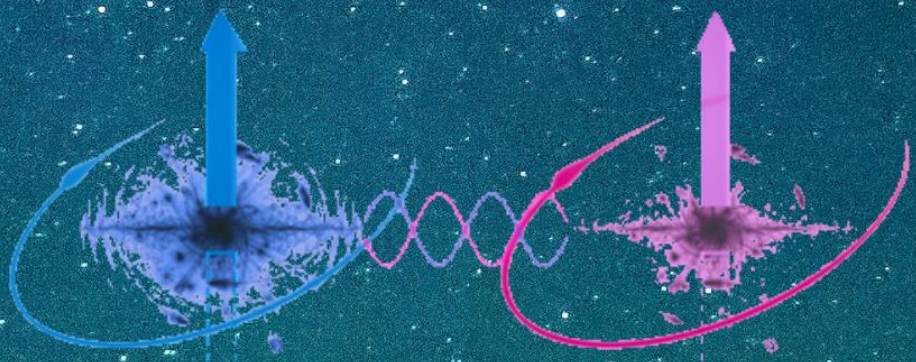
DIPL.ING.(FH)KLAUS ROCK

# HTTP-QuSS

## HTTP - QUANTUM SPEED AND SECURITY

February 14, 2022

## QUBIT DATA TRANSMISSION INTEGRATION



$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

ROCK TECHNOLOGIES
Bonhoefferstr. 37 | 73432 Aalen | Germany | +49-7367-9222-958

# Table of Contents

# 1.0 Introduction to Quantum Internet (QNet)

## 1.1 How Close we are to the Future of Qubit Data Transmission?

We could expect the quantum internet based upon laser driven GEO, MEO and LEO Satellites to be among us by 2026. Maybe it was the excitement surrounding the launch of a Chinese quantum satellite, which happened 2019. But why could we understand that claim as "bold"? Is it impossible for the quantum internet, often seen as the future of our communications, to be massively adopted 5 years from today?

We do not know that much about quantum communications, let alone a quantum internet. Experts are still figuring out some of the basic aspects surrounding it, from how to better transmit quantum data to how to store it. So, predicting this outcome for such a relatively short time is kind of bold.

## 1.2 What Is The Quantum Internet?

This seems like a simple question, doesn't it? However, the answer could be more complex than you think. As Ronald Hanson, an experimental physicist working on the subject with a team from the Delft University of Technology in the Netherlands, puts it: "People talk about quantum networks to mean vastly different things."

That should give you an idea of how chaotic the development surrounding the quantum internet is right now — there is no agreement even in the terms and concepts used to build it! But there are certain things that can be said to somewhat understand what we mean by quantum internet. First, it is important to discern what a quantum network is.

As with any network, a quantum network implies the interconnection of several nodes (devices or computers) that exchange quantum information instead of classic data. So, the second thing needed to understand the quantum internet is knowing what quantum information actually is

The current model to transmit information between our computers uses a binary system comprised of 0s and 1s. The chain of those numbers is what constitutes the information that is being exchanged. Quantum information, for its part, relies on quantum mechanics to transmit data. By using quantum bits (or qubits) as information units, this model can superpose a 0 and a 1 in the same unit.

Though that seems rather odd and impossible, current experiments are using qubits to encode classical information in what is called **q**uantum **k**ey **d**istribution (**QKD**). This is the most basic use of qubits for data transmission. The next step would imply the transfer of quantum states directly between the nodes through a property of quantum systems called entanglement.

When two particles of a quantum system interact, they can get entangled. Once that happens, both particles can be described with a single quantum state. In other words, any measurement applied to a particle instantly alters the state of the other particle, even when they are kilometers apart. So, instead of exchanging measurements and how to read them (as it happens with QKD), a quantum network could exchange quantum states between its nodes.

Of course, a quantum network is not the quantum internet. For that to happen, it would take something else for any two users connected to a wide network to be able to store and exchange qubits. We're a long way from having that, though: There still aren't networks connecting quantum processors (which will turn those networks into a quantum internet), nor are there quantum repeaters outside a lab (which will extend the limited range of qubit transmission).

## Why Would Anyone Care If We Get There?

Quantum internet could change a lot of things. In its earliest stages, it can provide a safer environment for data transmission since it could be impossible to decipher which state a series of qubits is without any entanglement. Additionally, quantum computers could serve for scientific research, from the measurement of gravitational waves to the sharpening of images taken by distant optical telescopes.

On a general level, a quantum internet could be the answer to tasks that call for coordination, synchronization, and privacy at their highest levels. Thus, this kind of internet could be the solution for one of the biggest issues we face in our digital age — the security of our data. That is not all. The possibilities of a quantum internet could change a lot of things, including how we communicate and even how we vote.

## 1.3 How Far Are We from A Quantum Internet?

There are four steps before we get to a quantum internet:

1. **Trusted-Node Network**

   This could also be considered step No. 0, as nothing truly "quantum-like" happens during transmission. In this step, users only use quantum-generated codes whose encryption key must be shared (even by the service provider).

2. **Prepare and Measure**

   Users can send and measure quantum states, but there is no entanglement. Users can share a private encryption key that no one else knows.

3. **Entanglement Distribution Networks**

   Users can entangle qubit states but not store them.
   Possible already with Laser based GEO, MEO and LEO Satellites by entangled Photon Channels.

4. **Quantum Memory Networks**

   Quantum information can be transmitted and stored through entanglement.
   Possible shortly with **HTTP-QuSS QNet** Supercomputer Architecture and Single Stream Technology.

So, you can see where we are standing, right at the second step (prepare and measure) in this road map. The Chinese satellite launched in 2017 is the best effort to date for this kind of transmission, as it was able to link two laboratories separated by more than 1,200 kilometers.

Steps **3** and **4** we can reach within the next 5 Years with the Introduction of the **HTTP-QuSS** respectively **QNet** Technology.

# 2.0 Quantum Network

Quantum networks form an important element of quantum computing and quantum communication systems. Quantum networks facilitate the transmission of information in the form of quantum bits, also called qubits, between physically separated quantum processors. A quantum processor is a small quantum computer being able to perform quantum logic gates on a certain number of qubits. Quantum networks work in a similar way to classical networks. The main difference is that quantum networking, like quantum computing, is better at solving certain problems, such as modelling quantum systems.

## 2.1 Quantum Networks for Computation

Networked quantum computing or distributed quantum computing works by linking multiple quantum processors through a quantum network by sending qubits in-between them. Doing this creates a quantum computing cluster and therefore creates more computing potential. Less powerful computers can be linked in this way to create one more powerful processor. This is analogous to connecting several classical computers to form a computer cluster in classical computing. Like classical computing this system is scale-able by adding more and more quantum computers to the network. Currently quantum processors are only separated by short distances

## 2.2 Quantum Networks for Communication

In the realm of quantum communication, one wants to send qubits from one quantum processor to another over long distances. This way local quantum networks can be intra connected into a quantum internet. A quantum internet supports many applications, which derive their power from the fact that by creating quantum entangled qubits, information can be transmitted between the remote quantum processors. Most applications of a quantum internet require only very modest quantum processors. For most quantum internet protocols, such as quantum key distribution in quantum cryptography, it is sufficient if these processors can prepare and measuring only a single qubit at a time. This contrasts with quantum computing where interesting applications can only be realized if the (combined) quantum processors can easily simulate more qubits than a classical computer (around 60). Quantum internet applications require only small quantum processors, often just a single qubit, because quantum entanglement can already be realized between just two qubits. A simulation of an entangled quantum system on a classical computer cannot simultaneously provide the same security and speed.

## 2.3 Overview of the Elements of a Quantum Network

The basic structure of a quantum network and more generally a quantum internet is analogous to a classical network. First, we have end nodes on which applications are ultimately run. These end nodes are quantum processors of at least one qubit. Some applications of a quantum internet require quantum processors of several qubits as well as a quantum memory at the end nodes.

Second, to transport qubits from one node to another, we need communication lines. For the purpose of quantum communication, standard telecom fibers can be used. For networked quantum computing, in which quantum processors are linked at short distances, different wavelengths are chosen depending on the exact hardware platform of the quantum processor.

Third, to make maximum use of communication infrastructure, one requires optical switches capable of delivering qubits to the intended quantum processor. These switches need to preserve quantum coherence, which makes them more challenging to realize than standard optical switches.

