

Cost Effective Quantum Moves a Step Closer

Kyle Romero
204747283
Laboratory 7: Zhaowei Tan

What is quantum computing?

A branch of computer science that utilizes quantum-mechanical phenomena to complete data operations



How does quantum computing differ from classical computing?

Data

Instead of using bits, quantum computers use superposition to store information in qubits (quantum bits).

+

Operations

Instead of logic gates, quantum computers use quantum gates to perform operations on quantum bits.

+

Networking

Allows for the transmission of qubits between physically separate quantum processors

Quantum Supremacy

The term **quantum supremacy** refers to the hypothetical speedup advantage that a quantum computer would have over a classical computer. [1]



Quantum Key Distribution (QKD)

A method of performing a quantum cryptographic task that involves producing a shared, random key that can be used to encrypt and decrypt messages

Quantum Key Distribution Procedure

1. Key Generation

Quantum phenomena are used to generate a secret, shared key

01

03

02

3. Encoding

The information is encoded using the key generated and a different encryption algorithm

2. Key Distribution

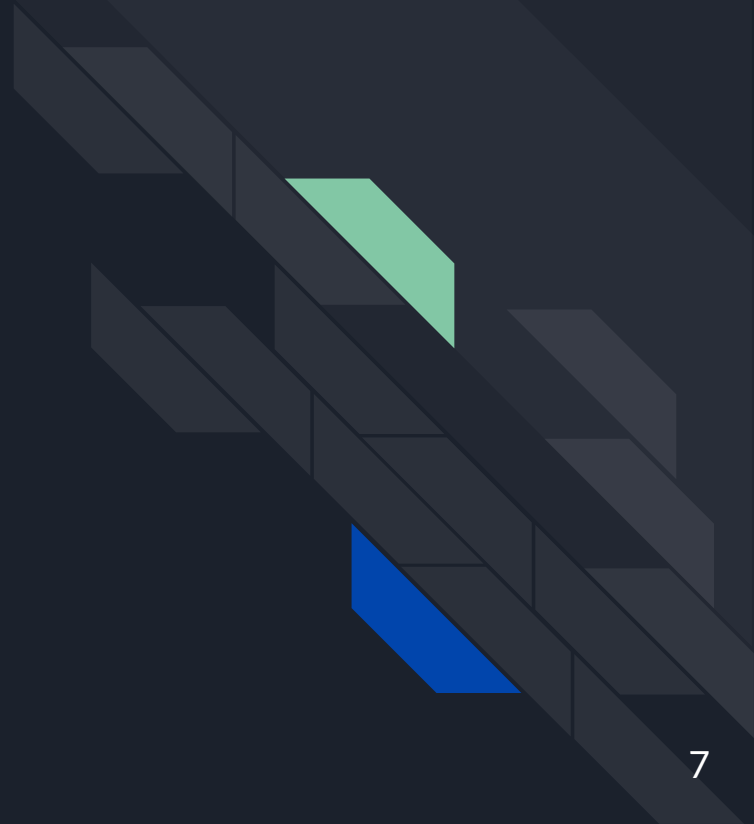
This key is shared between parties on the quantum network

How does QKD handle eavesdropping?

Any attempt by Eve to measure the key will inherently affect the quantum system and alert Alice and Bob that someone is eavesdropping.



This all sounds great...so
then what's the problem?





QKD is still vulnerable to quantum hacking...

The equipment used to generate the key could be targeted:

- Random Number Generator Attack
- Trojan Horse Attack

My article announces the development of a cost-effective measurement-device-independent quantum key distribution system.

