically, QKD is the method of distributing the key -- not the key itself or the messages it can enable users to send.

Key distribution on a conventional scale relies on [public key](#) cyphers that use complicated mathematical calculations and, therefore, require a prohibitive amount of processing power to break. The viability of public key ciphers, however, faces several issues, such as the constant implementation of new strategies used to attack these systems, weak random number generators and general advances in computing power. In addition, [quantum computing](#) will make much of today's public key encryption strategies unsafe and out of date.

QKD works on a scale much different from conventional key distribution in that QKD uses a quantum system that relies on basic and fundamental laws of nature to protect the data, rather than relying on mathematics. As an example, the no-cloning theorem states that it is impossible to create identical copies of an unknown quantum state, which prevents attackers from simply copying the data in the same manner that they can copy network traffic today. Additionally, if an attacker disturbs or looks at the system, the system will change in such a way that the intended parties involved will know. This is a process that is not vulnerable to increased processing power.

## How does QKD work?

QKD works by transmitting many light particles, or photons, over fiber optic cables between parties. Each photon has a random quantum state, and collectively, the photons sent make up a stream of ones and zeros. This stream of quantum states that make up ones and zeros are called [qubits](#) -- the equivalent of bits in a [binary](#) system. When a photon reaches its receiving end, it'll travel through a beam splitter, which forces the photon to randomly take one path or another into a photon collector. The receiver will then respond to the original sender with data regarding the sequence of the photons sent, and the sender will then compare that with the emitter, which would

have sent each photon. Photons in the wrong beam collector are discarded, and what's left is a specific sequence of bits. This bit sequence can then be used as a key to encrypt data. Any errors and data leakage are removed during a phase of error correction and other post-processing steps. Delayed privacy amplification is another post-processing step that removes any information an eavesdropper might have gained about the final secret key.

There are many different types of QKD, but two main categories are prepare-and-measure protocols and [entanglement](#)-based protocols. Prepare-and-measure protocols focus on measuring unknown quantum states. This type of protocol can be used to detect eavesdropping, as well as how much data was potentially intercepted. Entanglement-based protocols focus around quantum states in which two objects are linked together, forming a combined quantum state. The concept of entanglement means that measurement of one object thereby affects the other. In this method, if an eavesdropper accesses a previously trusted node and changes something, the other involved parties will know.

By implementing quantum entanglement or quantum [superpositions](#), just the process of trying to observe the photons will change the system, making an intrusion detectable.

Other more specific types of QKD include discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD). DV-QKD will encode quantum information in variables using a photon detector to measure quantum states. An example of a DV-QKD protocol is the BB84 protocol. CV-QKD encodes quantum information on the amplitude and phase quadrants of a laser, sending the light to a receiver. The Silberhorn protocol uses this method.

Some examples of QKD protocols are the following:

- BB84
- Silberhorn
- Decoy state
- KMB09
- E91

## Challenges of QKD

Primarily, there are three prevailing challenges to QKD: the integration of QKD systems into current infrastructure, the distance in which photons can travel and the use of QKD in the first place. For now, it is currently difficult to implement an ideal infrastructure for QKD. QKD is perfectly secure in theory, but in practice, imperfections in tools like single photon detectors create many security vulnerabilities. It is important to keep security analysis in mind.

Modern fiber optic cables are typically limited in how far they can carry a photon. Commonly, this range is seen to be upward of 100 km. Some groups and organizations have managed to increase this range for the implementation of QKD. For example, the University of Geneva and Corning Inc. worked together to construct a system capable of carrying a photon 307 km under ideal conditions.

In addition, Quantum Xchange launched Phio, a QKD network in the U.S. capable of delivering quantum keys an apparent unlimited distance using a patent-pending, out-of-band delivery system called Phio Trusted Xchange.

One of the main challenges of QKD is that it relies on already having a classically authenticated channel of communications established. This means that one of the participating users has probably already exchanged a symmetric key in the first place, creating a sufficient level of security. A system can already be made sufficiently secure without QKD through using another advanced encryption standard. However, as the use of quantum computers becomes more frequent, the possibility that an attacker could utilize quantum computing's ability to crack into current encryption methods rises -- making QKD more relevant.

## Implementation

QKD has been worked on and implemented for a relatively long period of time. Some examples of where QKD has been implemented are the following:

- In 2007, Los Alamos National Laboratory and the National Institute of Standards and Technology (NIST) used the BB84 protocol over a 148.7 km optical fiber.
- In 2005, University of Geneva and Corning Inc. used a fiber optic wire of 307 km.
- University of Cambridge and Toshiba collaborated in making a high-bit-rate QKD system using the BB84 protocol.
- Peking University and Beijing University of Posts and Telecommunications collaborated on creating a QKD system.
- In 2017, University of Science and Technology of China measured entangled photons over 1,203 km.
- China and the Institute for Quantum Optics and Quantum Information (IQOQI) in Vienna



SearchSecurity



multiple entities, such as Boston University, Harvard University and IBM Research.