Finally, one requires a quantum repeater to transport qubits over long distances. Repeaters appear in-between end nodes. Since qubits cannot be copied, classical signal amplification is not possible. By necessity, a quantum repeater works in a fundamentally different way than a classical repeater.

## 2.4 Elements of a Quantum Network

### 2.4.1 End Nodes | Quantum Processors

End nodes can both receive and emit information. Telecommunication lasers and parametric down-conversion combined with photodetectors can be used for quantum key distribution. In this case, the end nodes can in many cases be very simple devices consisting only of beam splitters and photodetectors.

However, for many protocols more sophisticated end nodes are desirable. These systems provide advanced processing capabilities and can also be used as quantum repeaters. Their chief advantage is that they can store and retransmit quantum information without disrupting the underlying quantum state. The quantum state being stored can either be the relative spin of an electron in a magnetic field or the energy state of an electron. They can also perform quantum logic gates.

One way of realizing such end nodes is by using colour centres in diamond, such as the nitrogen-vacancy centre. This system forms a small quantum processor featuring several qubits. NV centres can be utilized at room temperatures. Small scale quantum algorithms and quantum error correction has already been demonstrated in this system, as well as the ability to entangle two remote quantum processors, and perform deterministic quantum teleportation.

Another possible platform are quantum processors based on Ion traps, which utilize radio-frequency magnetic fields and lasers. In a multispecies trapped-ion node network, photons entangled with a parent atom are used to entangle different nodes. Also, cavity quantum electrodynamics (Cavity QED) is one possible method of doing this. In Cavity QED, photonic quantum states can be transferred to and from atomic quantum states stored in single atoms contained in optical cavities. This allows for the transfer of quantum states between single atoms using optical fiber in addition to the creation of remote entanglement between distant atoms.

### 2.4.2 Communication Lines | Physical Layer

Over long distances, the primary method of operating quantum networks is to use optical networks and photon-based qubits. This is due to optical networks having a reduced chance of decoherence. Optical networks have the advantage of being able to re-use existing optical fiber. Alternately, free space networks can be implemented that transmit quantum information through the atmosphere or through a vacuum.

#### 2.4.2.1 Fiber Optic Networks

Optical networks using existing telecommunication fiber can be implemented using hardware like existing telecommunication equipment. This fiber can be either single-mode or multi-mode, with multi-mode allowing for more precise communication. At the sender, a single photon source can be created by heavily attenuating a standard telecommunication laser such that the mean number of photons per pulse is less than 1. For receiving, an avalanche photodetector can be used. Various methods of phase or polarization control can be used such as interferometers and beam splitters. In the case of entanglement-based protocols, entangled photons can be generated through spontaneous parametric down-conversion. In both cases, the telecom fiber can be multiplexed to send non-quantum timing and control signals.

#### 2.4.2.2 Free Space Networks

Free space quantum networks operate like fiber optic networks but rely online of sight between the communicating parties instead of using a fiber optic connection. Free space networks can typically support higher transmission rates than fiber optic networks and do not have to account for polarization scrambling caused by optical fiber. However, over long distances, free space communication is subject to an increased chance of environmental disturbance on the photons.

Importantly, free space communication is also possible from a satellite to the ground. A quantum satellite capable of entanglement distribution over 1,203 km has been demonstrated. The experimental exchange of single photons from a global navigation satellite system at a slant distance of 20,000 km has also been reported. These satellites can play an important role in linking smaller ground-based networks over larger distances.

### 2.4.3 Repeaters

Long distance communication is hindered by the effects of signal loss and decoherence inherent to most transport mediums such as optical fiber. In classical communication, amplifiers can be used to boost the signal during transmission, but **in a quantum network amplifier cannot be used since qubits cannot be copied** – **known as the no-cloning theorem**. That is, to implement an amplifier, the complete state of the flying qubit would need to be determined, something which is **both unwanted and impossible**.

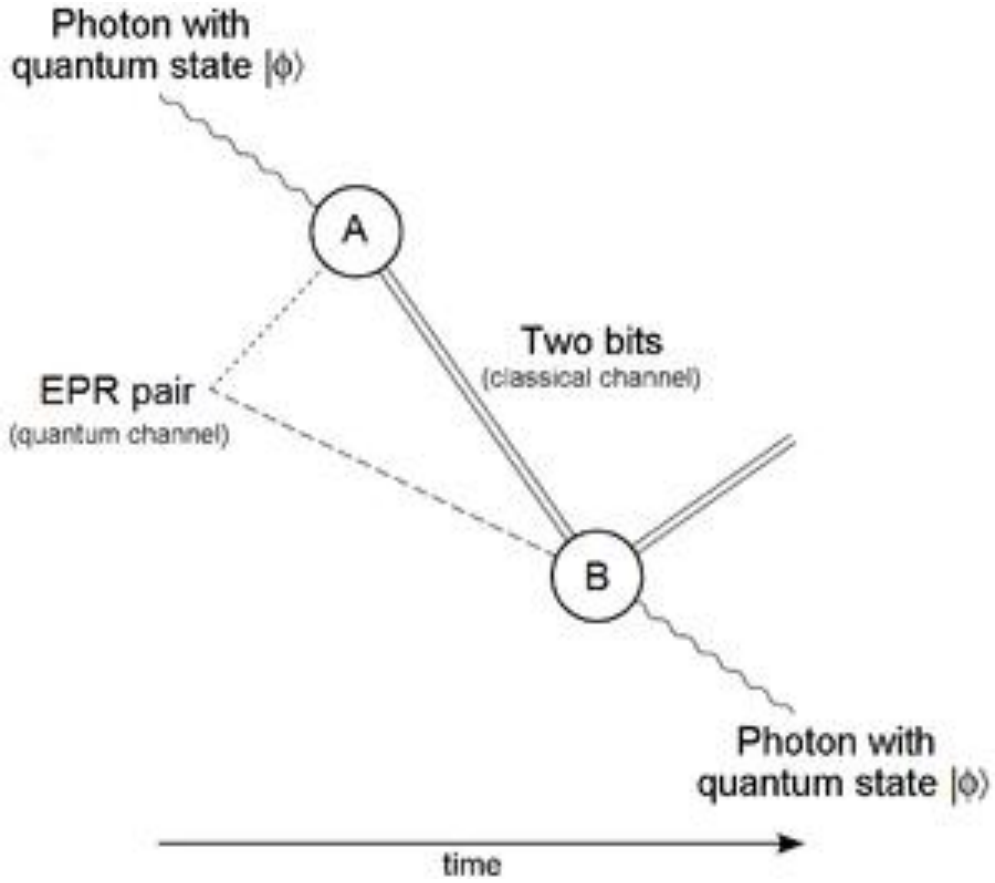
#### 2.4.3.1 Trusted Repeaters

An intermediary step which allows the testing of communication infrastructure are trusted repeaters. Importantly, a trusted repeater cannot be used to transmit qubits over long distances. Instead, a trusted repeater can only be used to perform quantum key distribution with the additional assumption that the repeater is trusted. Consider two end nodes ***A*** and ***B***, and a trusted repeater ***R*** in the middle. ***A*** and ***R*** now perform quantum key distribution to generate a key $k_{AB}$. ***R*** decrypts to obtain $k_{AB}$. ***R*** then re-encrypts $k_{AB}$ using the key $k_{RB}$ and sends it to ***B***. ***B*** decrypts to obtain $k_{AB}$. ***A*** and ***B*** now share the key $k_{AB}$. The key is secure from an outside eavesdropper, but clearly the repeater ***R*** also know $k_{AB}$. This means that any subsequent communication between ***A*** and ***B*** does not provide end to end security, but is only secure if ***A*** and ***B*** trust the repeater ***R***.

### 2.4.3.2 Quantum Repeaters

A true quantum repeater allows the end to end generation of quantum entanglement, and thus - **by using quantum teleportation** - the end to end transmission of qubits. In quantum key distribution protocols one can test for such entanglement. This means that when making encryption keys, the sender and receiver are secure even if they do not trust the quantum repeater. Any other application of a quantum internet also requires the end to end transmission of qubits, and thus a quantum repeater.

Quantum repeaters allow entanglement and can be established at distant nodes without physically sending an entangled qubit the entire distance.




