Part 8

Quantum Cryptography

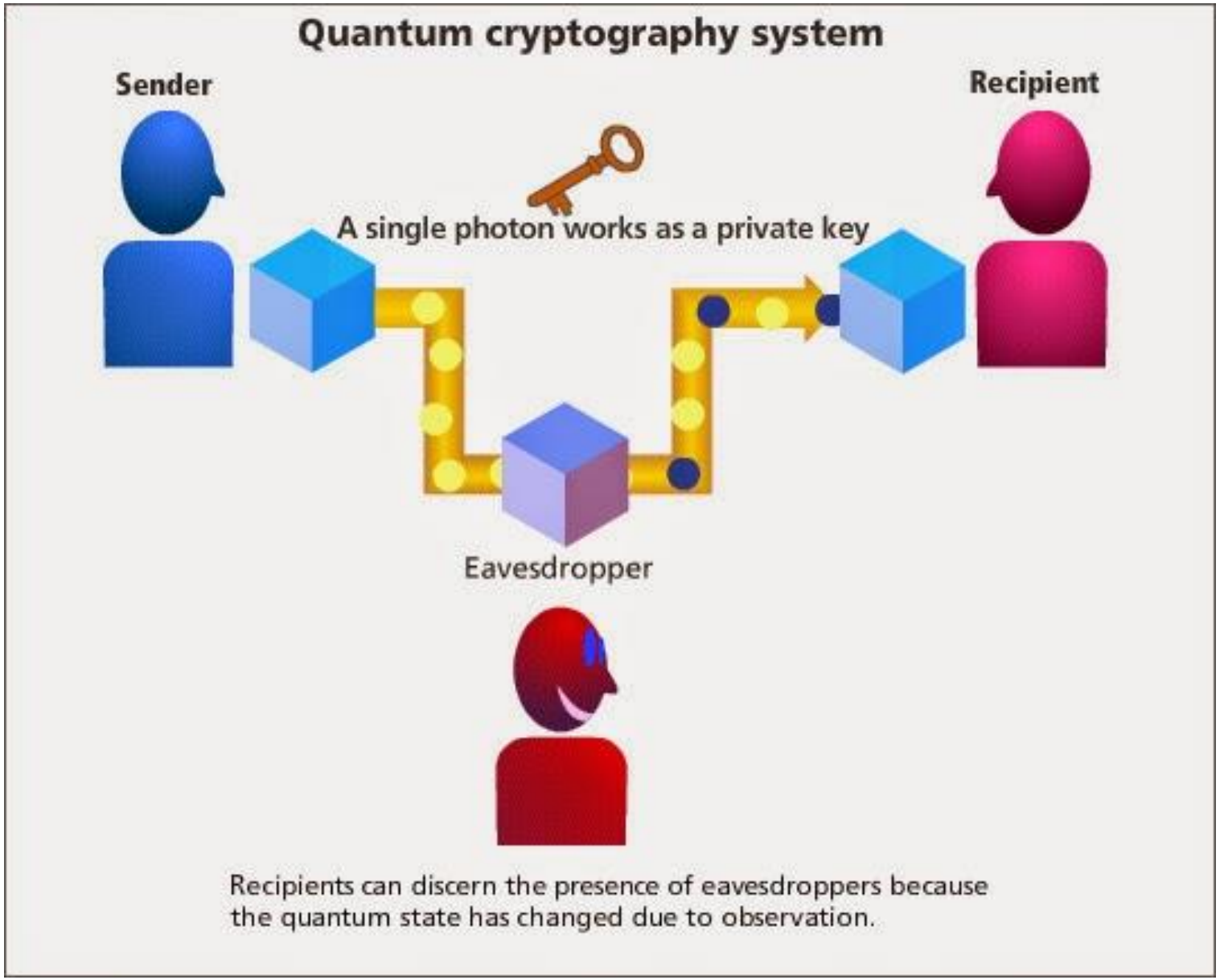
Quantum Cryptography

- Quantum cryptography uses **physics** to develop a cryptosystem completely secure against being compromised without knowledge of the sender or the receiver of the messages.
- The word Quantum itself refers to the most **fundamental behavior of the smallest particles** of matter and energy.
- Quantum cryptography is different from traditional cryptographic systems in that it **relies more on physics**, rather than **mathematics**, as a key aspect of its security model.

- Essentially, quantum cryptography is based on the **usage of individual particles/waves of light (photon) and their intrinsic quantum properties to develop an unbreakable cryptosystem** (because it is impossible to measure the quantum state of any system without disturbing that system.)

