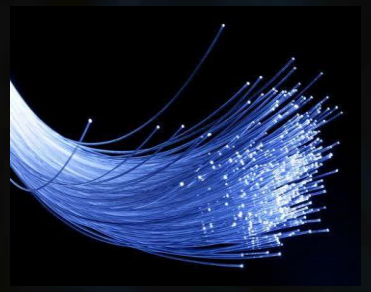
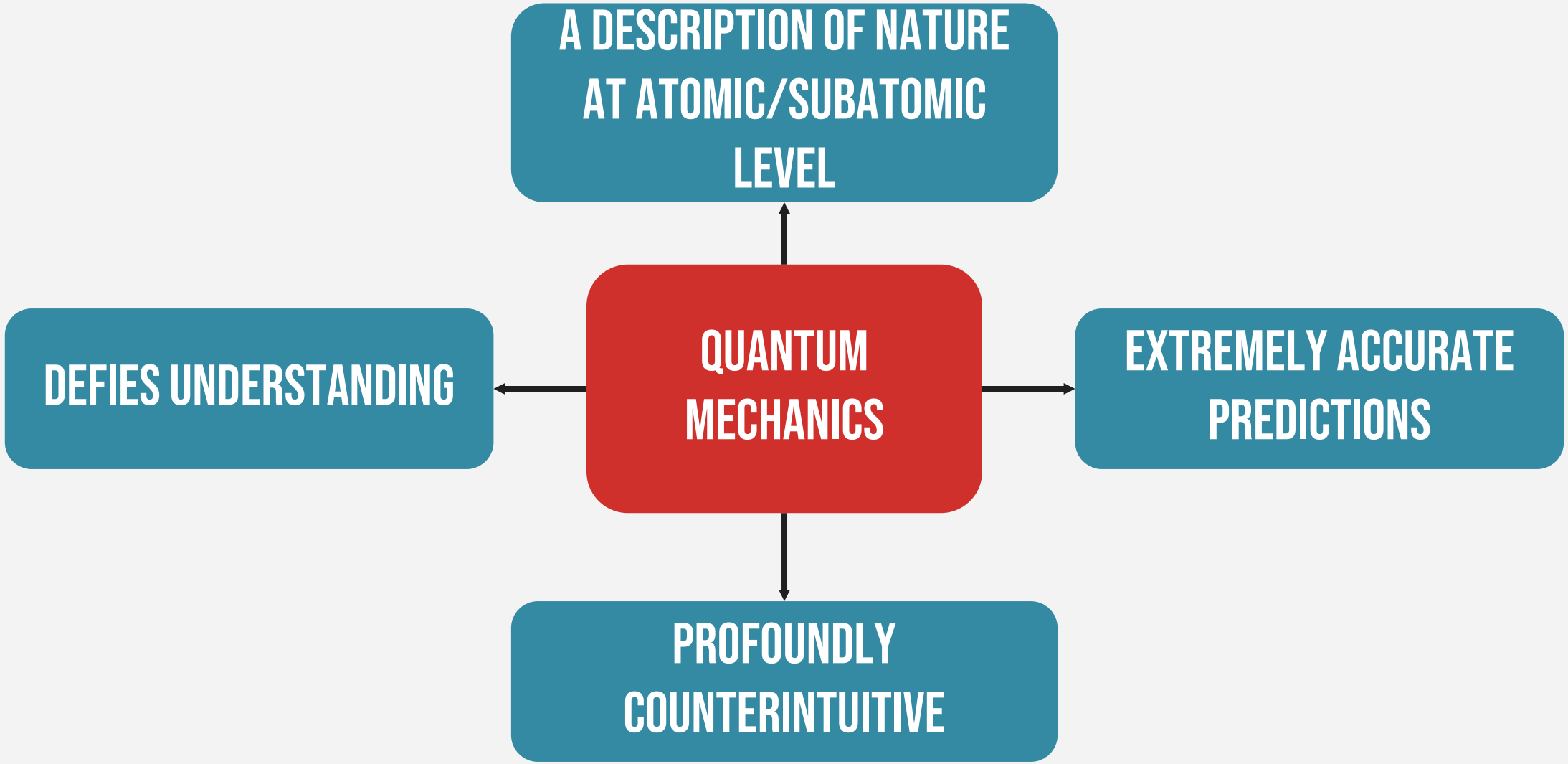
The Quantum and the Social

Bernardo A. Huberman




A DESCRIPTION OF NATURE AT ATOMIC/SUBATOMIC LEVEL
DEFIES UNDERSTANDING
QUANTUM MECHANICS
EXTREMELY ACCURATE PREDICTIONS
PROFOUNDLY COUNTERINTUITIVE