- In 2018, Quantum Xchange launched the first quantum network in the U.S., offering 1,000 km of fiber optic cable and 19 colocation centers along the Boston-to-Washington, D.C., corridor and metro hubs.
- To make QKD systems easier to deploy, the European Telecommunications Standards Institute (ETSI) released a standard in February 2019 that provides a standard interface for devices and applications to receive quantum keys.

Commercial companies, such as ID Quantique, Toshiba, QuintessenceLabs and MagiQ Technologies Inc., have also started offering commercial QKD systems. In addition, Tokyo is beginning to test its own QKD network.

## QKD attack methods

Even though QKD is seen to be completely secure in theory, imperfect implementations of QKD open the potential to compromise security. Techniques for breaching QKD systems have been

discovered in real-life applications because of these imperfections. For example, even though the BB84 protocol should be secure, there is currently no way to implement it perfectly.

The phase remapping attack was devised to create a backdoor that an eavesdropper could enter. The attack takes advantage of the fact that one party member must allow signals to enter and exit its device. This process takes advantage of methods used widely in many commercial QKD systems.

Another attack method is the photon number splitting attack. In an ideal setting, one user should be able to send one photon at a time to the other user. However, most of the time, additional similar photons are sent at once. These photons could be intercepted without either party knowing. The photon number splitting attack takes advantage of this.

To combat this type of attack, an improvement to the BB84 protocol was later implemented -- called *decoy state QKD* -- which uses a set of decoy signals mixed in with the intended BB84 signal while enabling both parties the ability to detect if an eavesdropper is listening in.

## History of QKD

QKD got its start with the first proposal of quantum cryptography in the 1970s when Stephen Wiesner at Columbia University came up with the idea of quantum conjugate coding. Wiesner's paper was published in 1983. Years later, Charles H. Bennett introduced a concept of secure communication, basing his ideas on Wiesner's work. Bennett also came up with BB84 -- the first quantum cryptography protocol -- which worked using nonorthogonal states. Moreover, it was in 1990 that Artur Ekert discovered another method to QKD, basing his idea around quantum entanglement.

## Future of QKD

The Quantum-Safe Security Working Group (QSSWG) was formed in the Cloud Security Alliance ([CSA](#)) in order to promote the adoption of new technologies that would help quantum computing be adopted at a steady pace. As more time passes, new technology is being worked on to improve high data rates and increase the overall effective distance of QKD. QKD is beginning to be used more widely in a commercial sense, with new networks and companies offering commercial QKD systems.

[Margaret Rouse](#) asks:

**What do you think the future of QKD holds?**



[Join the Discussion](#)

---

This was last updated in January 2020

## Continue Reading About quantum key distribution (QKD)

- [The next stage in quantum key distribution](#)
- [Quantum key distribution is the future for secure comms](#)
- [Accenture Labs explores quantum computing applications](#)
- [Free-space optical quantum key distribution systems: challenges and trends](#)
- [Quantum key distribution \(QKD\)](#)


## Related Terms

---


### Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified ... [See complete definition](#) 

### cryptography

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the ... [See complete definition](#) 

### encryption

Encryption is the method by which information is converted into secret code that hides the information's true meaning. [See complete definition](#) 

---

## Dig Deeper on Disk and file encryption tools

### 3 ways to use quantum technology features in your enterprise

By: David Petersson

#### Singtel and NUS claim quantum breakthrough

By: Aaron Tan

#### BT switches on quantum network link at Adastral Park

By: Alex Scroxton

#### Trusted nodes: The next generation in quantum key distribution

By: Peter Allison

 **Join the conversation**

 **1 comment**

Share your comment

☒ Send me notifications when other members comment.

Add My Comment

Oldest ▼

[] **Margaret Rouse**



- 23 Jan 2020 3:12 PM

What do you think the future of QKD holds?

Reply

[CLOUD SECURITY](#) [NETWORKING](#) [CIO](#) [ENTERPRISE DESKTOP](#) [CLOUD COMPUTING](#) [COMPUTER WEEKLY](#)



Search**CloudSecurity**

## Choosing between proxy vs. API CASB deployment modes

Curious how to choose the right CASB deployment mode for your organization? Before you buy, compare how proxy vs. API CASB ...

---

## How to use the Mitre ATT&CK framework for cloud security

Learn how to use the Mitre ATT&CK security framework to keep your enterprise cloud environment -- whether AWS, GCP, Azure, Azure ...

[About Us](#) [Meet The Editors](#) [Contact Us](#) [Videos](#) [Photo Stories](#) [Definitions](#)

[Guides](#) [Advertisers](#) [Business Partners](#) [Media Kit](#) [Corporate Site](#)

[Contributors](#) [CPE and CISSP Training](#) [Reprints](#) [Events](#) [E-Products](#)

All Rights Reserved,  
Copyright 2000 - 2020, TechTarget

[Privacy Policy](#)

[Do Not Sell My Personal Info](#)