Related QKD Networks

Major quantum network projects and QKD protocols implemented						
Quantum network	Start	BB84	BBM92	E91	DPS	COW
DARPA QKD 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 Wuho, China	2009	Yes	No	No	No	No
Geneva area network (SwissQuantum)	2010	Yes	No	No	No	Yes

Source: https://en.wikipedia.org/wiki/Quantum_network

To date, there is no network connecting quantum processors that exists outside of the lab.[2]

Different protocols take advantage of different properties of quantum mechanics to accomplish the same general objective




Related Devices

Vulnerabilities in quantum key distribution systems have been recognized for awhile and potential solutions were found in:

Potential solutions were found in:

- Device-Independent QKD
- Semi-Device Independent QKD
- One-Sided Device Independent QKD

The best balance of practicality and performance was realized in
measurement-device-independent QKD



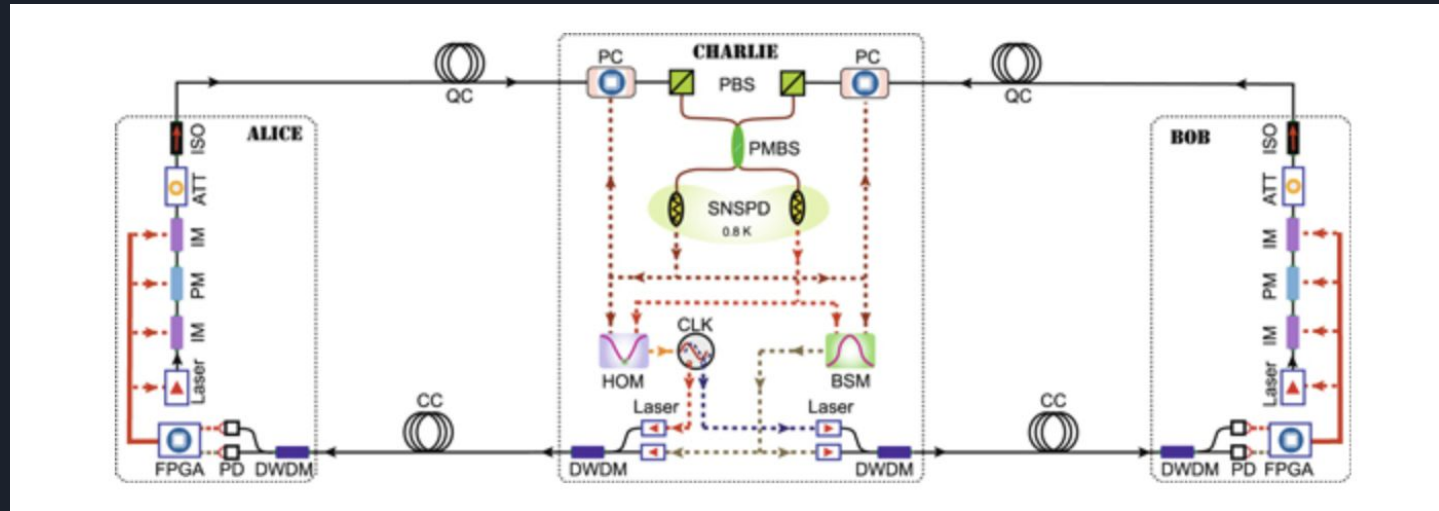
A cost-effective measurement-device-independent quantum key distribution system for quantum networks

Published in Quantum Science and Technology, Volume 2, Number 4

Main Idea: This measurement-device-independent QKD system relies on commercially available hardware such as distributed feedback lasers and field-programmable gate arrays.