Remarkable Facts about Quantum Physics

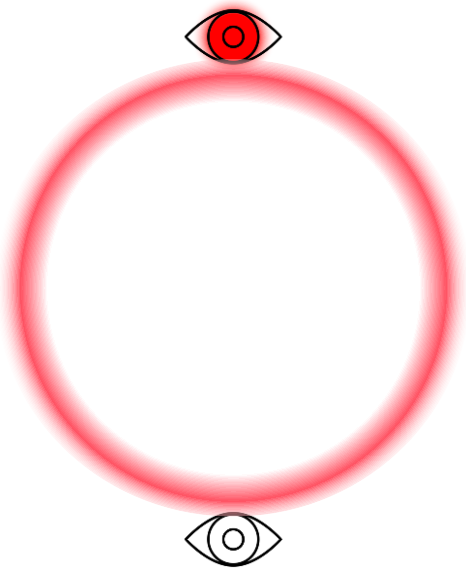
Superposition

- A system can be in many states simultaneously before it is measured (example: light is both particle and wave).

Very counter intuitive

A Spooky Phenomenon

Bob

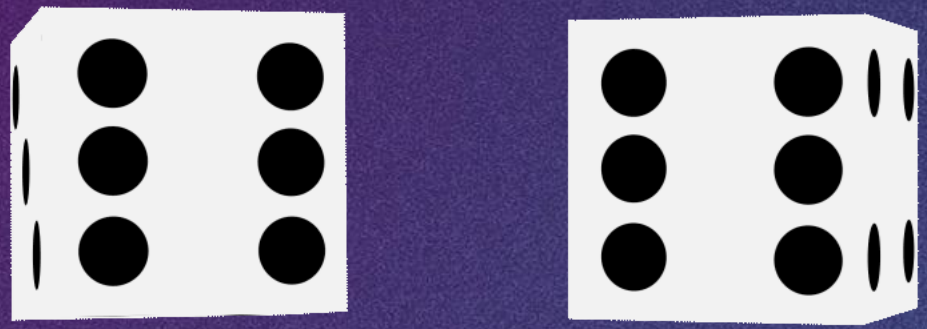


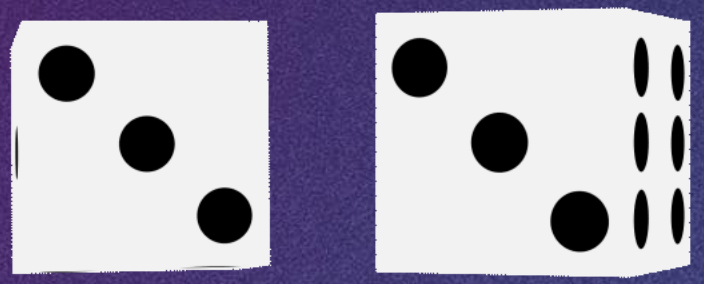
Alice

Another Spooky Phenomenon: Entanglement

Separate entities can be correlated and ‘interact instantaneously” over arbitrary distances

Another Spooky Phenomenon: Entanglement





Practical Implications

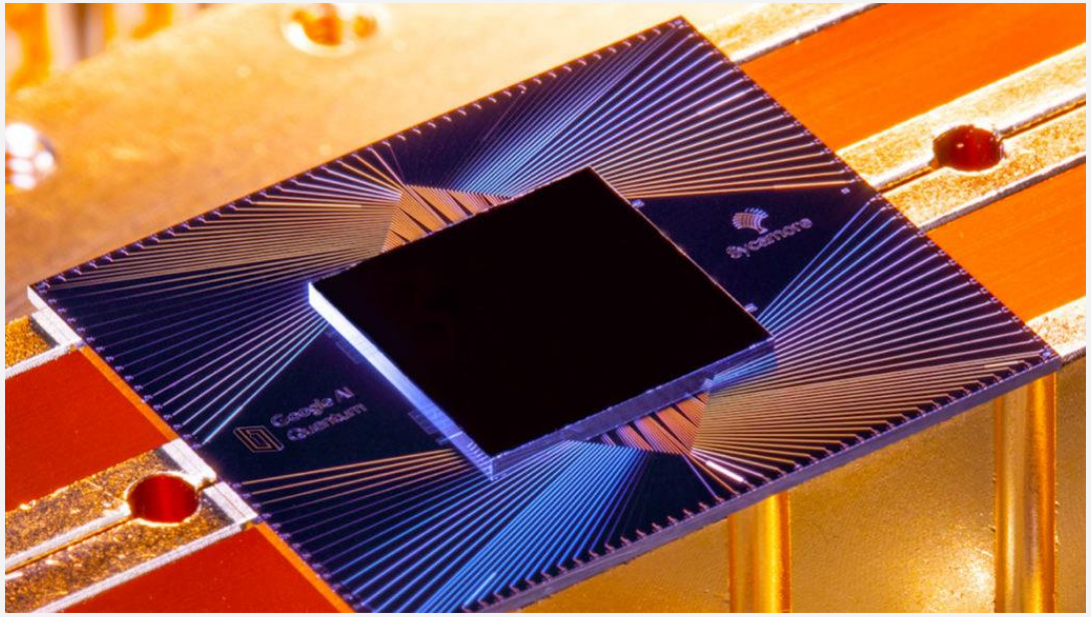
Computing

- With the qubit as unit of information instead of the bit, a quantum computer will swiftly solve very hard problems by running simultaneously all possible scenarios.