In this case, the quantum network consists of many short distance links of perhaps tens or hundreds of kilometers. In the simplest case of a single repeater, two pairs of entangled qubits are established: $|\boldsymbol{A}\rangle$ and $|\boldsymbol{R_a}\rangle$ located at the sender and the repeater, and a second pair $|\boldsymbol{R_b}\rangle$ and $|\boldsymbol{B}\rangle$ located at the repeater and the receiver. These initial entangled qubits can be easily created, for example through parametric down conversion, with one qubit physically transmitted to an adjacent node. At this point, the repeater can perform a bell measurement on the qubits $|\boldsymbol{R_a}\rangle$ and $|\boldsymbol{R_b}\rangle$ thus teleporting the quantum state of $|\boldsymbol{R_a}\rangle$ to $|\boldsymbol{B}\rangle$. This has the effect of "swapping" the entanglement such that $|\boldsymbol{A}\rangle$ and $|\boldsymbol{B}\rangle$ are now entangled at a distance twice that of the initial entangled pairs. A network of such repeaters can be used linearly or in a hierarchical fashion to establish entanglement over great distances.

Hardware platforms suitable as end nodes above can also function as quantum repeaters. However, there are also hardware platforms specific only to the task of acting as a repeater, without the capabilities of performing quantum gates.

#### 2.4.3.3 Error Correction

Error correction can be used in quantum repeaters. Due to technological limitations, however, the applicability is limited to very short distances as quantum error correction schemes capable of protecting qubits over long distances would require an extremely large number of qubits and hence extremely large quantum computers.

Errors in communication can be broadly classified into two types: Loss errors (due to optical fiber/environment) and operation errors (such as depolarization, dephasing etc.). While redundancy can be used to detect and correct classical errors, redundant qubits cannot be created due to the no-cloning theorem. As a result, other types of error correction must be introduced such as the Shor code or one of several more general and efficient codes. All these codes work by distributing the quantum information across multiple entangled qubits so that operation errors as well as loss errors can be corrected.

In addition to quantum error correction, classical error correction can be employed by quantum networks in special cases such as quantum key distribution. In these cases, the goal of the quantum communication is to securely transmit a string of classical bits. Traditional error correction codes such as Hamming codes can be applied to the bit string before encoding and transmission on the quantum network.

#### 2.4.3.4 Entanglement Purification

Quantum decoherence can occur when one qubit from a maximally entangled bell state is transmitted across a quantum network. Entanglement purification allows for the creation of nearly maximally entangled qubits from many arbitrary weakly entangled qubits, and thus provides additional protection against errors. Entanglement purification (also known as Entanglement distillation) has already been demonstrated in Nitrogen-vacancy centres in diamond.

### 2.4.4 Applications

A quantum internet supports numerous applications, enabled by quantum entanglement. In general, quantum entanglement is well suited for tasks that require coordination, synchronization, or privacy.

Examples of such applications include quantum key distribution, clock synchronization, protocols for distributed system problems such as leader election or byzantine agreement, extending the baseline of telescopes, as well as position verification, secure identification and two-party cryptography in the noisy-storage model. A quantum internet also enables secure access to a quantum computer in the cloud. Specifically, a quantum internet enables very simple quantum devices to connect to a remote quantum computer in such a way that computations can be performed there without the quantum computer finding out what this computation actually is (the input and output quantum states cannot be measured without destroying the computation, but the circuit composition used for the calculation will be known).

#### 2.4.4.1 Secure Communications

When it comes to communicating in any form the largest issue has always been keeping your communications private. From when couriers were used to send letters between ancient battle

commanders to secure radio communications that exist today the main purpose is to ensure that what a sender sends out to the receiver reaches the receiver unmolested. This is an area in which Quantum Networks particularly excel. By applying a quantum operator that the user selects to a system of information the information can then be sent to the receiver without a chance of an eavesdropper being able to accurately be able to record the sent information without either the sender or receiver knowing. This works because if a listener tries to listen in then they will change the information in an unintended way by listening thereby tipping their hand to the people on whom they are attacking. Secondly, without the proper quantum operator to decode the information they will corrupt the sent information without being able to use it themselves.

#### 2.4.4.2 WEB Browsing and common TCP Applications

Integrating our HTTP-QuSS Architecture and Technology as Node Endpoints into quantum Internet consisting of a Supercomputer and SoC Clients even WEB Browsing and common TCP Applications are possible in the near Future.

### 2.4.5 Current Status

#### 2.4.5.1 Quantum Internet

At present, there is no network connecting quantum processors, or quantum repeaters deployed outside a lab.

#### 2.4.5.2 Quantum Key Distribution Networks

Several test networks have been deployed that are tailored to the task of quantum key distribution either at short distances (but connecting many users), or over larger distances by relying on trusted repeaters. These networks do not yet allow for the end to end transmission of qubits or the end to end creation of entanglement between far away nodes.

**Major quantum network projects and QKD protocols implemented**

| Quantum network | Start | BB84 | BBM92 | E91 | DPS | COW |
|---|---|---|---|---|---|---|
| DARPA Quantum Network | 2001 | Yes | No | No | No | No |
| SECOCQ QKD network in Vienna | 2003 | Yes | Yes | No | No | Yes |
| Tokyo QKD network | 2009 | Yes | Yes | No | Yes | No |
| Hierarchical network in Wuhu, China | 2009 | Yes | No | No | No | No |
| Geneva area network (SwissQuantum) | 2010 | Yes | No | No | No | Yes |

#### 2.4.5.2 DARPA Quantum Network

Starting in the early 2000s, DARPA began sponsorship of a quantum network development project with the aim of implementing secure communication. The DARPA Quantum Network became operational within the BBN Technologies laboratory in late 2003 and was expanded further in 2004 to include nodes at Harvard and Boston Universities. The network consists of multiple physical layers including fiber optics supporting phase-modulated lasers and entangled photons as well free-space links.

### 2.4.5.3 SECOQC Vienna QKD Network

From 2003 to 2008 the Secure Communication based on Quantum Cryptography (SECOQC) project developed a collaborative network between a number of European institutions. The architecture chosen for the SECOQC project is a trusted repeater architecture which consists of point-to-point quantum links between devices where long-distance communication is accomplished using repeaters

### 2.4.5.4 Chinese hierarchical Network

In May 2009, a hierarchical quantum network was demonstrated in Wuhu, China. The hierarchical network consists of a backbone network of four nodes connecting a number of subnets. The backbone nodes are connected through an optical switching quantum router. Nodes within each subnet are also connected through an optical switch and are connected to the backbone network through a trusted relay

### 2.4.5.5 Geneva Area Network (SwissQuantum)

The SwissQuantum network developed and tested between 2009 and 2011 linked facilities at CERN with the University of Geneva and hepia in Geneva. The SwissQuantum program focused on transitioning the technologies developed in the SECOQC and other research quantum networks into a production environment. The integration with existing telecommunication networks, and its reliability and robustness

### 2.4.5.6 Tokyo QKD Network

In 2010, several organizations from Japan and the European Union setup and tested the Tokyo QKD network. The Tokyo network build upon existing QKD technologies and adopted a SECOQC like network architecture. For the first time, one-time-pad encryption was implemented at high enough data rates to support popular end-user application such as secure voice and video conferencing. Previous large-scale QKD networks typically used classical encryption algorithms such as AES for high-rate data transfer and use the quantum-derived keys for low rate data or for regularly re-keying the classical encryption algorithms.

### 2.4.5.7 Beijing-Shanghai Trunk Line

In September 2017, a 2000-km quantum key distribution network between Beijing and Shanghai, China, was officially opened. This trunk line will serve as a backbone connecting quantum networks in Beijing, Shanghai, Jinan in Shandong province and Hefei in Anhui province. During the opening ceremony, two employees from the Bank of Communications completed a transaction from Shanghai to Beijing using the network. The State Grid Corporation of China is also developing a managing application for the link. The line uses 32 trusted nodes as repeaters. A quantum telecommunication network has been also put into service in Wuhan, capital of central China's Hubei Province, which will be connected to the trunk. Other similar city quantum networks along the Yangtze River are planned to follow.

## 3.0 Quantum Entanglement

Quantum entanglement is the physical phenomenon that occurs when a pair or group of particles is generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the pair or group cannot be described independently of the state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical and quantum physics: entanglement is a primary feature of quantum mechanics lacking in classical mechanics.

