Enhanced Cryptography through Quantum Key Distribution and Satellites: The BB84 Protocol

Xiaoya Gao, Avni Iyer

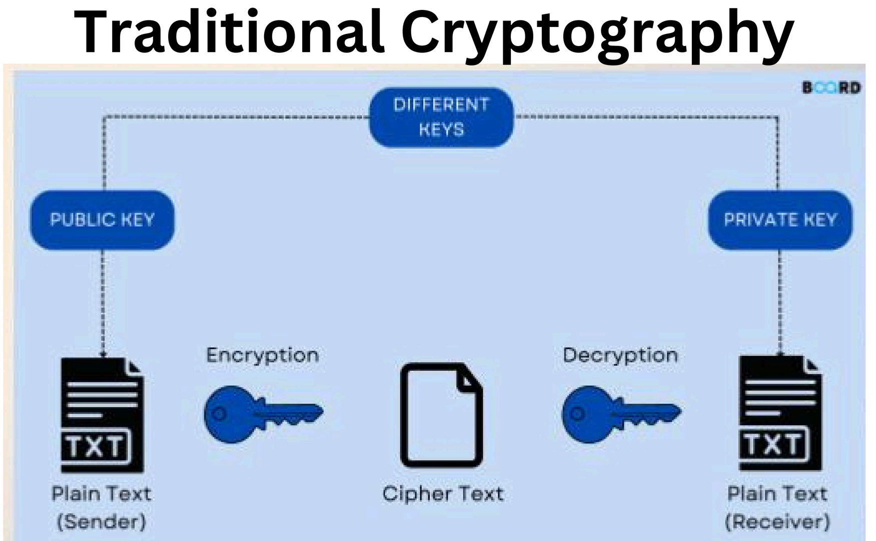
Abstract: Today, government and military units rely on satellites to transmit sensitive data. However, the rise in computational power of quantum computers poses a significant threat to traditional cybersecurity algorithms, rendering them highly susceptible to attacks. Quantum Key Distribution (QKD) offers a promising solution by using principles of quantum mechanics such as superposition and the uncertainty principle to eliminate mathematical algorithms, thus increasing eavesdropping detection accuracy drastically. Utilizing QKD for satellites in Low Earth Orbit is key for the future of our cybersecurity as they increase efficiency by eliminating fiber repeaters and establishing multiple connections through a single satellite. The BB84 protocol is a QKD single-photon based algorithm that solves the intercept-and-resend attacks that are commonly employed by hackers. Through this study, we use three Python 3.12 simulations to explore the shortcomings of current BB84 protocol approaches for satellite applications. Furthermore, we illustrate why privacy amplification and error channel connections are essential for total cybersecurity.

1 | Background

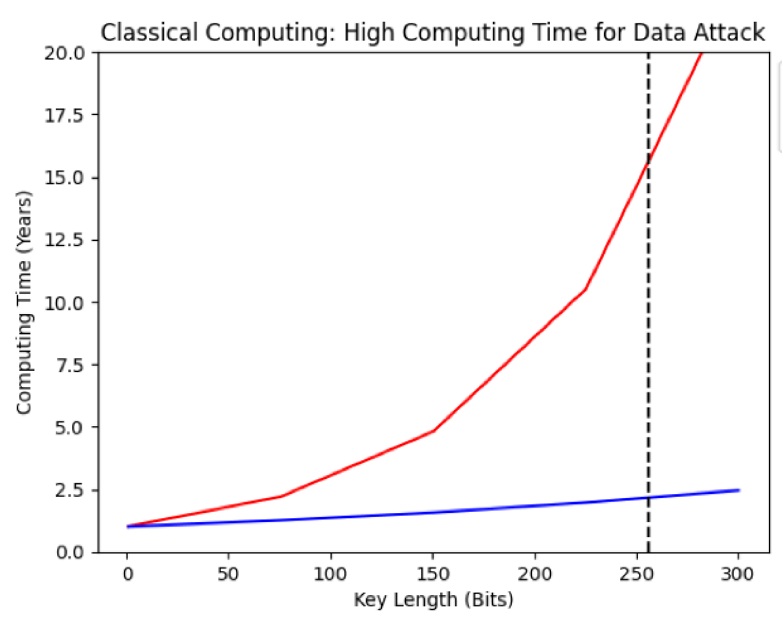
A traditional Algorithm: AES-256

- **128 bits divided into blocks, uses symmetric keys[7]**
- **Considered unbreakable: used by government and military[14]**
  - **Often implemented in satellites[4]**
- **Traditional computers need billions of years to break[1]**