Networks and Information

- It makes super secure communications possible, solves coordination problems, can run truly private auctions, and makes possible provable secure voting.

Quantum Computing



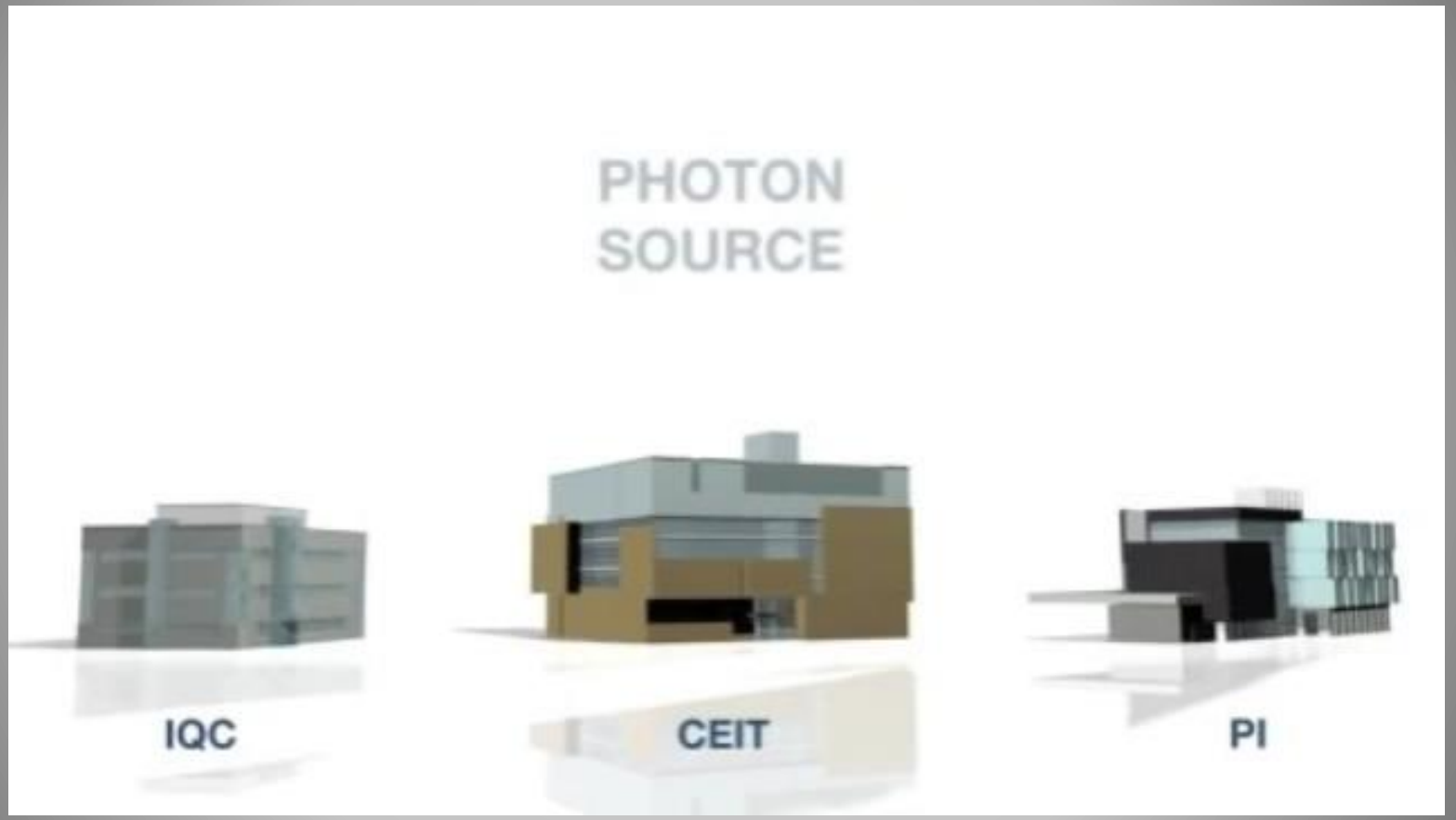
- Sycamore
- 200 sec vs 10K years

- Jiuzhang
- 200 sec vs half a billion years

Secure Communication Using Entanglement

CableLabs®

Schematic diagram



Video: University of Waterloo

The Social

What kind of interactions between individuals and institutions can be affected by quantum technologies?