Measurements of physical properties such as position, momentum, spin, and polarization performed on entangled particles are found to be perfectly correlated. For example, if a pair of entangled particles is generated such that their total spin is known to be zero, and one particle is found to have clockwise spin on a first axis, then the spin of the other particle, measured on the same axis, will be found to be counter clockwise. However, this behaviour gives rise to seemingly paradoxical effects: any measurement of a property of a particle results in an irreversible wave function collapse of that particle and will change the original quantum state. In the case of entangled particles, such a measurement will affect the entangled system as a whole.

Such phenomena were the subject of a 1935 paper by Albert Einstein, Boris Podolsky, and Nathan Rosen, and several papers by Erwin Schrödinger shortly, thereafter, describing what came to be known as the EPR paradox. Einstein and others considered such behaviour to be impossible, as it violated the local realism view of causality (Einstein referring to it as "**spooky action at a distance**") and argued that the accepted formulation of quantum mechanics must therefore be incomplete.

Later, however, the counterintuitive predictions of quantum mechanics were verified experimentally in tests in which polarization or spin of entangled particles were measured at separate locations, statistically violating Bell's inequality. In earlier tests it could not be absolutely ruled out that the test result at one point could have been subtly transmitted to the remote point, affecting the outcome at the second location. However so-called "loophole-free" Bell tests have been performed in which the locations were separated such that communications at the speed of light would have taken longer—in one case 10,000 times longer—than the interval between the measurements.

According to some interpretations of quantum mechanics, the effect of one measurement occurs instantly. Other interpretations which do not recognize wavefunction collapse dispute that there is any "effect" at all. However, all interpretations agree that entanglement produces correlation between the measurements and that the mutual information between the entangled particles can be exploited, but that any transmission of information at faster-than-light speeds is impossible.

Quantum entanglement has been demonstrated experimentally with photons, neutrinos, electrons, molecules as large as buckyballs, and even small diamonds. The utilization of entanglement in communication, computation and quantum radar is a very active area of research and development.

## 3.1 History

Article headline regarding the Einstein–Podolsky–Rosen paradox (EPR paradox) paper, in the May 4, 1935 issue of The New York Times.

The counterintuitive predictions of quantum mechanics about strongly correlated systems were first discussed by Albert Einstein in 1935, in a joint paper with Boris Podolsky and Nathan Rosen. In this study, the three formulated the Einstein–Podolsky–Rosen paradox (EPR paradox), a thought experiment that attempted to show that quantum mechanical theory was incomplete. They wrote: "We are thus forced to conclude that the quantum-mechanical description of physical reality given by wave functions is not complete."

However, the three scientists did not coin the word entanglement, nor did they generalize the special properties of the state they considered. Following the EPR paper, Erwin Schrödinger wrote a letter to Einstein in German in which he used the word Verschränkung (translated by himself as entanglement) "to describe the correlations between two particles that interact and then separate, as in the EPR experiment."

Schrödinger shortly thereafter published a seminal paper defining and discussing the notion of "entanglement." In the paper, he recognized the importance of the concept, and stated: "I would not call [entanglement] one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."

Like Einstein, Schrödinger was dissatisfied with the concept of entanglement, because it seemed to violate the speed limit on the transmission of information implicit in the theory of relativity. Einstein later famously derided entanglement as "**spukhafte Fernwirkung**" or "spooky action at a distance."

The EPR paper generated significant interest among physicists, which inspired much discussion about the foundations of quantum mechanics (perhaps most famously Bohm's interpretation of quantum mechanics) but produced relatively little other published work. Despite the interest, the weak point in EPR's argument was not discovered until 1964, when John Stewart Bell proved that one of their key assumptions, the principle of locality, as applied to the kind of hidden variables interpretation hoped for by EPR, was mathematically inconsistent with the predictions of quantum theory.

Specifically, Bell demonstrated an upper limit, seen in Bell's inequality, regarding the strength of correlations that can be produced in any theory obeying local realism, and showed that quantum theory predicts violations of this limit for certain entangled systems. His inequality is experimentally testable, and there have been numerous relevant experiments, starting with the pioneering work of Stuart Freedman and John Clauser in 1972 and Alain Aspect's experiments in 1982. An early experimental breakthrough was due to Carl Kocher, who already in 1967 presented an apparatus in which two photons successively emitted from a calcium atom were shown to be entangled – the first case of entangled visible light. The two photons passed diametrically positioned parallel polarizers with higher probability than classically predicted but with correlations in quantitative agreement with quantum mechanical calculations. He also showed that the correlation varied only upon (as cosine square of) the angle between the polarizer settings and decreased exponentially with time lag between emitted photons. Kocher's apparatus, equipped with better polarizers, was used by Freedman and Clauser who could confirm the cosine square dependence and use it to demonstrate a violation of Bell's inequality for a set of fixed angles. All these experiments have shown agreement with quantum mechanics rather than the principle of local realism.

For decades, each had left open at least one loophole by which it was possible to question the validity of the results. However, in 2015 an experiment was performed that simultaneously closed both the detection and locality loopholes, and was heralded as "loophole-free"; this experiment ruled out a large class of local realism theories with certainty. Alain Aspect notes that the "setting-independence loophole" – which he refers to as "far-fetched", yet, a "residual loophole" that "cannot be ignored" – has yet to be closed, and the free-will / super determinism loophole is unclosable; saying "no experiment, as ideal as it is, can be said to be totally loophole-free."

A minority opinion holds that although quantum mechanics is correct, there is no superluminal instantaneous action-at-a-distance between entangled particles once the particles are separated.

Bell's work raised the possibility of using these super-strong correlations as a resource for communication. It led to the 1984 discovery of quantum key distribution protocols, most famously BB84 by Charles H. Bennett and Gilles Brassard and E91 by Artur Ekert. Although BB84 does not use entanglement, Ekert's protocol uses the violation of a Bell's inequality as a proof of security.

## 3.2 Meaning of Entanglement

An entangled system is defined to be one whose quantum state cannot be factored as a product of states of its local constituents; that is to say, they are not individual particles but are an inseparable whole. In entanglement, one constituent cannot be fully described without considering the other(s). The state of a composite system is always expressible as a sum, or superposition, of products of states of local constituents; it is entangled if this sum necessarily has more than one term.

Quantum systems can become entangled through various types of interactions. For some ways in which entanglement may be achieved for experimental purposes, see the section below on methods. Entanglement is broken when the entangled particles decohere through interaction with the environment; for example, when a measurement is made.

As an example of entanglement: a subatomic particle decays into an entangled pair of other particles. The decay events obey the various conservation laws, and as a result, the measurement outcomes of one daughter particle must be highly correlated with the measurement outcomes of the other daughter particle (so that the total momenta, angular momenta, energy, and so forth remains roughly the same before and after this process). For instance, a spin-zero particle could decay into a pair of spin-½ particles. Since the total spin before and after this decay must be zero (conservation of angular momentum), whenever the first particle is measured to be spin up on some axis, the other, when measured on the same axis, is always found to be spin down. (This is called the spin anti-correlated case; and if the prior probabilities for measuring each spin are equal, the pair is said to be in the singlet state.)

The special property of entanglement can be better observed if we separate the said two particles. Let us put one of them in the White House in Washington and the other in Buckingham Palace (think about this as a thought experiment, not an actual one). Now, if we measure a particular characteristic of one of these particles (say, for example, spin), get a result, and then measure the other particle using the same criterion (spin along the same axis), we find that the result of the measurement of the second particle will match (in a complementary sense) the result of the measurement of the first particle, in that they will be opposite in their values.

The above result may or may not be perceived as surprising. A classical system would display the same property, and a hidden variable theory (see below) would certainly be required to do so, based on conservation of angular momentum in classical and quantum mechanics alike. The difference is that a classical system has definite values for all the observables all along, while the quantum system does not. In a sense to be discussed below, the quantum system considered here seems to acquire a probability distribution for the outcome of a measurement of the spin along any axis of the other particle upon measurement of the first particle. This probability distribution is in general different from what it would be without measurement of the first particle. This may certainly be perceived as surprising in the case of spatially separated entangled particles.