Traditional Cryptography



Classic cryptography mathematically encodes and decodes messages[6]



The Quantum Threat:

While a classical computer would take around 18 years to break AES-256, a quantum computer will be able to in minutes.[7]

- **Quantum computers have high computational power[14]**
  - **Utilizes quantum mechanic properties[14]**
- **By 2050, they could break encryption within minutes[7]**

2 | Quantum Key Distribution: The BB84 Protocol (Bennett-Brassard 1984)

- **Solves the intercept-resend attack method (man in the middle)**
- **Qubits sent through fiber cables as photons between Alice & Bob**

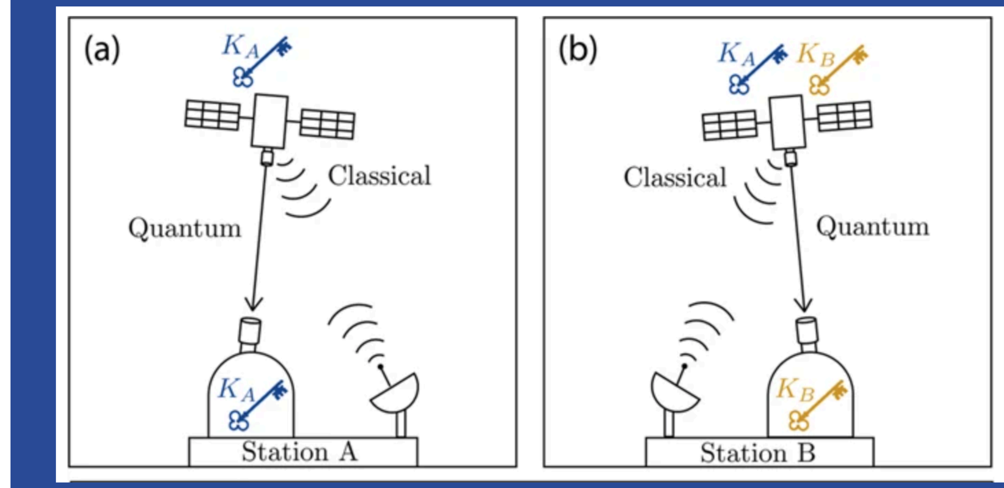
Classical	**Quantum**
• Bits are 0 *or* 1 • Measure momentum and position • Mathematical algorithms are keys	• Qubits are 0 *and* 1 until measured • Once measured by eavesdropper, photon state changes • Matching polarization of photons becomes key

Alice random bits	0	1	1	0	1	0	0	1
Alice sending Basis	+	×	+	×	×	+	×	+
Alice polarization	→	↖	↑	↗	↖	→	↗	↑
Eve basis measurement	+	+	×	×	+	×	×	+
Polarization Eve measures and sends	→	→	↗	↗	↑	↗	↗	↑
Bob basis measurement	+	×	×	×	+	×	+	+
Polarization Bob measures	→	↗	↗	↗	↑	↗	→	↑
Shared secret key	0	0	-	0	-	-	-	1
Error generated	√	x		√				√

A graphical representation of an encrypted conversation between Alice and Bob[2]

- **Low-Density Parity-Check (LDPC): an error correction method that compares receiver's and sender's bits and reduce error due to noise[5]**
- **Privacy Amplification: reduces information access to eavesdopper by converting key to a hash[11]**

3 | Satellites Application

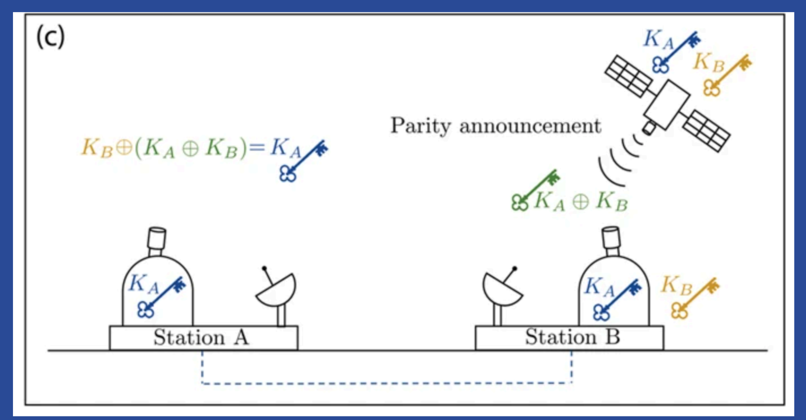


Current Challenges

- **Channel errors with the bouncing of photons[14]**
- **Satellites are currently unable to produce information carrying coherent photons[14]**
- **Atmospheric changes can affect QKD transmission[8]**

Why Satellites?