Private exchanges, finance, coordination, voting, auctions.

All of these are now protected by public and private key encryptions.

What about coordination without communication?

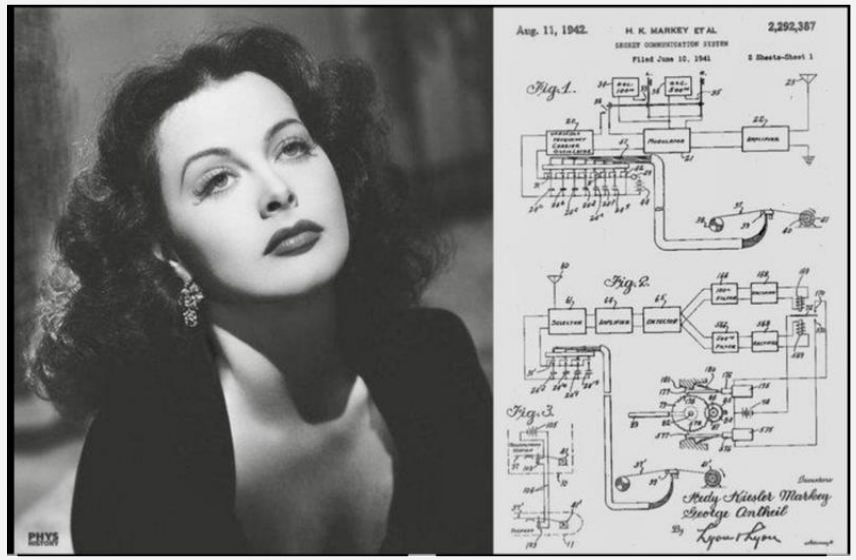
Impossible classically.

Spread-Spectrum Communication

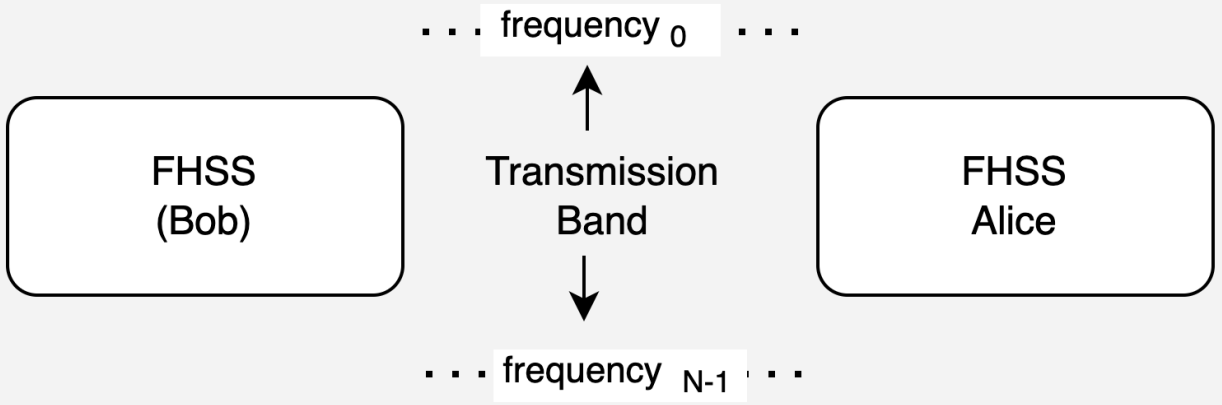
Reliable and secure wireless communication

- Dynamically switch carrier frequencies within a pre-designated band
- Mitigate narrowband interference
- Enhance resistance against interference and eavesdropping