- Quantum cryptography uses **photons** to transmit **a key**. Once the key is transmitted, coding and encoding using the normal secret-key method can take place.
- But how does a photon become a key? How do you attach information to a photon's spin?

- This is where binary code comes into play. Each type of a photon's spin represents one piece of information -- usually a 1 or a 0, for binary code.
- This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o.
- So a binary code can be assigned to each photon -- for example, a photon that has a vertical spin (|) can be assigned a 1.


Quantum cryptography system
Sender
Recipient
A single photon works as a private key
Eavesdropper
Recipients can discern the presence of eavesdroppers because
the quantum state has changed due to observation.

- “If you build it correctly, no hacker can hack the system. The question is what it means to build it correctly,” said physicist Renato Renner from the Institute of Theoretical Physics in Zurich.

- Regular, non-quantum encryption can work in a variety of ways but generally a message is scrambled and can only be unscrambled using a secret key. The trick is to make sure that whomever you're trying to hide your communication from doesn't get their hands on your secret key.
- Cracking the private key in a modern crypto system would generally require figuring out the factors of a number that is the product of two insanely huge prime numbers.
- The numbers are chosen to be so large that, with the given processing power of computers, it would take longer than the lifetime of the universe for an algorithm to factor their product.

- But such encryption techniques have their vulnerabilities. Certain products – called **weak keys** – happen to be easier to factor than others. Also, **Moore's Law** continually ups the processing power of our computers.
- Even more importantly, mathematicians are constantly developing new algorithms that allow for easier factorization.

- Quantum cryptography avoids all these issues. Here, the key is **encrypted into a series of photons** that get passed between two parties trying to share secret information.
- **The Heisenberg Uncertainty** Principle dictates that an adversary can’t look at these photons without changing or destroying them.

- “In this case, it doesn’t matter what technology the adversary has, they’ll never be able to break the laws of physics,” said physicist Richard Hughes of Los Alamos National Laboratory in New Mexico, who works on quantum cryptography.

Problems with using Quantum Cryptography

- But in practice, quantum cryptography comes with its own load of weaknesses. It was recognized in 2010, for instance, that a hacker could **blind a detector** with a strong pulse, rendering it unable to see the secret-keeping photons.

- Photons are often generated using **a laser** tuned to such a low intensity that it’s producing one single photon at a time.
- There is a certain probability that the laser will make a photon encoded with your secret information and then a second photon with that same information.
- In this case, all an enemy has to do is steal that second photon and they could gain access to your data while you’d be none the wiser.

- Alternatively, noticing when a single photon has arrived can be tricky.
- Detectors might not register that a particle has hit them, making you think that your system has been hacked when it’s really quite secure.

- Any encryption method will only be as secure as the **humans running** it, added Hughes.
- Whenever someone claims that a particular technology “is fundamentally unbreakable, people will say that’s snake oil,” he said. “Nothing is unbreakable.”

- Quantum cryptography is based on the principle of **quantum key distribution (QKD),** which enables two parties to generate a shared secret key that can be used to encrypt and decrypt messages.
- The key is generated by transmitting single photons or quantum states between the parties, and measuring the properties of the photons to obtain a series of random numbers that form the key.
- Because of the laws of quantum mechanics, it is not possible for an eavesdropper to intercept the key without being detected.

- The security of quantum cryptography comes from the fact that the act of measuring a quantum state collapses the state, making it impossible to determine the original state without introducing an error.
- This means that any attempt to intercept the key will alter the state of the photons and make it immediately apparent to the communicating parties.

- Quantum cryptography has been demonstrated to be highly secure, but it has some limitations, such as the need for **a direct line of sight** between the communicating parties, and the **limited distance** over which the quantum states can be transmitted.
- Despite these limitations, quantum cryptography is widely seen as a promising technology for secure communication and is being actively researched and developed by many organizations and universities around the world.

Challenges facing Quantum Cryptography

- **Technical challenges:** Implementing quantum cryptography systems can be complex and require specialized knowledge and equipment.

- **Distance limitations:** Currently, quantum cryptography systems have limited transmission distances and require a direct line of sight between the communicating parties.

- **Cost:** Quantum cryptography systems can be expensive to implement and maintain, making it difficult for smaller organizations to adopt the technology.

- **Interoperability:** Different quantum cryptography systems may not be compatible with each other, making it difficult to establish secure communication between parties using different systems.