## 3.3 Paradox

The paradox is that a measurement made on either of the particles apparently collapses the state of the entire entangled system—and does so instantaneously, before any information about the measurement result could have been communicated to the other particle (assuming that information cannot travel faster than light) and hence assured the "proper" outcome of the measurement of the other part of the entangled pair. In the Copenhagen interpretation, the result of a spin measurement on one of the particles is a collapse into a state in which each particle has a definite spin (either up or down) along the axis of measurement. The outcome is taken to be random, with each possibility having a probability of 50%. However, if both spins are measured along the same axis, they are found to be anti-correlated. This means that the random outcome of the measurement made on one particle seems to have been transmitted to the other, so that it can make the "right choice" when it too is measured.

The distance and timing of the measurements can be chosen to make the interval between the two measurements spacelike, hence, any causal effect connecting the events would have to travel faster than light. According to the principles of special relativity, it is not possible for any information to travel between two such measuring events. It is not even possible to say which of the measurements came first. For two spacelike separated events x1 and x2 there are inertial frames in which x1 is first and others in which x2 is first. Therefore, the correlation between the two measurements cannot be explained as one measurement determining the other: different observers would disagree about the role of cause and effect.

(In fact similar paradoxes can arise even without entanglement: the position of a single particle is spread out over space, and two widely separated detectors attempting to detect the particle in two different places must instantaneously attain appropriate correlation, so that they do not both detect the particle.)

## 3.4 Hidden Variables Theory

A possible resolution to the paradox is to assume that quantum theory is incomplete, and the result of measurements depends on predetermined "hidden variables". The state of the particles being measured contains some hidden variables, whose values effectively determine, right from the moment of separation, what the outcomes of the spin measurements are going to be. This would mean that each particle carries all the required information with it, and nothing needs to be transmitted from one particle to the other at the time of measurement. Einstein and others (see the previous section) originally believed this was the only way out of the paradox, and the accepted quantum mechanical description (with a random measurement outcome) must be incomplete.

## 3.5 Violations of Bell's Inequality

Local hidden variable theories fail, however, when measurements of the spin of entangled particles along different axes are considered. If many pairs of such measurements are made (on a large number of pairs of entangled particles), then statistically, if the local realist or hidden variables view were correct, the results would always satisfy Bell's inequality. Several experiments have shown in practice that Bell's inequality is not satisfied. However, prior to 2015, all of these had loophole problems that were considered the most important by the community of physicists. When measurements of the entangled particles are made in moving relativistic reference frames, in which each measurement (in its own relativistic time frame) occurs before the other, the measurement results remain correlated.

The fundamental issue about measuring spin along different axes is that these measurements cannot have definite values at the same time—they are incompatible in the sense that these measurements' maximum simultaneous precision is constrained by the uncertainty principle. This is contrary to what is found in classical physics, where any number of properties can be measured simultaneously with arbitrary accuracy. It has been proven mathematically that compatible measurements cannot show Bell-inequality-violating correlations, and thus entanglement is a fundamentally non-classical phenomenon.

## 3.6 Other types of Experiments

In experiments in 2012 and 2013, polarization correlation was created between photons that never coexisted in time. The authors claimed that this result was achieved by entanglement swapping between two pairs of entangled photons after measuring the polarization of one photon of the early pair, and that it proves that quantum non-locality applies not only to space but also to time.

In three independent experiments in 2013 it was shown that classically communicated separable quantum states can be used to carry entangled states. The first loophole-free Bell test was held in TU Delft in 2015 confirming the violation of Bell inequality.

In August 2014, Brazilian researcher Gabriela Barreto Lemos and team were able to "take pictures" of objects using photons that had not interacted with the subjects but were entangled with photons that did interact with such objects. Lemos, from the University of Vienna, is confident that this new quantum imaging technique could find application where low light imaging is imperative, in fields like biological or medical imaging.

In 2015, Markus Greiner's group at Harvard performed a direct measurement of Renyi entanglement in a system of ultracold bosonic atoms.

From 2016 various companies like IBM, Microsoft etc. have successfully created quantum computers and allowed developers and tech enthusiasts to openly experiment with concepts of quantum mechanics including quantum entanglement

## 3.7 Mystery of Time

There have been suggestions to look at the concept of time as an emergent phenomenon that is a side effect of quantum entanglement. In other words, time is an entanglement phenomenon, which places all equal clock readings (of correctly prepared clocks, or of any objects usable as clocks) into the same history. This was first fully theorized by Don Page and William Wootters in 1983. The Wheeler–DeWitt equation that combines general relativity and quantum mechanics – by leaving out time altogether – was introduced in the 1960s and it was taken up again in 1983, when Page and Wootters made a solution based on quantum entanglement. Page and Wootters argued that entanglement can be used to measure time.

In 2013, at the Istituto Nazionale di Ricerca Metrologica (INRIM) in Turin, Italy, researchers performed the first experimental test of Page and Wootters' ideas. Their result has been interpreted to confirm that time is an emergent phenomenon for internal observers but absent for external observers of the universe just as the Wheeler-DeWitt equation predicts

## 3.8 Source for the Arrow of Time

Physicist Seth Lloyd says that quantum uncertainty gives rise to entanglement, the putative source of the arrow of time. According to Lloyd, "The arrow of time is an arrow of increasing correlations. „The approach to entanglement would be from the perspective of the causal arrow of time, with the assumption that the cause of the measurement of one particle determines the effect of the result of the other particle's measurement.

## 3.9 Emergent Gravity

Based on AdS/CFT correspondence, Mark Van Raamsdonk suggested that spacetime arises as an emergent phenomenon of the quantum degrees of freedom that are entangled and live in the boundary of the space-time. Induced gravity can emerge from the entanglement first law.

## 3.10 Non-Locality and Entanglement

In the media and popular science, quantum non-locality is often portrayed as being equivalent to entanglement. While this is true for pure bipartite quantum states, in general entanglement is only necessary for non-local correlations, but there exist mixed entangled states that do not produce such correlations. A well-known example is the Werner states that are entangled for certain values of $p_{sym}$ but can always be described using local hidden variables. Moreover, it was shown that, for arbitrary numbers of parties, there exist states that are genuinely entangled but admit a local model. The mentioned proofs about the existence of local models assume that there is only one copy of the quantum state available at a time. If the parties can perform local measurements on many copies of such states, then many apparently local states (e.g., the qubit Werner states) can no longer be described by a local model. This is true for all distillable states. However, it remains an open question whether all entangled states become non-local given sufficiently many copies.

In short, entanglement of a state shared by two parties is necessary but not sufficient for that state to be non-local. It is important to recognize that entanglement is more commonly viewed as an algebraic concept, noted for being a prerequisite to non-locality as well as to quantum

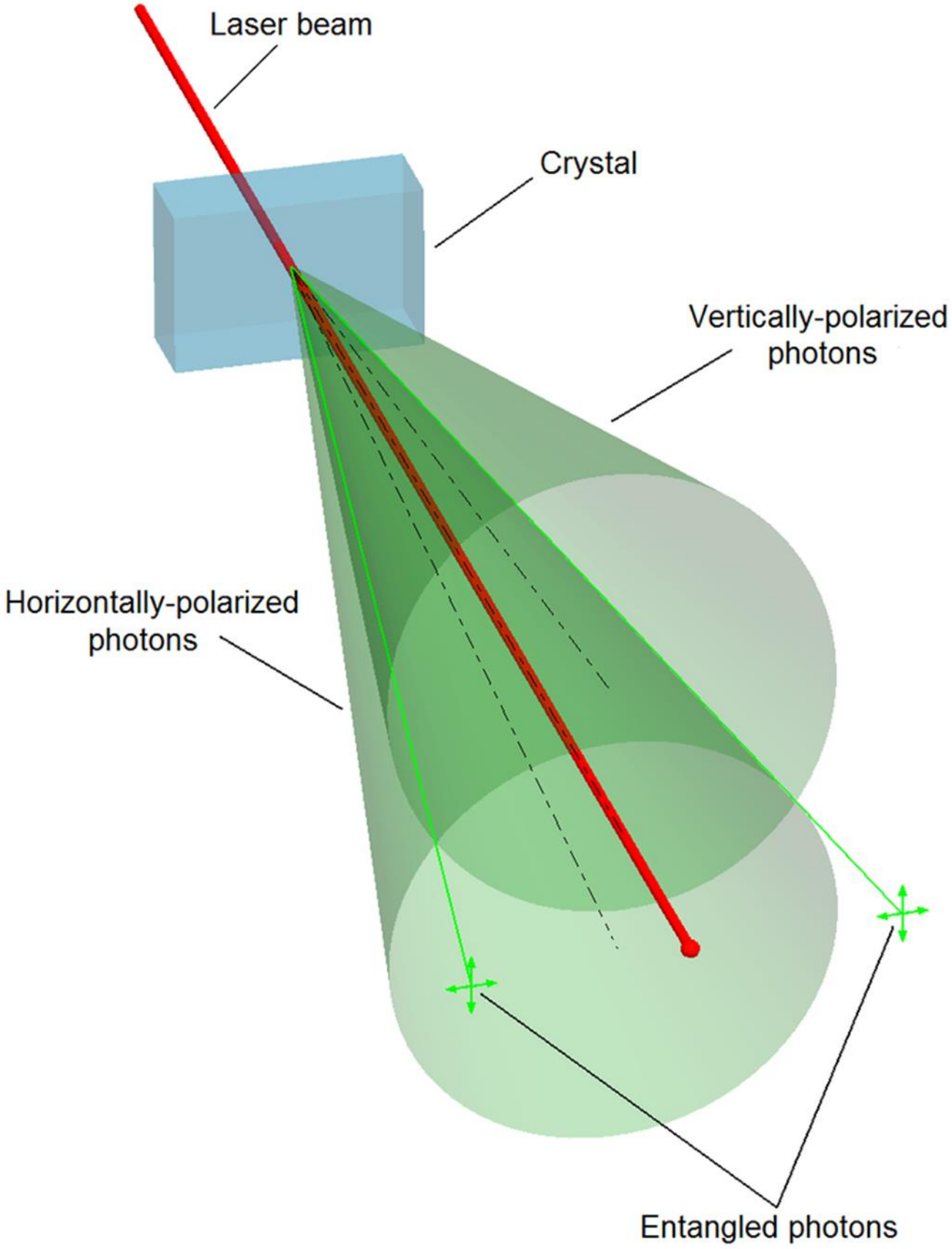
teleportation and to super dense coding, whereas non-locality is defined according to experimental statistics and is much more involved with the foundations and interpretations of quantum mechanics

## 3.11 Methods of creating Entanglement

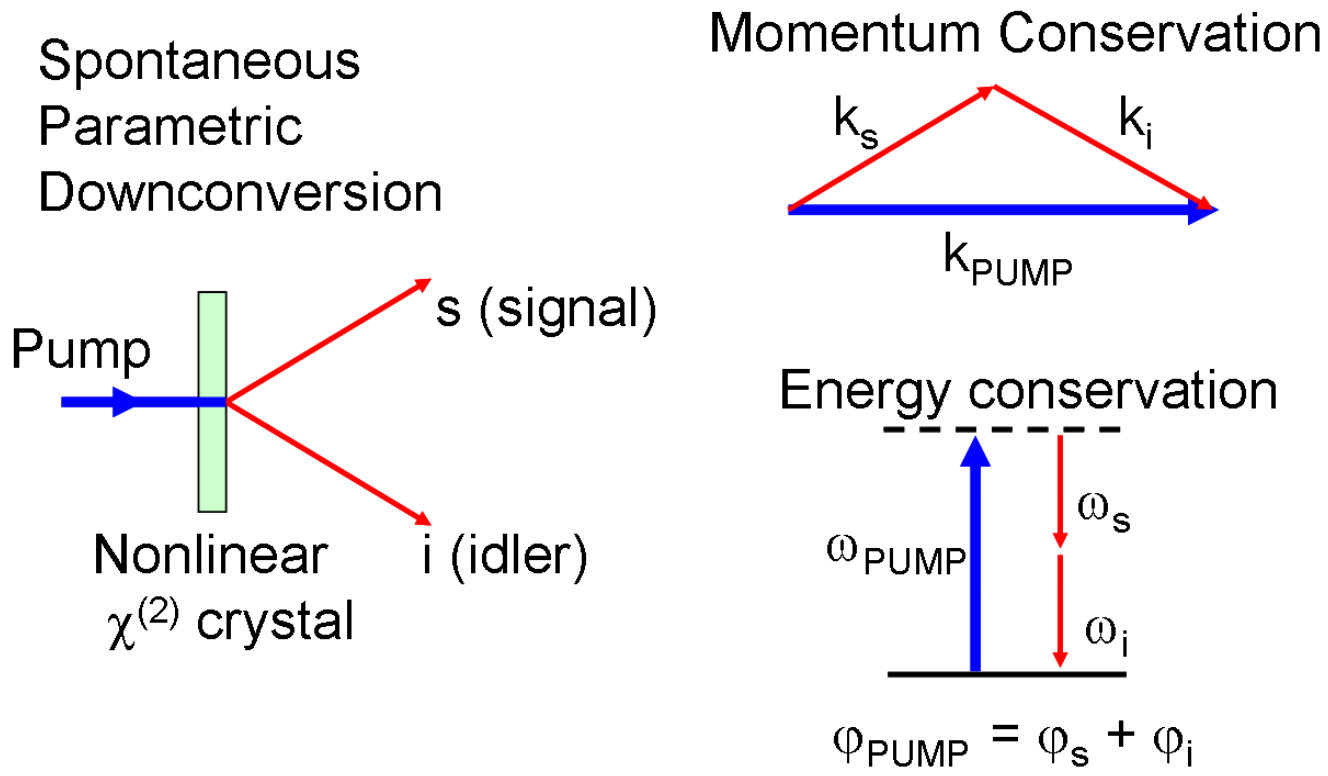
Entanglement is usually created by direct interactions between subatomic particles. These interactions can take numerous forms. One of the most used methods is spontaneous parametric down-conversion to generate a pair of photons entangled in polarisation. Other methods include the use of a fiber coupler to confine and mix photons, photons emitted from decay cascade of the bi-exciton in a quantum dot, the use of the Hong–Ou–Mandel effect, etc., In the earliest tests of Bell's theorem, the entangled particles were generated using atomic cascades.

It is also possible to create entanglement between quantum systems that never directly interacted, using entanglement swapping. Two independently prepared, identical particles may also be entangled if their wave functions merely spatially overlap, at least partially

## 4.0 Spontaneous Parametric Down-Conversion (SPDC)



Spontaneous parametric down-conversion (also known as SPDC, parametric fluorescence or parametric scattering) is a nonlinear instant optical process that converts one photon of higher energy (namely, a pump photon), into a pair of photons (namely, a signal photon, and an idler photon) of lower energy, in accordance with the law of conservation of energy and law of conservation of momentum. It is an important process in quantum optics, for the generation of entangled photon pairs, and of single photons.




## 4.1 Basic Process

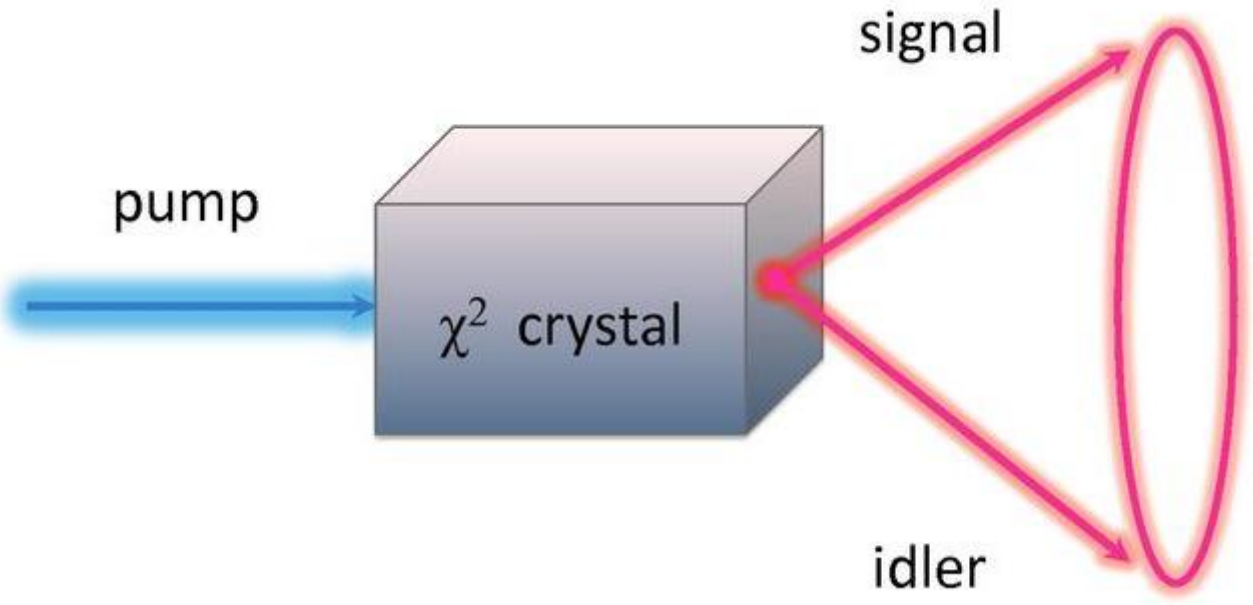
A nonlinear crystal is used to split photon beams into pairs of photons that, in accordance with the law of conservation of energy and law of conservation of momentum, have combined energies and momenta equal to the energy and momentum of the original photon and crystal lattice. Because the index of refraction changes with frequency, only certain triplets of frequencies will be phase-matched so that simultaneous energy and momentum conservation can be achieved. Phase-matching is most achieved using birefringent nonlinear materials, whose index of refraction changes with polarization. As a result of this, different types of SPDC are categorized by the polarizations of the input photon (the pump) and the two output photons (signal and idler). If the signal and idler photons share the same polarization with each other and with the destroyed pump photon it is deemed Type-0 SPDC; if the signal and idler photons share the same polarization to each other, but are orthogonal to the pump polarization, it is Type-I SPDC. If the signal and idler photons have perpendicular polarizations, it is deemed Type II SPDC.