H. Lamar and Antheil-1942



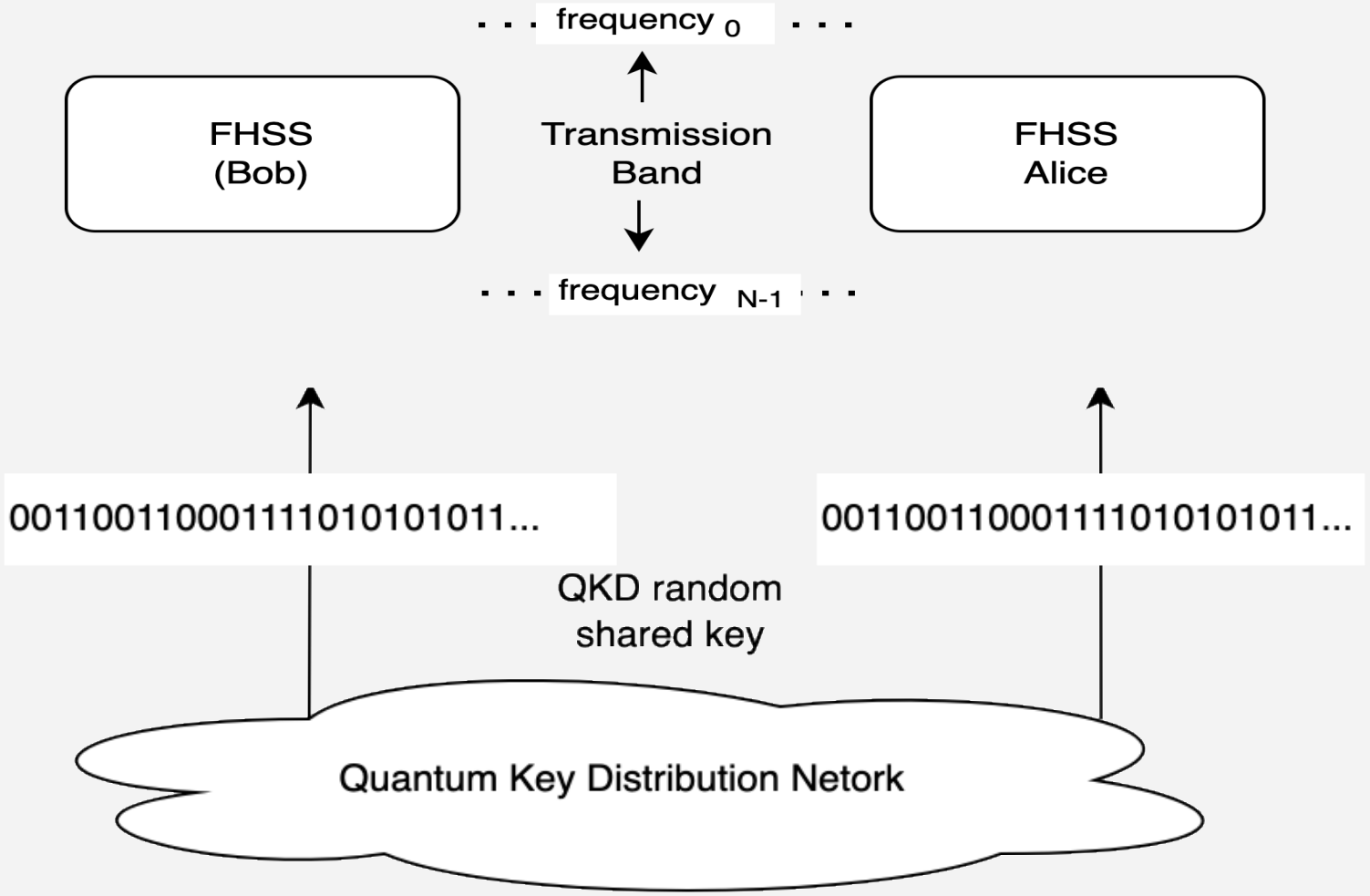
Spread Spectrum Commuinication



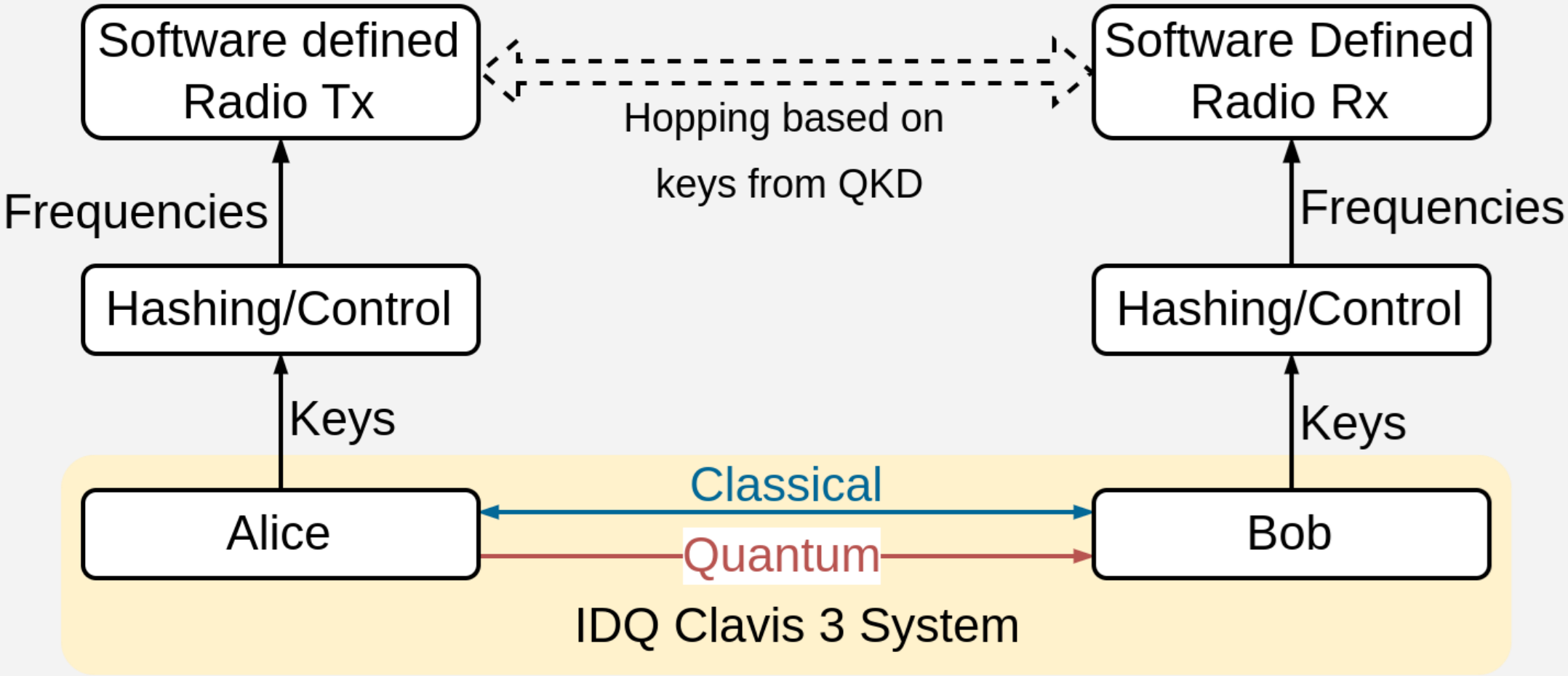
Two problems: 1. How do Bob and Alice coordinate the frequency sequence.
2. An eavesdropper can learn the sequence.

Answers: 1. Use quantum entanglement to coordinate.
2. Use quantum superposition to make the sequence truly random.

Quantum Solution



Quantum Spread Spectrum



Secure Multiparty Computation

Parts of the data belongs to multiple owners.

They collectively want to perform analytic studies on the entire dataset.

While respecting the privacy and security concerns of each individual party.

Example: average age or income

An initial ”leader” chooses a secret large number and forward it to the next person,

who adds his/her number to it, and passes it along to the next one.

And so on, until it gets back to the leader.

Then leader substracts from that large number the secret one, divides by the total number of people, and presto comes the average result from the aggregation of private data.

The individual transmissions are encrypted via a public key system

How secure is it?

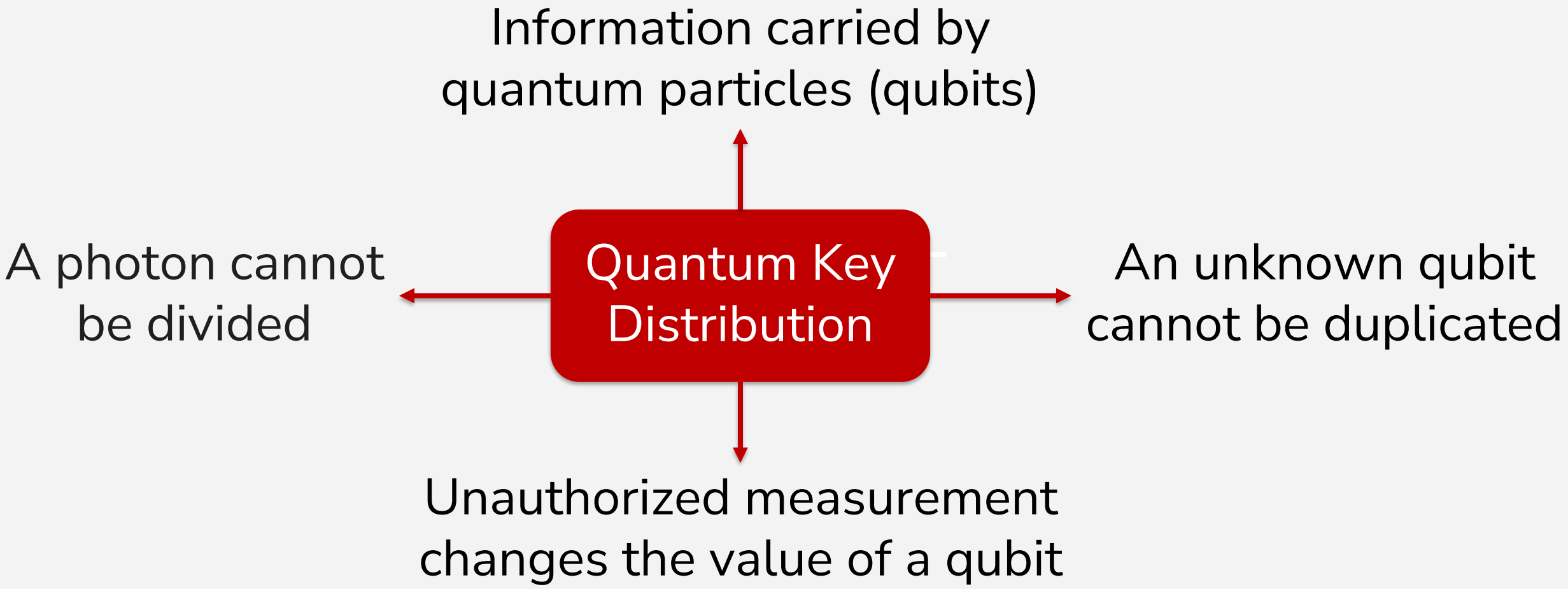
Security based on the intractability of the discrete logarithm.

Given integers *a* and *b* and prime *p*, it is computationally hard to find integer *x* such that,

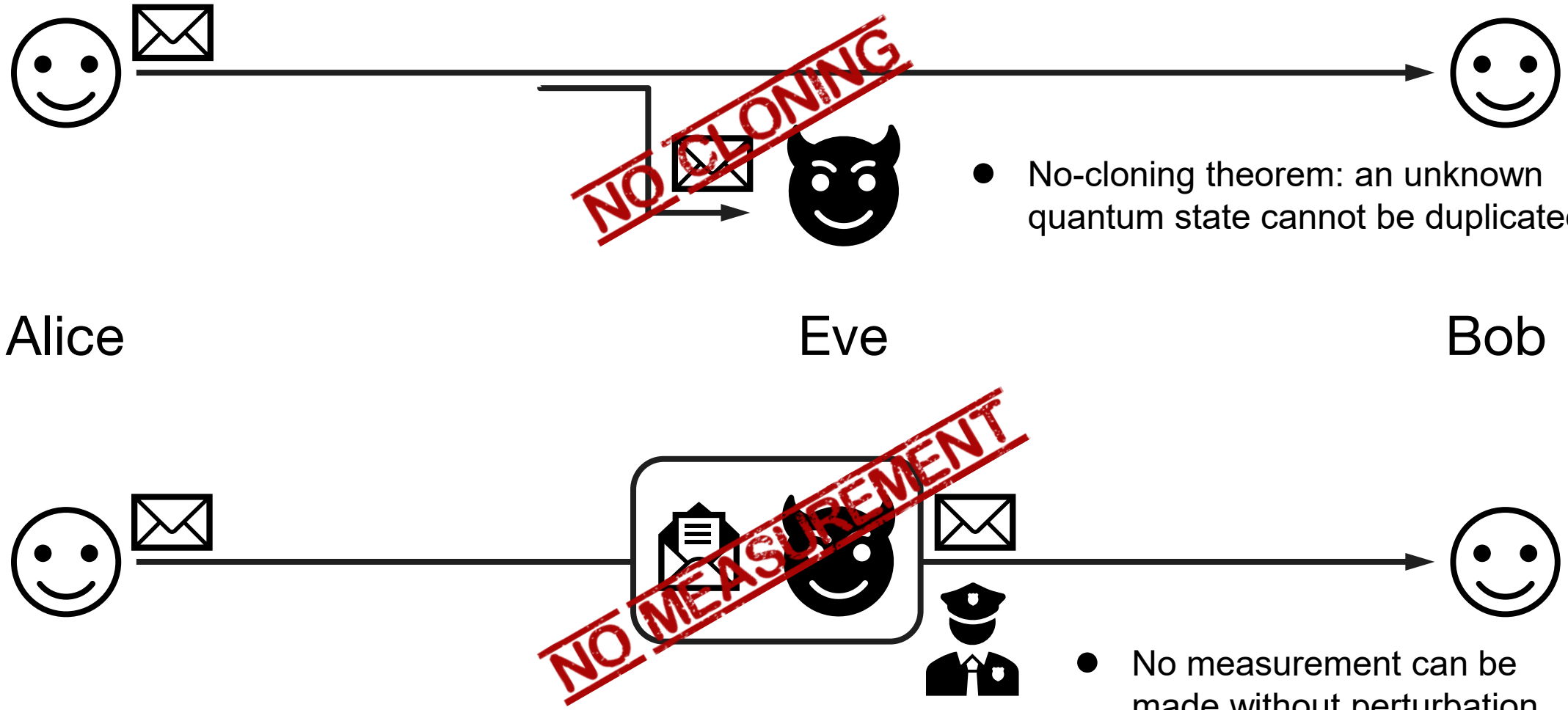
$$b^x = a \pmod{p}$$

But a quantum computer running Schor's algorithm can easily invert it.