- **Eavesdropping attacks:** While quantum cryptography is highly secure against eavesdropping, there is still a risk of other types of attacks, such *as denial-of-service attacks or tampering with the communication channel.*

- **Scalability**: It is still unclear how well quantum cryptography systems will scale to meet the demands of large-scale communication networks.

Quantum cryptography requirements for its implementation

- **Quantum States**: Quantum cryptography requires the use of quantum states, such as single photons, to transmit information.

- **Direct Line of Sight**: Currently, quantum cryptography systems require a direct line of sight between the communicating parties, which limits their practical applications.

- **Specialized Equipment**: Implementing a quantum cryptography system requires specialized equipment, such as single-photon detectors, lasers, and optical fibers, to transmit and measure the quantum states.

- **Technical Expertise**: Implementing a quantum cryptography system requires a high level of technical expertise, as the technology is still emerging and requires specialized knowledge.

- **High Bandwidth**: Quantum cryptography systems require a high bandwidth to transmit the quantum states and generate the shared secret key.

- **Real-Time Monitoring**: Quantum cryptography systems must be monitored in real-time to detect any attempts at eavesdropping or tampering with the communication channel.

Applications of Quantum Cryptography

- **Banking and Finance**: Quantum cryptography can be used to secure financial transactions and prevent unauthorized access to sensitive information.

- **Military and Government Communications**: Quantum cryptography can be used to protect sensitive government and military communications from eavesdropping and tampering.

- **Healthcare**: Quantum cryptography can be used to secure the transmission of sensitive patient information, such as medical records and test results.

- **E-commerce**: Quantum cryptography can be used to secure online transactions, such as online banking and shopping.

- **Smart Grid**: Quantum cryptography can be used to secure the communication between smart grid devices, such as meters and control systems, to prevent unauthorized access to the energy grid.

- **Quantum Computing**: Quantum cryptography can be used to secure communication between quantum computing devices and prevent unauthorized access to quantum algorithms and results.

- **Satellite Communication**: Quantum cryptography can be used to secure satellite communication, such as the transmission of satellite imagery and scientific data.

Quantum Internet

- Building a quantum internet is a key ambition for many countries around the world, such a breakthrough will give them competitive advantage in a promising disruptive technology, and opens a new world of innovations and unlimited possibilities.

- Recently the US Department of Energy (DoE) published the first blueprint of its kind, laying out a step-by-step strategy to make the quantum internet dream come true,. The main goal is to make it impervious to any cyber hacking.
- It will “metamorphosize our entire way of life,” says the Department of Energy. Nearly **$625** million in federal funding is expected to be allocated to the project.

- A quantum internet would be able to **transmit large volumes of data across immense distances at a rate that exceeds the speed of light**. You can imagine all the applications that can benefit from such speed.

- Traditional computer data is coded in either zeros or ones. Quantum information is superimposed in both zeros and ones simultaneously.
- Academics, researchers and IT professionals will need to create **devices for the infrastructure of quantum internet including: quantum routers, repeaters, gateways, hubs, and other quantum tools**.
- A whole new industry will be born based on the idea of quantum internet exists in **parallel** to the current ecosystem of companies we have in regular internet.

- The “traditional internet “, as the regular internet is sometimes called, will still exist. It is expected that large organizations will rely on the quantum internet to **safeguard data**, but that individual consumers will continue to use the classical internet.

- Experts predict that the **financial sector** will benefit from the quantum internet when it comes to securing online transactions.
- The **healthcare** sectors and the public sectors are also expected to see benefits.
- In addition to providing a faster, safer internet experience, quantum computing will better position organizations to solve complex problems, like **supply chain management**.
- Furthermore, it will expedite the exchange of vast amounts of data, and carrying out large-scale sensing experiments in **astronomy, materials discovery and life sciences**

- But first let’s explain some of the basic terms of the quantum world: Quantum computing is the area of study focused on developing computer technology based on the principles of quantum theory.
- The quantum computer, following the laws of quantum physics, would gain enormous processing power through the ability to be in multiple states, and to perform tasks using all possible permutations simultaneously.

What is Quantum Internet

- The quantum internet is a network that will let quantum devices exchange some information within an environment that harnesses the **odd laws** of quantum mechanics.
- In theory, this would lend the quantum internet unprecedented capabilities that are impossible to carry out with today's web applications.

- In the quantum world, data can be encoded in the state of qubits, which can be created in quantum devices like a quantum computer or a quantum processor.
- And the quantum internet, in simple terms, will involve sending qubits across a network of **multiple quantum devices** that are physically separated.
- Crucially, all of this would happen thanks to the wild properties that are unique to **quantum states**.

- That might sound similar to the standard internet. But sending qubits around through a quantum channel, rather than a classical one, effectively means leveraging the behavior of particles when taken at their smallest scale – so-called "quantum states".

- Unsurprisingly, qubits cannot be used to send the kind of data we are familiar with, like emails and WhatsApp messages.
- But the strange behavior of qubits is opening up huge opportunities in other, more **niche applications**.

Quantum Communications

• One of the most exciting avenues that researchers, armed with qubits, are exploring, is communications ***security***.

• Quantum security leads us to the concept of *quantum cryptography* which uses physics to develop a cryptosystem completely secure against being compromised without knowledge of the sender or the receiver of the messages.

- Essentially, quantum cryptography is based on the usage of individual particles/waves of light (photon) and their intrinsic quantum properties to develop an unbreakable cryptosystem (*because it is impossible to measure the quantum state of any system without disturbing that system*.)

- Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key? How do you attach information to a photon's spin?

- This is where binary code comes into play. Each type of a photon's spin represents one piece of information -- usually a 1 or a 0, for binary code.
- This code uses strings of 1s and 0s to create a coherent message.
- For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon -- for example, a photon that has a vertical spin **(|)** can be assigned a 1.

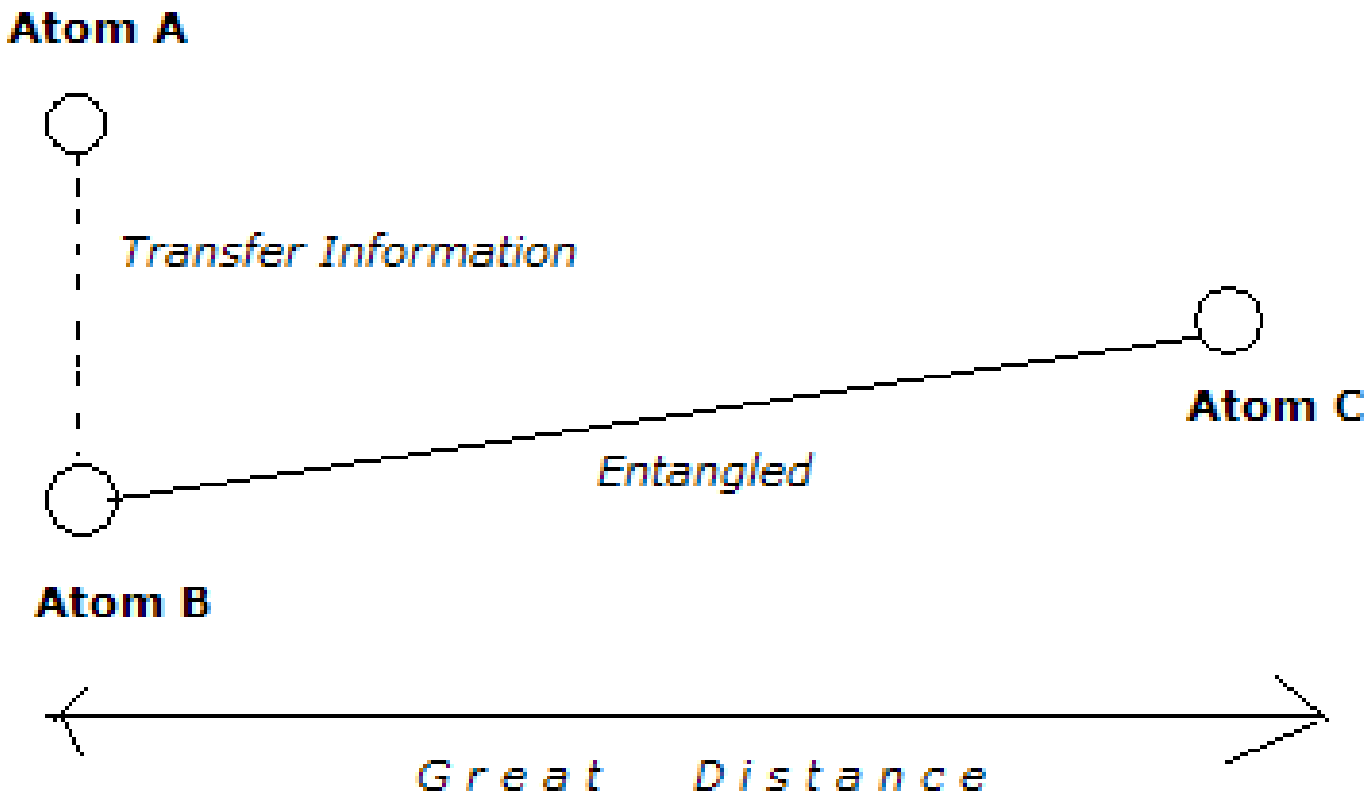
- Regular, non-quantum encryption can work in a variety of ways but generally a message is scrambled and can only be unscrambled using a secret key.
- The trick is to make sure that whomever you're trying to hide your communication from doesn't get their hands on your secret key. But such encryption techniques have their vulnerabilities.
- Certain products – called weak keys – happen to be easier to factor than others.
- Also, Moore's Law continually ups the processing power of our computers.
- Even more importantly, mathematicians are constantly developing new algorithms that allow for easier factorization of the secret key.