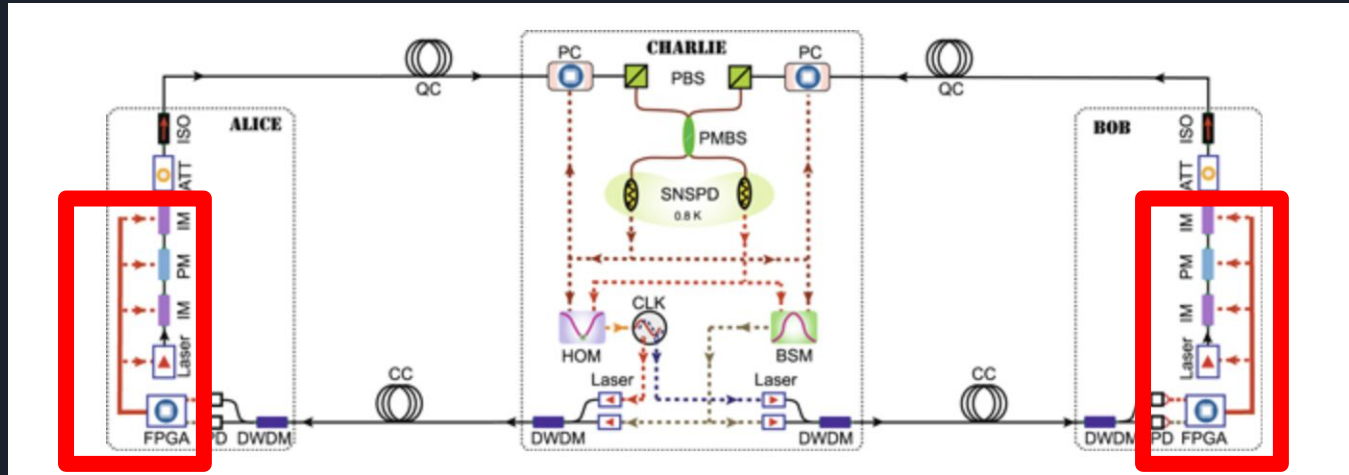
Components

1. Qubit preparation module
2. Control Modules
3. BSM Module
4. Time-tagging modules



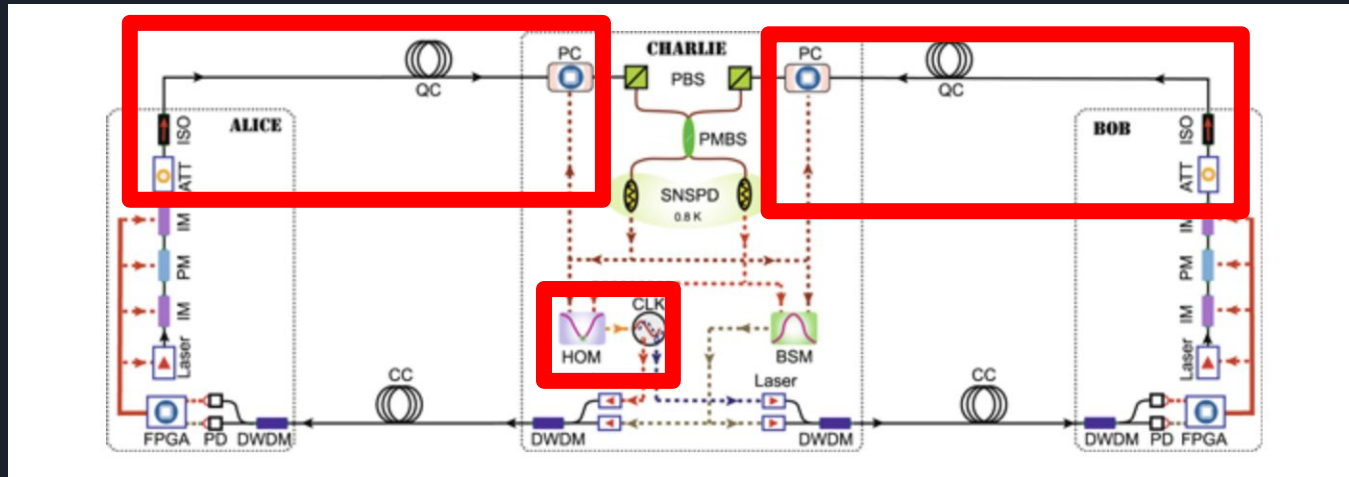
Qubit Preparation Module

- Uses random values on FPGA board to produce laser bursts that are modified by the phase modulator (PM) and intensity modulator (IM) to generate qubits
- Several protections against potential quantum hacking:
 - Optic Isolator on laser protects against Trojan Horse Attack
 - Phase modulation protects against unambiguous state discrimination



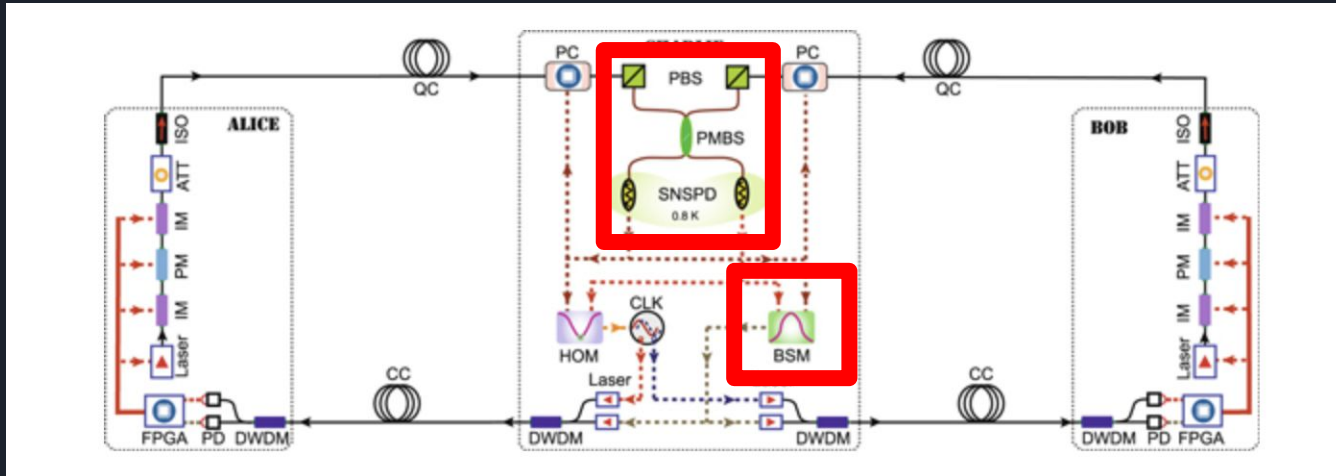
Control Modules

- In order for Charlie to function properly, we need stabilization of photons emitted by the lasers in all degrees of freedom (spatial, temporal, polarization, and spectral degrees)
- Feedback module allows for efficient key distribution, since they are not distributed at the same time that the feedback happens



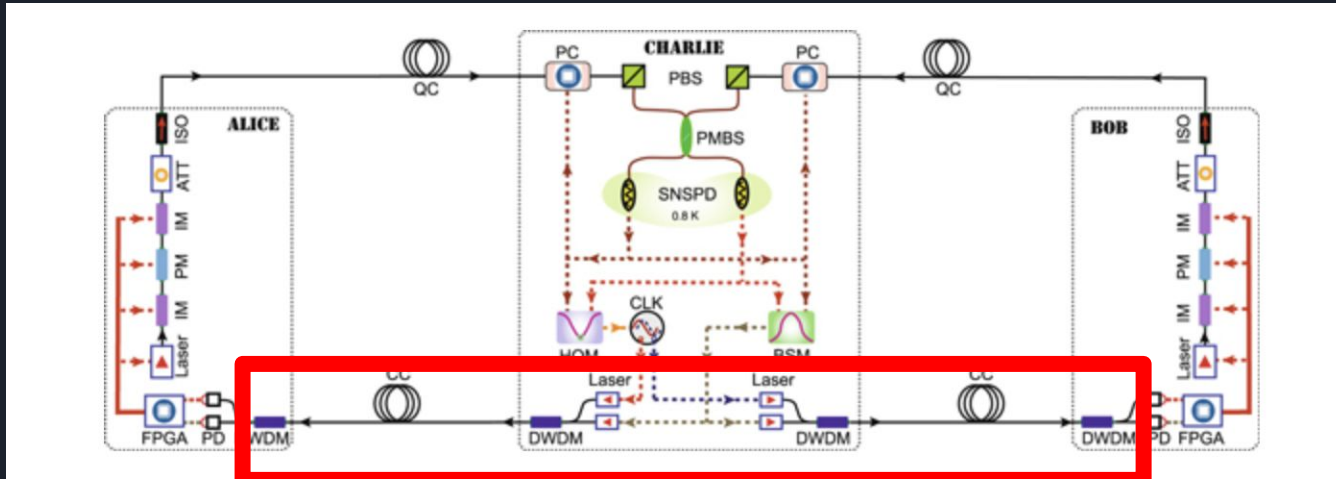
BSM Module

- The two photons are combined at the polarization maintaining beam splitter (PMBS)
- Produces a key based on projections onto a specific bases used in quantum mechanics called the Bell State



Time-tagging Modules

- Records Alice and Bob's qubit preparations and outputs from the BSM Module
- Knowing this information allows us to discern the properties of the two photons that were combined in the PMBS
- Detects eavesdropping and/or secure key generation





Goals and Challenges

Goals:

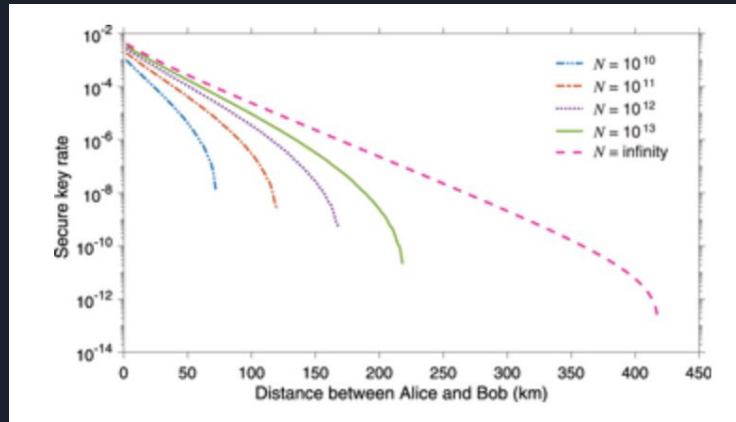
- A QKD that is secure from most forms of quantum hacking
- Provide a cost-effective system without sacrificing performance
- Ability to perform accurately over long distances

Challenges:

- Multitudes of quantum hacking strategies already exist and are quite robust
- Physical systems are less ideal than theoretical systems
- Quantum mechanics is HARD

Results

- N = # of pairs of qubits emitted by Alice and Bob
- We can see that the secure key rate is very low; however, this clock runs at 20MHz so it takes ~ 1.4 hours for $N=10^{13}$ at a distance of close to 200km
- Researchers note that advancements in quantum processing could increase this speed by over 100x if the clock speed could be increased to 2 GHz





Implications

Specific:

- Demonstrated cost-effective implementation of quantum key distribution system, that works over long distances
- Shown minimal impact on performance from using readily available components

Broad:

- Reliable quantum key distribution systems could provide secure information transfer for financial transactions, nuclear launch codes, medical records, etc.



Impressions

- Reiterate: Quantum computing is HARD; Chemistry is scary
- I mainly found the cryptographic aspects more interesting than the quantum computing
- Applications are widespread—privacy is important to everyone
- I'm excited to see where this new technology heads in the future
- I would consider studying cryptography and quantum computing in the future



Sources

[1] “Quantum key distribution.” *Wikipedia*, Wikimedia Foundation, 26 Oct. 2017, en.wikipedia.org/wiki/Quantum_key_distribution.

[2] “Quantum network.” *Wikipedia*, Wikimedia Foundation, 29 Oct. 2017, en.wikipedia.org/wiki/Quantum_network.

[3] IOPPublishing. “Cost effective quantum moves a step closer.” *EurekAlert!*, www.eurekalert.org/pub_releases/2017-09/ip-ceq091817.php.

[4] Raju Valivarthi et al 2017 *Quantum Sci. Technol.* 2 04LT01