Quantum Key Distribution is Absolutely Secure



Quantum Key Distribution



- No-cloning theorem: an unknown quantum state cannot be duplicated

- No measurement can be made without perturbation

Online Voting

There exist many schemes for online voting.

Required: completeness, privacy and fairness.

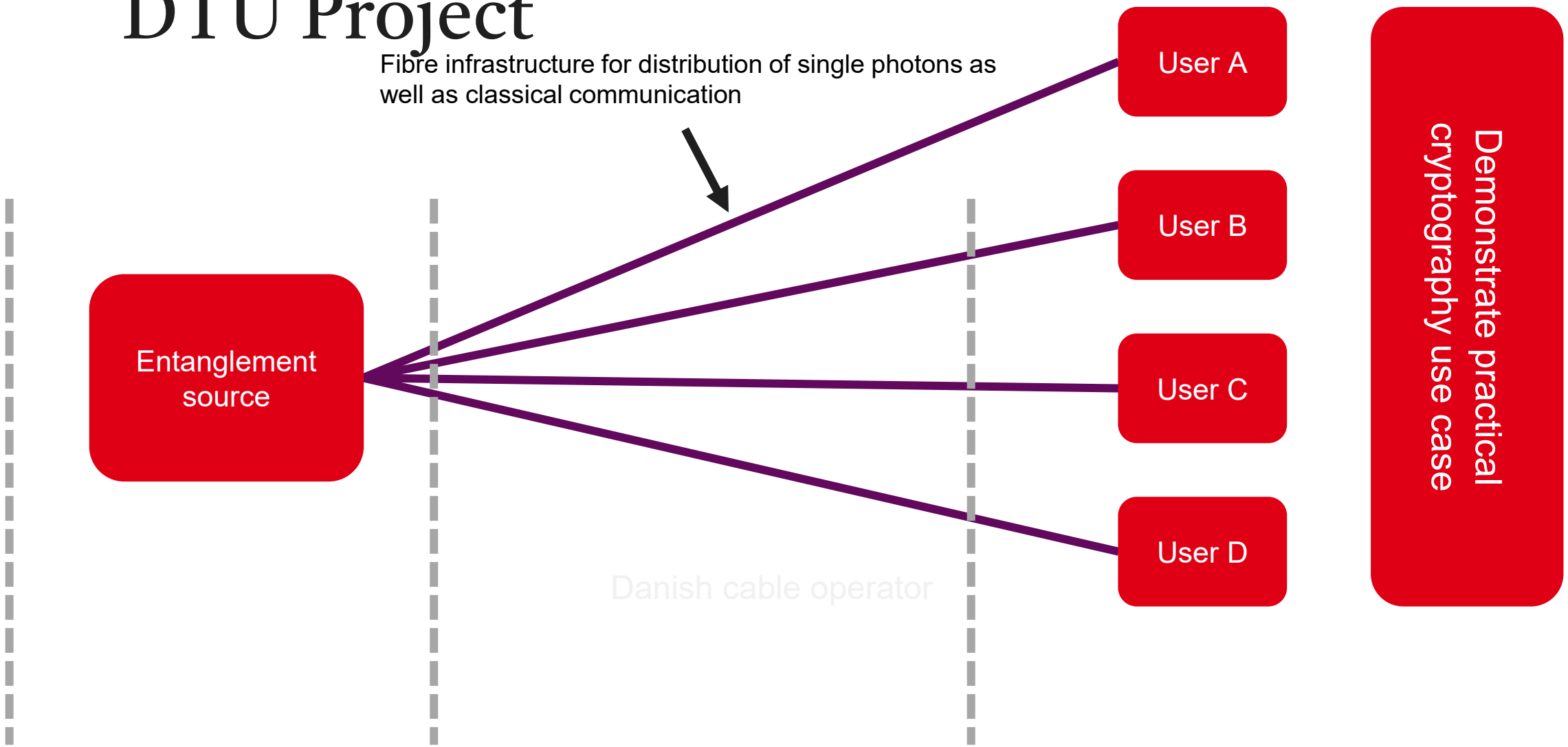
Many solutions exist, all based on public or private encryption.

Ripe for Quantum Key Distribution.

Fatal problem for QKD implementation:
pairs of keys needed between voter and tally service.

Solution: point to multipoint deployment of keys.

DTU Project


Fibre infrastructure for distribution of single photons as well as classical communication
Entanglement source
User A
User B
User C
User D
Demonstrate practical cryptography use case
Danish cable operator
Efficient generation of entangled photons
Transmission of entangled photons and coexistence with classical data traffic
Detection of photons and generation of secret keys

Concluding Remarks

However exotic, quantum information technologies are starting to be part of the landscape. And changing social interactions.

And the electronic membrane that LEO satellites have created over the earth are beaming entangled photons to earth (Misius, etc.)

While quantum computing is in the future, quantum networks are very real today.