- Quantum cryptography avoids all these issues. Here, the key is encrypted into a series of photons that get passed between two parties trying to share secret information.
- The Heisenberg Uncertainty Principle dictates that an adversary can’t look at these photons without changing or destroying them

Quantum Teleportation

- **Quantum teleportation** is a technique for transferring quantum information from a sender at one location to a receiver some distance away.
- While teleportation is commonly portrayed in science fiction as a means to transfer physical objects from one location to the next, quantum teleportation only transfers ***quantum information***.
- An interesting note is that the sender knows neither the location of the recipient nor the quantum state that will be transferred.

- For the first time, a team of scientists and researchers have achieved sustained, high-fidelity ‘quantum teleportation’ — the instant transfer of ‘qubits’, the basic unit of quantum information.
- The collaborative team, which includes NASA’s jet propulsion laboratory, successfully demonstrated sustained, long-distance teleportation of qubits of photons (quanta of light) with fidelity greater than 90%. the qubits (quantum bits) were teleported 44 kilometers (27 miles) over a fiber-optic network using state-of-the-art single-photon detectors and off-the-shelf equipment


Atom A
Transfer Information
Atom C
Entangled
Atom B
Great Distance

- Quantum teleportation is the transfer of quantum states from one location to another.
- Through quantum entanglement, two particles in separate locations are connected by an invisible force, famously referred to as "***spooky action at a distance***" by Albert Einstein.
- Regardless of the distance, the encoded information shared by the "entangled" pair of particles can be passed between them.

- By sharing these quantum qubits, the basic units of quantum computing, researchers are hoping to create networks of quantum computers that can share information at blazing-fast speeds.
- But keeping this information **flow stable over long distances has proven extremely difficult**. Researchers are now hoping to scale up such a system, using both entanglement to send information and quantum memory to store it as well

- On the same front, researchers have advanced their quantum technology researches with a chip that could be scaled up and used to build the quantum simulator of the future using nanochip that allows them to produce enough stable photons encoded with quantum information to scale up the technology.

- The chip, which is said to be less than **one-tenth of the thickness** of a human hair, may enable the researchers to achieve ‘quantum supremacy’ – where a quantum device can solve a given computational task faster than the world’s most powerful supercomputer.

Quantum Teleportation: Paving the Way for a Quantum Internet

- In July, the US Department of Energy unveiled a blueprint for the first quantum internet, connecting several of its National Laboratories across the country. A quantum internet would be able to transmit large volumes of data across immense distances at a rate that **exceeds the *speed of light***. You can imagine all the applications that can benefit from such speed.

- Traditional computer data is coded in either zeros or ones. Quantum information is superimposed in both zeros and ones simultaneously.
- Academics, researchers and IT professionals will need to create devices for the infrastructure of quantum internet including: quantum routers, repeaters, gateways, hubs, and other quantum tools.
- A whole new industry will be born based on the idea of quantum internet exists in parallel to the current ecosystem of companies we have in regular internet.

- The “traditional internet “, as the regular internet is sometimes called, will still exist. It is expected that large organizations will rely on the quantum internet to safeguard data, but that individual consumers will continue to use the classical internet

- Experts predict that the financial sector will benefit from the quantum internet when it comes to securing online transactions. The healthcare sectors and the public sectors are also expected to see benefits.
- In addition to providing a faster, safer internet experience, quantum computing will better position organizations to solve complex problems, like supply chain management.
- Furthermore, it will expedite the exchange of vast amounts of data, and carrying out large-scale sensing experiments in astronomy, materials discovery and life sciences

- Midterm on 3/9
- HW # 2 due 3/12
- Review 3/7