The conversion efficiency of SPDC is typically very low, with the highest efficiency obtained on the order of 4 pairs per 106 incoming photons for PPLN in waveguides. However, if one half of the pair (the "signal") is detected at any time then its partner (the "idler") is known to be present. The degenerate portion of the output of a Type I down converter is a squeezed vacuum that contains only even photon number terms. The degenerate output of the Type II down converter is a two-mode squeezed vacuum.

## 4.2 Example

An SPDC scheme with the Type II output

In a commonly used SPDC apparatus design, a strong laser beam, termed the "pump" beam,




is directed at a BBO (beta-barium borate) crystal. Most of the photons continue straight through the crystal. However, occasionally, some of the photons undergo spontaneous down-conversion with Type II polarization correlation, and the resultant correlated photon pairs have trajectories that are constrained along the edges of two cones, whose axes are symmetrically arranged relative to the pump beam. Also, due to the conservation of momentum, the two photons are always symmetrically located along the edges of the cones, relative to the pump beam. Importantly, the trajectories of the photon pairs may exist simultaneously in the two lines where the cones intersect. This results in entanglement of the photon pairs whose polarization are perpendicular.

Another crystal is KDP (potassium dihydrogen phosphate) which is mostly used in Type I down conversion, where both photons have the same polarization.

## 4.3 History

SPDC was described as early as 1970 by D. Klyshko and co-authors, and D. C. Burnham and D. L. Weinberg. It was first applied to experiments related to coherence by two independent pairs of researchers in the late 1980s: Carroll Alley and Yanhua Shih, and Rupamanjari Ghosh and Leonard Mandel. The duality between incoherent (Van Cittert–Zernike theorem) and biphoton emissions was found.

## 4.4 Applications

SPDC allows for the creation of optical fields containing (to a good approximation) a single photon. As of 2005, this is the predominant mechanism for an experimenter to create single photons (also known as Fock states). The single photons as well as the photon pairs are often used in quantum information experiments and applications like quantum cryptography and Bell test experiments.

SPDC is widely used to create pairs of entangled photons with a high degree of spatial correlation. Such pairs are used in ghost imaging, in which information is combined from two light detectors: a conventional, multi-pixel detector that does not view the object, and a single-pixel (bucket) detector that does view the object.

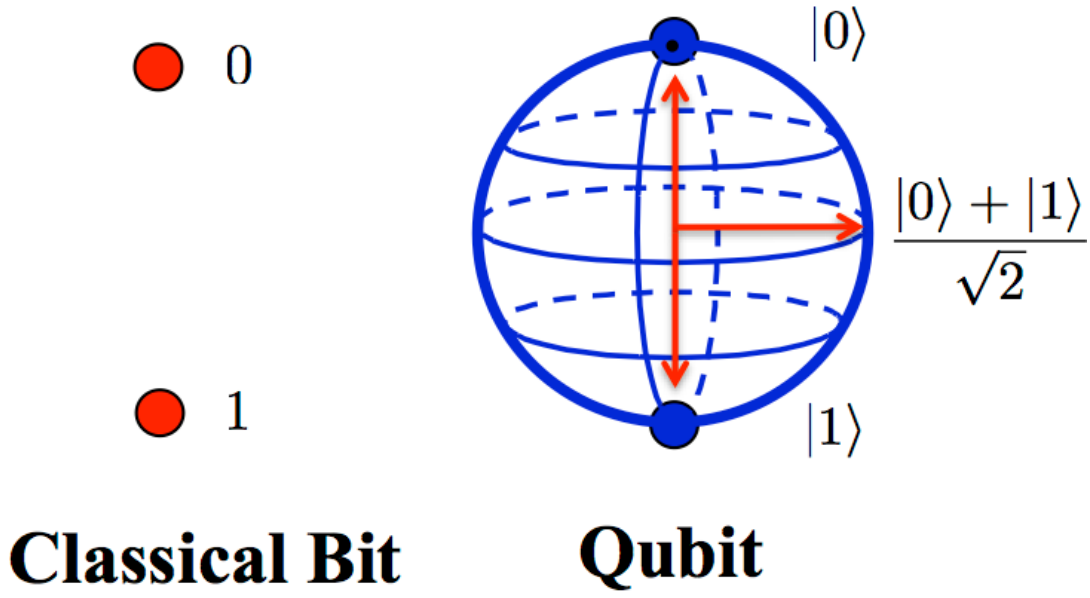
## 4.5 Alternatives

The newly observed effect of two-photon emission from electrically driven semiconductors has been proposed as a basis for more efficient sources of entangled photon pairs. Other than SPDC-generated photon pairs, the photons of a semiconductor-emitted pair usually are not identical but have different energies. Until recently, within the constraints of quantum uncertainty, the pair of emitted photons were assumed to be co-located: they are born from the same location. However, a new nonlocalized mechanism to produce correlated photon pairs in SPDC has highlighted that occasionally the individual photons that constitute the pair can be emitted from spatially separated points.

## 5.0 Qubit

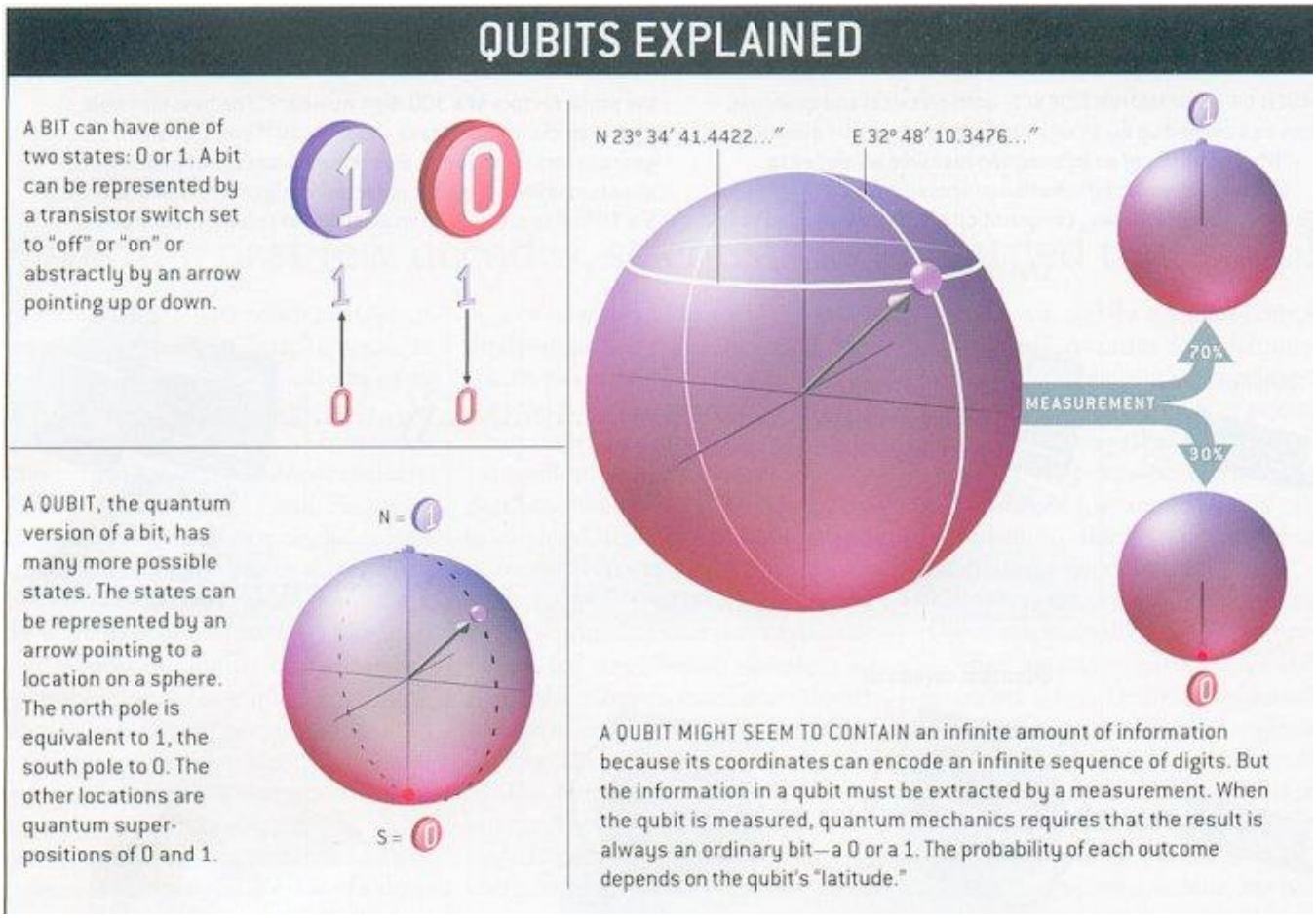
In quantum computing, a qubit or quantum bit (sometimes qbit) is the basic unit of quantum information - the quantum version of the classical binary bit physically realized with a two-state device. A qubit is a two-state (or two-level) quantum-mechanical system, one of the simplest quantum systems displaying the peculiarity of quantum mechanics.

Examples include: the spin of the electron in which the two levels can be taken as spin up and spin down; or the polarization of a single photon in which the two states can be taken to be the vertical polarization and the horizontal polarization. In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a coherent superposition of both states simultaneously, a property which is fundamental to quantum mechanics and quantum computing.



## 5.1 Multiple States

In superposition, a qubit can be in multiple states at the same time, having a value of not just 0 or 1, but both, and any amount of numbers in between. This has some serious implications for computing. Imagine a quantum computer playing chess, it would be able to analyse every single possible move all at once, and then pick the best one. This is in comparison to a modern computer, which would need to analyse and take actions one at a time.




## 5.2 Qubit Entanglement

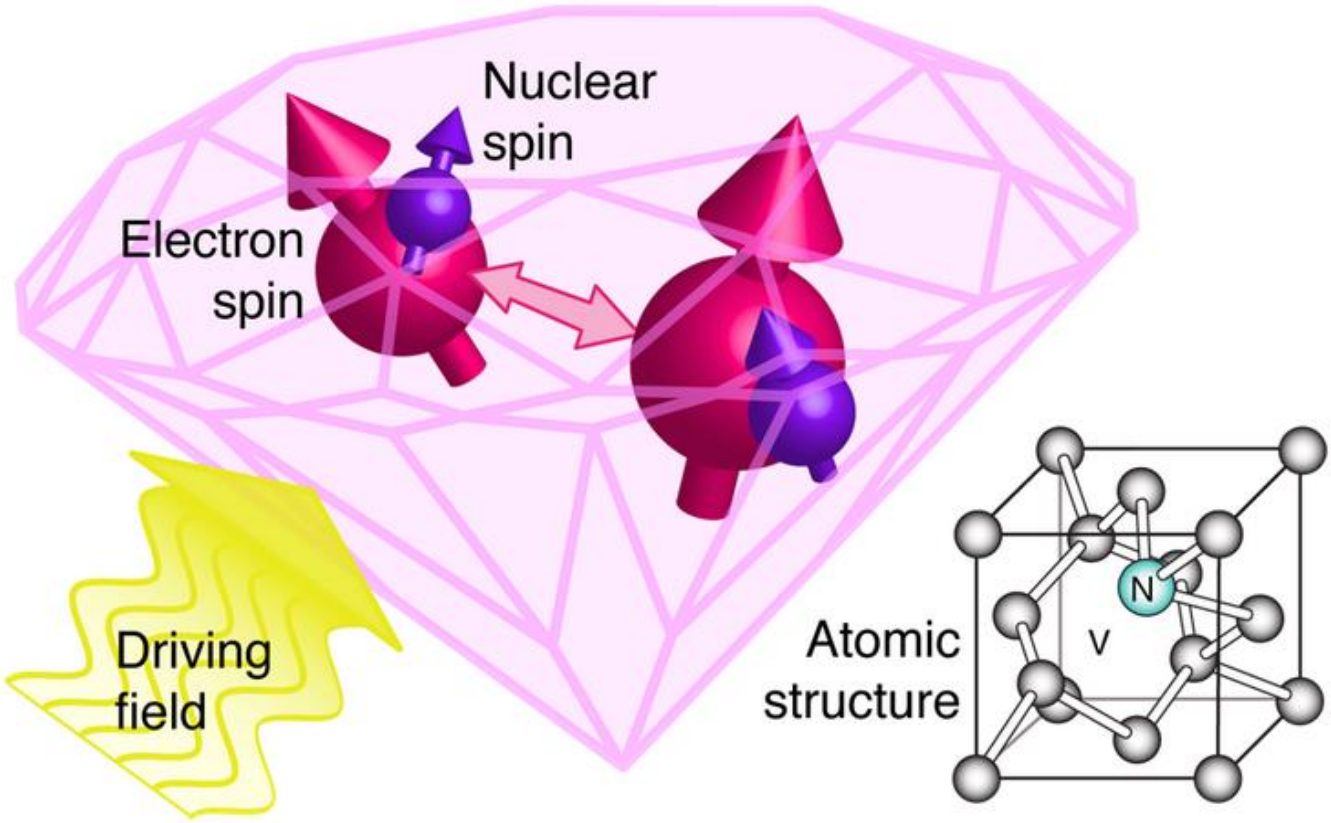
Another strange property of qubits is their ability to be linked together, called entanglement, even over massive distances where there is zero possibility of a physical connection. When two qubits are linked together, they will both share a similar state, or value, being 1 or 0. And each qubit that you add to the mix doubles the possible processing capabilities.

Imagine that these two entangled qubits are separated, with one each given to Alice and Bob. Alice makes a measurement of her qubit, obtaining - with equal probabilities - either **|0** or **|1** , i.e., she can now tell if her qubit has value "0" or "1". Because of the qubits' entanglement, Bob must now get the same measurement as Alice. For example, if she measures a **|0** , Bob must measure the same, as **|00** is the only state where Alice's qubit is a **|0**. In short, for these two entangled qubits, whatever Alice measures, so would Bob, with perfect correlation, in any basis, however far apart they may be and even though both cannot tell if their qubit has value "0" or "1" - a most surprising circumstance that cannot be explained by classical physics.

## 5.3 Diamond Qubits

We can have a qubit relying on sole support from Quantum Diamond Technologies, which is the only qubit to be powered by diamonds and light.

- **Benefits**: Unlike other qubits which need to operate at near zero temperatures, diamond vacancy qubits can work at room temperatures.
- **Bummers**: On the flip side, these qubits are also tough to entangle, does this have something to do with the temperature perhaps?
- **How it works**: A diamond lattice is combined with a nitrogen atom and vacancy, and a superposition state is controlled by light.
- **Records**: To date, this qubit has achieved a superposition state lasting 10 seconds, with 6 qubits entangled.




## 5.4 Parallel Computing Power of Qubits

If you entangled 300 qubits together, you could perform more parallel computations than there are known atoms in the universe. The possibilities are overwhelming to think about.