Quantum Communications: A Primer

Table of Contents

1. What is Quantum Anyway?

Quantum has been a buzzword lately, but without a PhD in quantum physics it is difficult to sort out the myth from reality. This paper is a primer geared towards the reader who wants to understand what the fuss is all about, and hopefully explain some basics about the second quantum revolution, quantum technology, and specifically, quantum communications.

1.1 The 30,000 Foot View

As a start, let's address the key points:

- Quantum communications is different than quantum computing. They both fall under the broad umbrella of quantum technologies but quantum computing is more famous. However, quantum communications is (arguably) more mature and ready for practical applications.
- All quantum technologies manipulate quantum properties of small particles for practical uses. The real-world applications are what separate quantum tech from quantum theory (the gory math) and quantum experiments (the lab research).
- There are different flavors of quantum communications, but they all manipulate the quantum properties of photons, or particles of light. And because they are particles of light, you need to harness their movement.
- There are also different applications for quantum communications. The most well-known is quantum key distribution, also known as QKD, quantum encryption, or quantum cryptography. But there are other applications, including quantum clock synchronization, quantum teleportation, quantum radar, and quantum networking.
- Quantum communications is related to optical communications, and typically utilizes the same wavelengths, hardware, and delivery medium (free-space directional links or fiber optics). But that means it has the same losses and directionality as optical communications, and cannot penetrate clouds or walls like RF.

1.2 The Myths and Misunderstandings

Because of all the breathless headlines, it is not easy to separate the science from the science fiction. Here are a few of the more common quantum myths:

- Quantum communications does not enable faster than light communications through entanglement.
- Quantum computing ≠ super-duper fast computing. Quantum computers can handle certain problems or algorithms better than conventional computers.
- Quantum is not scary/magical/weird. Sure, the math is hard and it acts differently than our experience with classical physics. But we are all bound by quantum effects and our understanding of this is growing.
- Quantum teleportation does not teleport matter, ala Star Trek, but teleports information.
- Einstein's famous comment "spooky action at a distance" did not mean he disagreed with entanglement, he just did not like some aspects of it. He was partially wrong about how

entanglement works but give him credit: he was the first to discover the concept of entanglement with a thought experiment!

- Nobody understands quantum physics. OK, that is not a myth.

2. How does Quantum Communications Work?

We are in the middle of the second quantum revolution, a time when quantum properties are being harnessed for new practical applications. It is known as the second because the first quantum revolution gave us the transistor, laser, and atomic clock. But this all started with some smart scientists a century ago.

2.1 Quantum Physics and the Birth of Quantum Communications

Quantum affects all objects, large and small, but its effects are most noticeable in small particles, such as photons, electrons, protons, atoms and molecules. What makes quantum physics such a difficult topic to comprehend is the behavior of small particles is impossible to directly observe, and so counter-intuitive from our understanding of classical physics. The scientists that pioneered our understanding of quantum mechanics over the last century - Einstein, Heisenberg, Schrödinger, Bohr – had to base their theories on experiments (including thought experiments) and complex equations. But their work led to these central tenets of quantum mechanics:

- Wave-particle duality: Photons exhibit both wave- and particle-like behavior.
- Uncertainty principle: The exact position and the exact momentum of a photon can never be simultaneously measured due to the wave-particle duality.
- No-cloning theorem: It is impossible to create an identical copy of an arbitrary unknown quantum state, which ensures that quantum information cannot be exactly copied.
- Entanglement: Under some conditions, groups of photons can be generated such that their properties are correlated beyond what is possible in classical physics. We refer to these "beyond-classical" correlations as "entanglement".

These basic laws opened the door to a wide range of quantum research with the realization that quantum properties were a resource to be exploited. Fast forward fifty years, and we get semiconductors and lasers; fast forward another fifty years to the second quantum revolution underway today. New quantum breakthroughs are being announced almost daily, but they all fall under three broad categories: quantum computing, quantum communications and quantum sensing (**Error! Reference source not found.**).

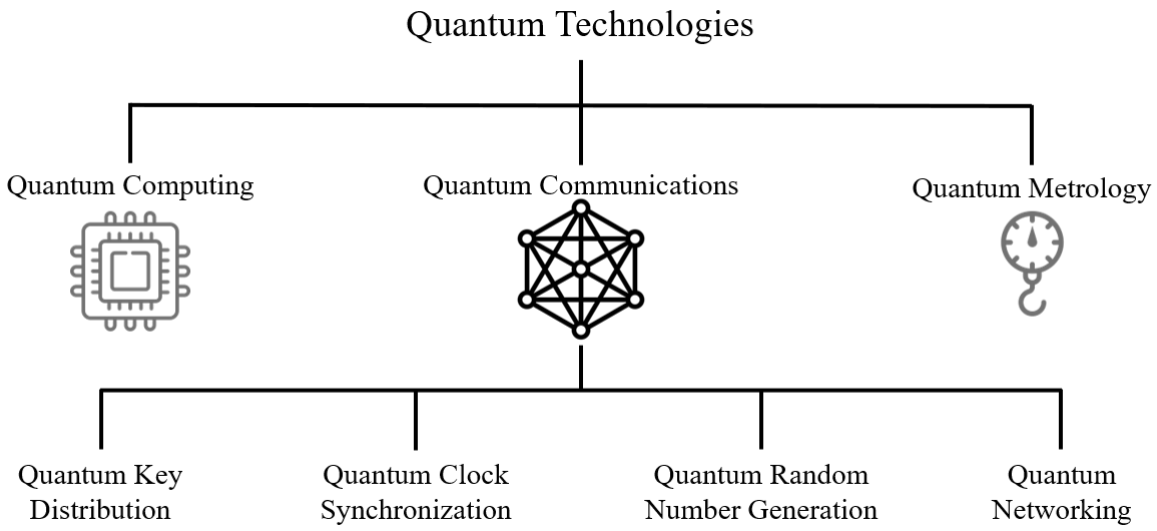

Figure 1. Quantum Technologies and Quantum Communications

The focus of the rest of this paper is quantum communications. Partly because it is not as famous, but also because it is the most advanced. Quantum communication was the first to be seriously developed and is technologically the most mature.

2.2 Quantum vs. Optical and RF Communications

Like other types of communications, quantum communications uses photons. Most quantum communication systems work with photons in the visible or near visible spectrum and is similar to traditional optical, or laser, communications. An optical communication link strives to provide high data rates through modulating a laser beam; a quantum communications channel strives to provide very secure communications by manipulating each individual photon on a beam.

Consider a typical free-space optical communications system available today, where a string of bits are modulated at a high data rate on a laser with 1 watt output power. At a constant output, the laser will produce roughly 7.8×10^{18} photons per second streaming from A (let's call them Alice) to B (call them Bob). A successful data link is achieved when enough photons reach the Bob's receiver to achieve a coherent link.

By contrast, a quantum communications channel uses the quantum property of individual photons. So instead of modulating the signal (which is essentially regulating the flow of photons), the quantum properties of the individual photons themselves are manipulated. Because of this "processing" quantum transmitters (known as sources) produce a lower photon output (typically in the millions of photons per second) than a laser. The quantum sources and detectors (receivers) are available today, but there is lots of room for improvement.

At a very basic level, the quantum-manipulated photons are transmitted by Alice and received by Bob. If an eavesdropper (call them Eve) observes the photon instead of Bob, the quantum properties of the photon are irreparably changed, and Alice and Bob can verify this with a check.

2.3 Different Flavors of Quantum Communications

At its core, quantum communication processes are based on either a prepare and measure or entanglement based protocols.

The best known Prepare-and-Measure protocol is BB84 (after the paper written by Charles Bennett and Gilles Brassard in 1984), which relies on the uncertainty principle and the quantum no-cloning theorem. Alice encodes random bits through the polarization of individual photons. Bob receives these photons, measures the polarization states, and, after protocol checks with Alice, verifies they both have the same unique, random, secure string of bits. Eve may intercept the photons and try to extract the information, but only Alice and Bob know the correct polarization to measure, any attempt by Eve introduces detectable disturbances.

Prepare-and-Measure has been demonstrated with low power lasers that emit very small numbers of photons (ideally, one) per pulse. Because of this, Prepare-and-Measure is also known as weak coherent pulse.

Entanglement-based protocols (such as E91, named after the 1991 Artur Ekert paper) takes advantage of quantum entanglement. Pairs of entangled photons are created and sent to Alice and Bob, who measure their correlated properties. If Eve intercepts one of the pairs, the entanglement is broken, introducing errors and making Eve's presence detectable.

In contrast to Prepare-and-Measure schemes, entanglement does not require encoding states into the photons. Instead, both parties share a source of maximally entangled photon pairs, which is a truly random process. The distribution of entangled photons necessary for this process is also the foundation for a truly quantum network. Shared entanglement is a basic resource for quantum teleportation and other applications of what could loosely be called the quantum internet.

2.4 Practical Applications for Quantum Communications

While quantum communications has been demonstrated in a lab for decades, the hardware and applications have now advanced to the point where it is being commercialized.

The main application is quantum key distribution (QKD), a method for securely delivering encryption keys. QKD takes advantage of these characteristics:

- Randomness – quantum communications can only create random strings of bits between the two parties, Alice and Bob. A pre-defined string of bits cannot be transmitted over a quantum channel, at least according to existing protocols.
- Low data rate – current quantum communication systems are only capable of low data rates today, in the neighborhood of kbps.
- Very secure – the strings of bits are not actually transmitted, per se, but created as part of the quantum communications process. This is more secure than existing systems where messages are delivered across the open network, making it susceptible to interception.

Because of these features, QKD allows for the distribution of secure shared randomness. One application is extremely secure keys that can then be used to seed other encryption mechanisms or directly to completely protect extremely sensitive information.

Quantum communications is also valuable for secure and accurate clock synchronization. Modern networks rely on timing reference from GPS, which has limited accuracy and can be easily spoofed. Quantum clock synchronization (QCS), in contrast, exploits the femtosecond-level correlations between pairs of entangled photons to provide accuracy that is orders of magnitude better than GPS. QCS also exploits two other quantum properties, the Quantum No-Cloning Theorem and Entanglement, to ensure that an adversary cannot receive a quantum signal and retransmit it.

The QCS protocol starts with two remote parties, Alice and Bob, with an unknown time delta between them. Each of them has an entangled photon source and receiver and the ability to link through free-space or fiber optic. Alice sends one of the photons of each entangled pair produced at her side to Bob and measures the other one according to her local clock. Bob performs the same operations on his side. Alice and Bob also each measure the time of arrival of incoming photons. They then share the times of arrival of the measured photons. Processing the data via a cross-correlation provides the time delta between their clocks (irrespective of distance between them). They also do a check to guarantee that the signal was not spoofed.

3. Why Quantum Communications?

The value of quantum communications is primarily due to its security. But within the quantum properties of photons there are other features that can be exploited for timing synchronization and networking.

3.1 Exposing Eavesdroppers

If Alice and Bob want to exchange a sensitive message over a long distance, it is commonly accepted that this message can be intercepted by Eve. All current communications networks are known to be susceptible to Eve, whether it is undersea cables, cellular networks, terrestrial fiber optic or coaxial cables, or satellite communications via RF or optical links. But not quantum communications.

When Alice and Bob communicate via a quantum channel, any attempt at interception by Eve is known by both parties. While quantum communications does not necessarily thwart Eve, it does provide knowledge that Eve is present and the link has been compromised. This provides an unprecedented level of security.

3.2 Timing Synchronization

Consider the case where Alice and Bob now want to synchronize their clocks. Again, they are separated by a distance but have the means to exchange signals. Alice can send a modulated signal to Bob, who then measures the phase on the signal. This phase measurement allows Bob to calculate the distance to Alice. If Bob knows the distance to a bunch of different reference points, then Bob can use this to calculate his relative time and position. This is the basic precept behind Global Positioning System (GPS) and other Global Navigation Satellite Systems (GNSS).

Without accurate timing, Alice and Bob do not know their positions and cannot navigate. And if they want to communicate data within a complex network, they need to know their timing in order to efficiently send and receive data.

But there are limitations with obtaining timing from RF or optical signals:

- Accuracy of the phase measurements and internal error sources.
- Alice and Bob need to first know the distance between them.
- Security, as any malicious party can relatively easily copy Alice's signal.

Quantum communications overcomes these limitations.

3.3 True Random Numbers are Tough to Make and Verify

This may seem like a niche need, but let's say that Alice wants to create a truly random string of bits. This may seem like a trivial exercise – Alice can use a computer's random number generator or simply flip a coin. But these are not truly random processes, and, even if they were, how would Alice know this for sure?

In the world of security this is a big headache. Fortunately, there are quantum processes that are provably random.

3.4 Teleportation – but not like Star Trek

There is a future scenario where Alice wants to transfer a specific type of quantum information to Bob. Maybe they both have quantum computers and they want to share their qubits. They could use classical communication channels. But that means they need to transfer their qubits to bits and send them via data packets. Not exactly efficient.

Quantum teleportation is a technique for transferring quantum information. Unfortunately this naming tends to make think that there is matter being transported, instead of just quantum information. But practical quantum teleportation is a stepping stone to the future of quantum networks and the mythical quantum internet. Alas, there is still a lot of development ahead before this is a reality.

4. Who is working on Quantum Communications?

Since the publication of the original papers decades ago, scientists have successfully conducted numerous quantum communications demonstrations.

The most advanced area of development today has been quantum communications over fiber optics using weak coherent pulse. Due to the attenuation in the glass, quantum links have been established between two nodes within short distances (less than 80 km). For longer distances quantum repeaters would need to be added. But the development continues apace by research labs and commercial companies across the world.

In contrast, space-based quantum communications provide better utility for long distance applications. At this stage, only a few groups in the world have completed on-orbit quantum communication demonstrations, with China leading the charge. Their Quantum Experiments at Space Scale (QUESS) proof-of-concept mission was launched on the Micius satellite in August 2016, where three key milestones were announced:

- QKD between satellite and ground stations using BB84 protocol

- Entanglement distribution between satellite and ground stations
- Ground-to-satellite quantum teleportation

But many more terrestrial and space-based projects are in development, many of which are outlined in the IOP Science Focus on Quantum Science and Technology Initiatives Around the World. There are also numerous private and public companies rolling out quantum communication systems.

5. When will Quantum Communications be Viable?

Today!

Quantum communication systems and QKD networks have been rolling out at a rapid pace over the last few years. Most of the development has occurred with government agencies but many private and public companies have embraced quantum communications. Where can I learn more?

For further reading on this interesting topic we recommend:

- "In Quantum We Trust", Accenture Paper
- "The Realist's Guide to Quantum Technology and National Security", Deloitte Paper
- "Quantum Cryptography Demystified: How It Works in Plain Language", ExtremeTech
- "Explainer: What is Quantum Communication?", MIT Technology Review
- "The Quantum Internet is Already being Built", Cosmos Magazine
- "Quantum Internet, a Vision for the Road Ahead", Science Magazine