Cost-effective quantum moves a step closer

Joel George

Transistors

- Transistor: switch that blocks current
- Transistors are approaching their physical limits in terms of size
- Quantum tunnelling interferes with atomic-sized transistors

Quantum Computing vs. Classical Computing

- 1 bit stores 0 or 1
- 1 qubit store 0, 1, or superposition of the two
- Gates output altered probabilities

Why is quantum computing important

- Won’t replace classical computing in most commercial fields soon
- Best applied in computation-heavy areas
    - Code cracking
    - Database searching
    - Simulations

Classical Cryptography vs. Quantum Computing

- Quantum computing can crack codes like passwords or symmetric keys in a timely manner
- Shor’s algorithm

Quantum Key Distribution

1. Alice generates randomly polarized photons.
2. Bob decrypts the photons randomly.
3. Bob publicly shares order of detectors with Alice.
4. Both throw out the values generated by mismatched detectors.
5. The remaining string of values is their secret key.

Theoretically ***unbreakable***

…in practice, hackable.

Measurement-device-independent QKD protocol

1. Alice and Bob generate random sequences of polarized photons.
2. These photons are sent to an *untrusted* central node owned by Charlie.
3. The control source outputs the relationship between each photon pairs.
4. For each successfully correlated photon pair, Alice and Bob share the basis used in polarizing that photon.
5. Alice and Bob only keep event records are only kept for photons with the same basis (i.e. photons with the same polarization/encoded bit).

Cost-effectiveness

-To sum it up, accessible and widely used equipment was function normally in an MDI-QKD system.

Why does any of this matter?

Why does any of this matter?

SECURITY.

Works Cited

1. Valivarthi, Raju, et al. “A Cost-Effective Measurement-Device-Independent Quantum Key Distribution System for Quantum Networks.” Quantum Science and Technology, vol. 2, no. 4, 2017, doi:10.1088/2058-9565/aa8790.

2. Merali, Zeeya. “Hackers Blind Quantum Cryptographers.” Nature, 2010, doi:10.1038/news.2010.436.

3. Lo, Hoi-Kwong, et al. “Measurement-Device-Independent Quantum Key Distribution.” Physical Review Letters, American Physical Society, 30 Mar. 2012, doi.org/10.1103/PhysRevLett.108.130503.

4. Diamanti, Eleni, et al. “Practical Challenges in Quantum Key Distribution.” Npj Quantum Information, vol. 2, no. 1, 2016, doi:10.1038/npjqi.2016.25.