- **Better data security[4]**
- **Better infrastructure setup**
- **Lowers cost and security risks[14]**
- **Can establish multiple connections through one satellite[14]**
- **Eliminates risk of tampering[4]**
- **Eliminates usage of fiber repeaters[14]**



A visualization of satellite QKD[3]

4 | Methods + Results

Using Python 3.12, we simulated superposition and matrix operations for the BB84 Protocol 3 times, each with a background noise error of 0.5% .

Without error correction, background noise and eavesdropping-induced error are indistinguishable: both are close to 5.5% within two tenths.

LDPC is essential to make the noise error null and actually detect for eavesdropping.

Simulation Number	Eavesdropping simulated?	Error correction method (LDPC)?	Error (mismatch between Alice and Bob's bits)
1			5.54%
2	✓		5.66%
3		✓	0.00%

Privacy Amplification further increases the error threshold by 3.5%:[14]

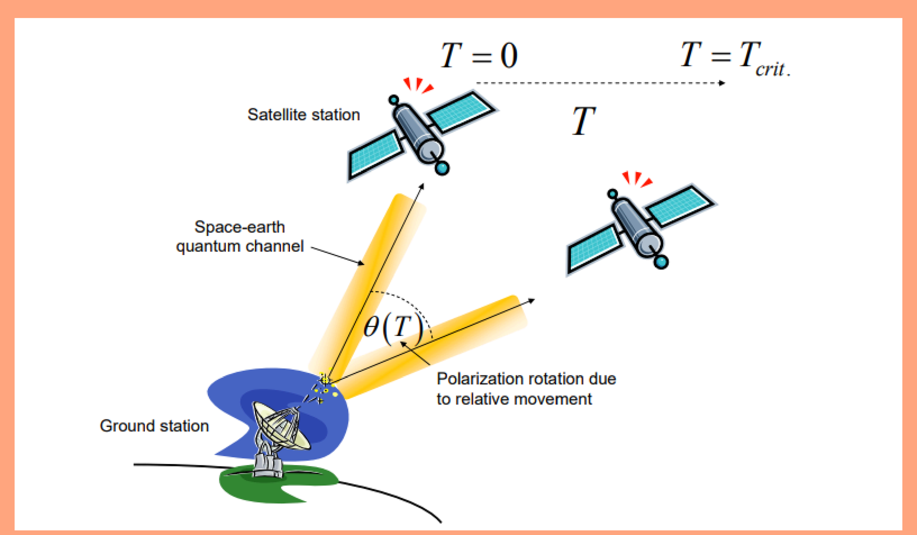
```
Final Key:
6d86701d08b4ceab2f98595358c31705ba0231cd592d865d4cf02095b3d9cc05
```

5 | Summary

- **Quantum computers will soon be able to hack traditionally unbreakable algorithms in minutes, but Quantum Key Distribution allows for increased security**
- **Satellites are the future of QKD**
- **The BB84 protocol significantly increases the probability of detecting an eavesdropper**
- **Without error corrections and privacy amplification, the BB84 protocol becomes useless as background noise contributes heavily to error**

6 | Future Directions

- **Advanced forms of error detection: ensuring that computational costs do not outweigh benefits**
  - **Pilot quantum error detection allows for the receiver to adjust based on errors in data transmission, but is computaitonally expensive**
  - **Important for satellites: light polarization affected by atmosphere[8]:**



Photons' polarization is changed by the atmosphere, causing a need for more advanced error correction methods like pilot qubits[8]

References

1. **AppSealing. *Understanding AES-128 encryption and its significance in the current threat landscape*. AppSealing. https://www.appsealing.com/aes-128-encryption/#:~:text=If%20you%20ask%20how%20long,a%20128%2Dbit%20AES%20key.**
2. ***BB84 Protocol Alice choice to Bob*. Quantum Computing Stack Exchange. https://quantumcomputing.stackexchange.com/questions/2172/bb84-protocol-alice-choice-to-bob.**
3. **Bedington, R.; Arrazola, J. M.; Ling, A. Progress in satellite quantum key distribution. *Npj Quantum Information* 2017, 3 (1). https://doi.org/10.1038/s41534-017-0031-5.**

Scan for full list of references: