Gokhale Education Society's

R. H. Sapat College of Engineering, Management Studies and Research,

Nashik - 422 005, (M.S.), INDIA

Seminar on,

Quantum Cryptography for UAV Communication

In partial fulfillment of requirements for the degree
Third Year Computer Engineering

By
Kasturi Mahesh Shirole
Roll No. : 53

Under the guidance of
Mrs. V.S.Nikam

INDEX

Introduction

Introduction to Quantum Cryptography.

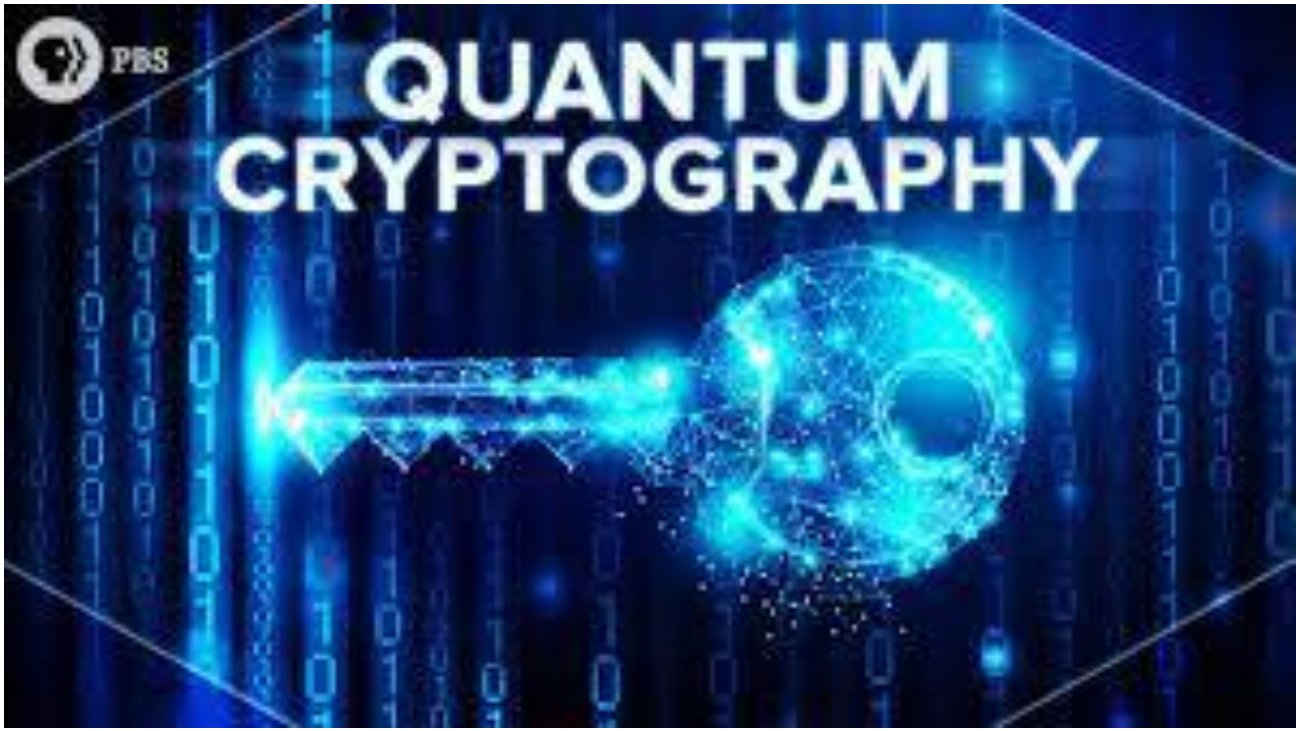
Quantum cryptography is a technique of cryptographic operations that makes use of the quantum mechanical phenomenon.

- **Quantum Key Distribution (QKD):** This is a central technique in quantum cryptography that addresses the problem of securely exchanging cryptographic keys.

- **Data Non-Copyability**: Quantum states cannot be copied due to the no-cloning theorem.

- **<u>Contribution of Gilles Brassard and Steven Wiesner</u>**: They played a significant role in the development of quantum key distributions. Wiesner introduced the theory of quantum conjugate coding.

- **<u>Creation of BB84 Protocol:</u>** Bennett and Brassard developed the BB84 protocol in 1984, which became a cornerstone in dynamic communication devices.



Literature Survey

Name Of Authors	Year	Contribution
N. Neji and T. Mostfa.	Jun. 2019	‘‘Communication technology for unmanned aerial vehicles: A qualitative assessment and application to precision agriculture’’
C.-Y. Chen, G.-J. Zeng, F.-J. Lin, Y.-H. Chou, and H.-C. Chao.	Sep. 2015	‘‘Quantum cryptography and its applications over the internet’’
R. Aggarwal, H. Sharma, and D. Gupta.	Apr. 2011	‘‘Analysis of various attacks over BB84 quantum key distribution protocol’’

ROLE OF UAV TECHNOLOGY

Agriculture

- Crop health monitoring
- Soil health assessment
- Improved resource utilisation

Forest and wildlife

- Wildlife conservation
- Managing human wildlife conflict
- Forest protection

Urban Development

- City survey
- Improved urban planning
- Project monitoring
- Project quality assessment

Healthcare

- Epidemic control
- Cleanliness & hygiene
- Healthcare delivery

Traffic Management

- Road surface condition monitoring
- Improve traffic management
- Traffic feedback

Homeland Security

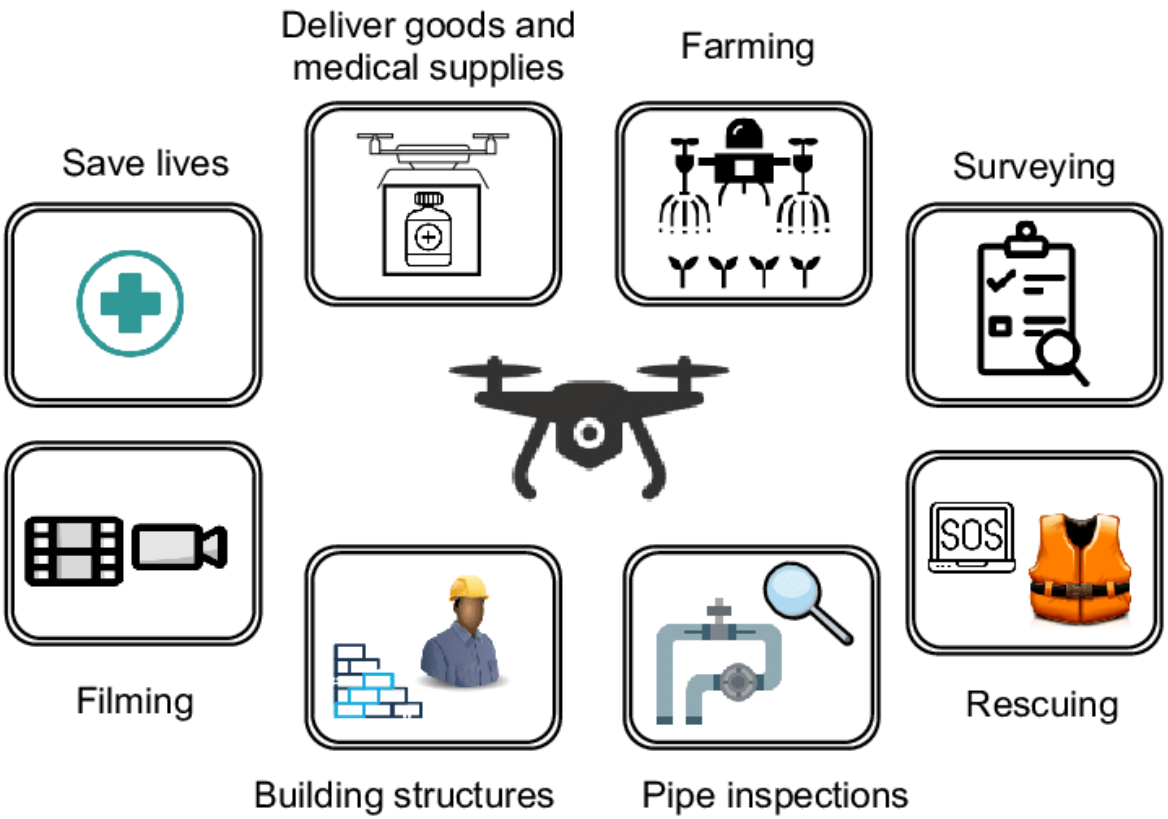
- Real time surveillance
- Security planning
- Drugs/Narcotics detection

Disaster Management

- Real time surveillance
- Search and rescue
- Delivery of essential goods

Mining

- Mineral scouting
- Managing encroachment
- Contract monitoring


Deliver goods and medical supplies
Farming
Save lives
Surveying
Filming
Rescuing
Building structures
Pipe inspections
SOS


Military and Law Enforcement
Photo and Video
Science Research
Goods Delivery
Tracking
Medical Equipment Delivery

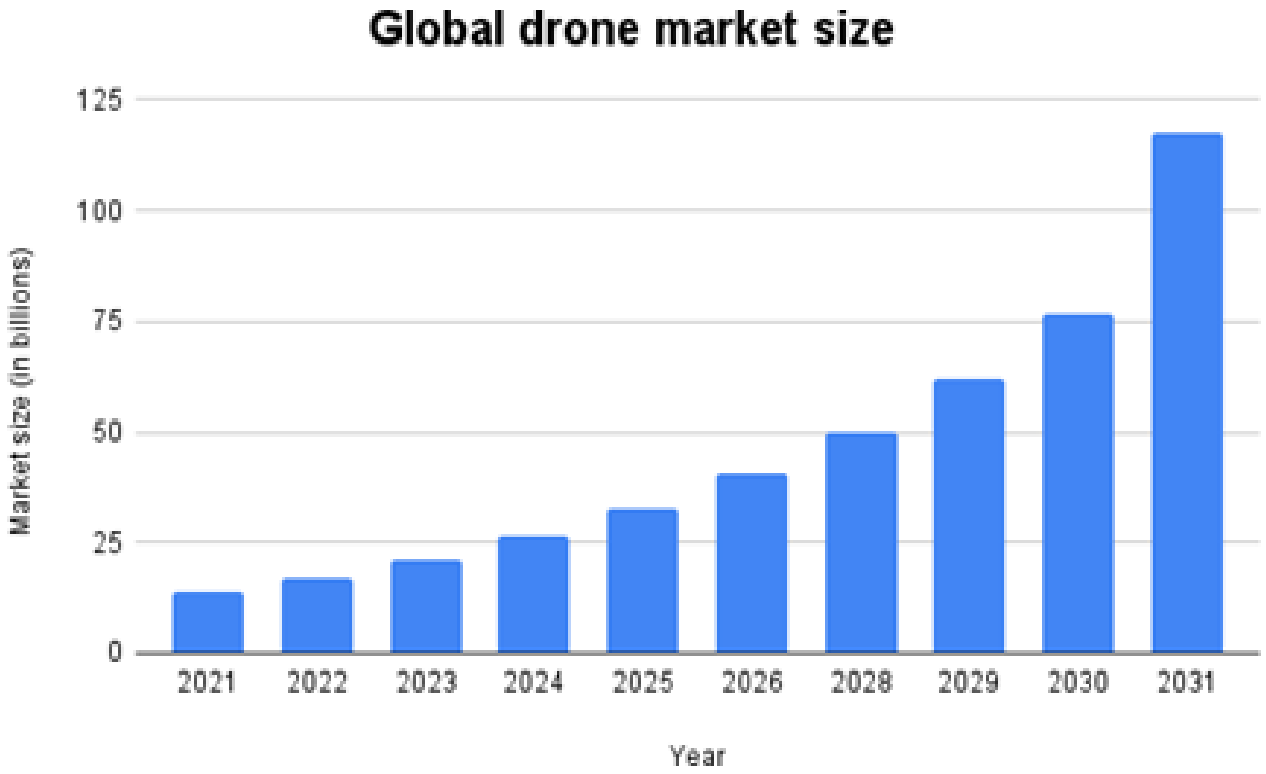


FIGURE 1. Market size of drones across the world

- The current market(2021) of drones across the world is 13.9 billion.

- As increasing UAV consumption, the data it carries becomes the nucleus for cyberattacks.

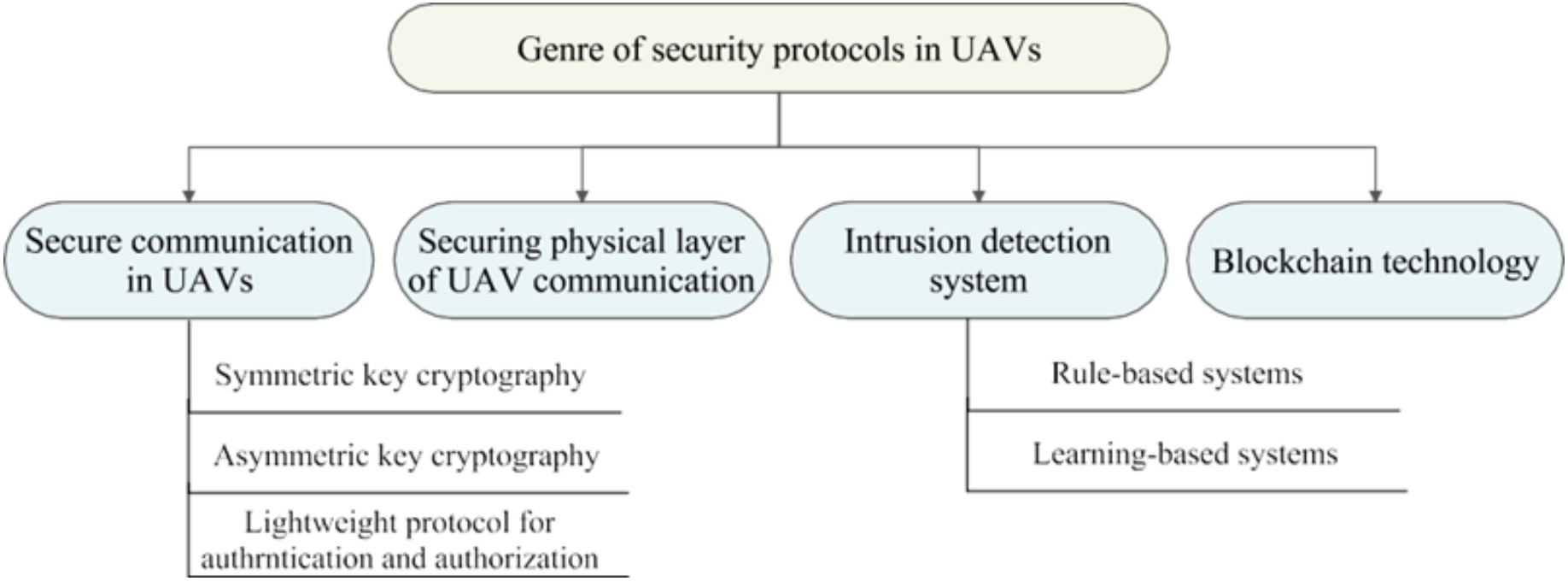


FIGURE 2. Various techniques to secure UAV communication

Unmanned Aerial Vehicle (UAV) Security:

- **Control Methods**: UAVs can be controlled through two primary methods: self-control and ground control channel (GCS).

- **Security Concerns in UAV Communication:** UAVs and Ground Control Stations (GCS) communicate through specific protocols like MAVLink , UranusLink, and UAVCAN

- **Vulnerabilities in UAV Communication:** Potential cyber-attacks, including eavesdropping and keylogging, threaten the integrity and privacy of UAV data.

- **Keyloggers and Privacy Concerns:** Keyloggers, software designed to record keystrokes, can compromise sensitive information transferred between UAVs. The lack of effective encryption standards can lead to unauthorized access to private data

- UAVs are vulnerable to cyber attacks, including **password theft**, **man-in-the-middle (MITM) attacks**, **denial of service (DoS) attacks**, **GPS jamming**, **spoofing**, and **open Wi-Fi vulnerabilities.**

- **Eavesdropping Attacks:** Eavesdropping involves unauthorized listening to transmissions, potentially allowing attackers to gain control over UAV communications.

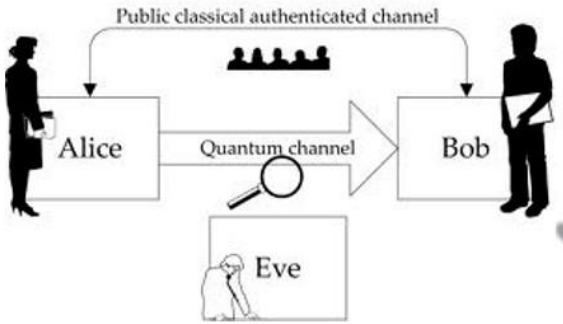
- **GPS Spoofing and Message Injection Risks:** GPS spoofing involves sending false GPS signals, which can lead to misguidance or capture of UAV nodes. Message injection attacks involve inserting pseudo-legitimate messages, potentially deceiving the UAV or ground station.

- **Message Deletion and Modification:** Attackers may attempt to manipulate messages to create false impressions of authenticity, affecting the communication link between UAV and GCS.

QUANTUM CRYPTOGRAPHY

Need of secure transmission between two parties

Confidentiality, integrity, availability and eavesdropper´s detectability is highly important for space communications.



Cryptography

Transmitted information is coded exchanging a randomly generated enciphering key between two parties through a non-secure channel.

Quantum Cryptography

New secure-communication technology used to implement space quantum communication protocols

Quantum key distribution (QKD)

CONCEPTS OF QUANTUM CRYPTOGRAPHY

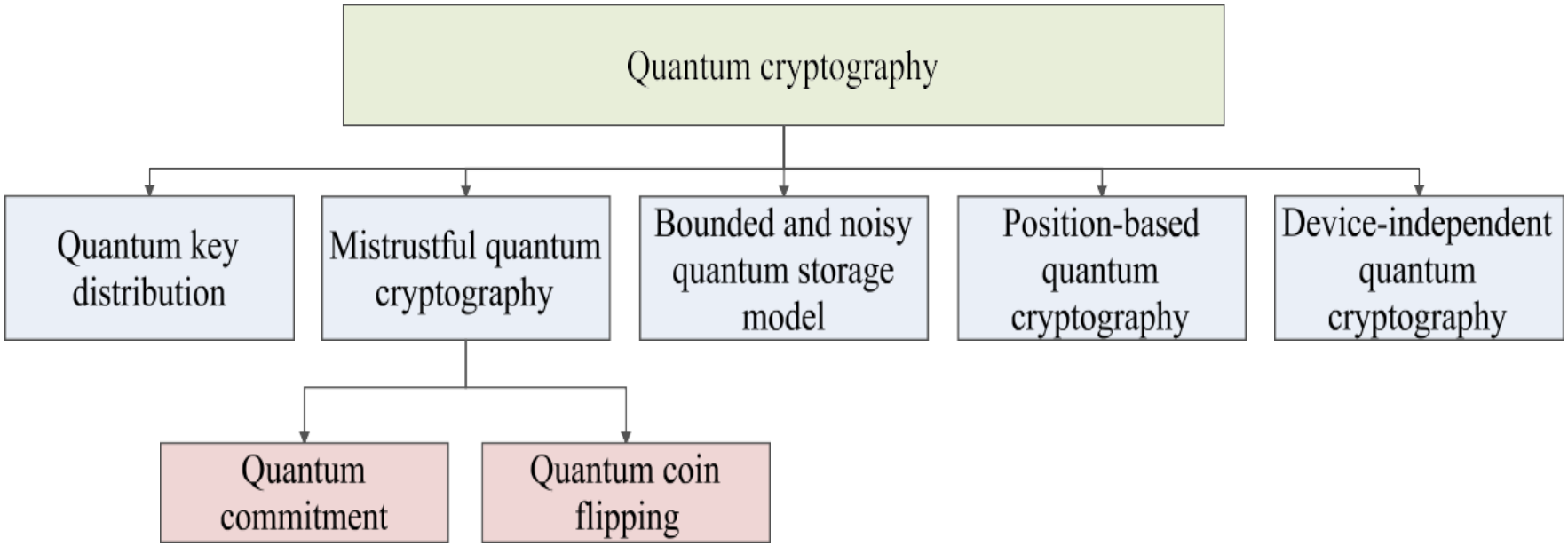
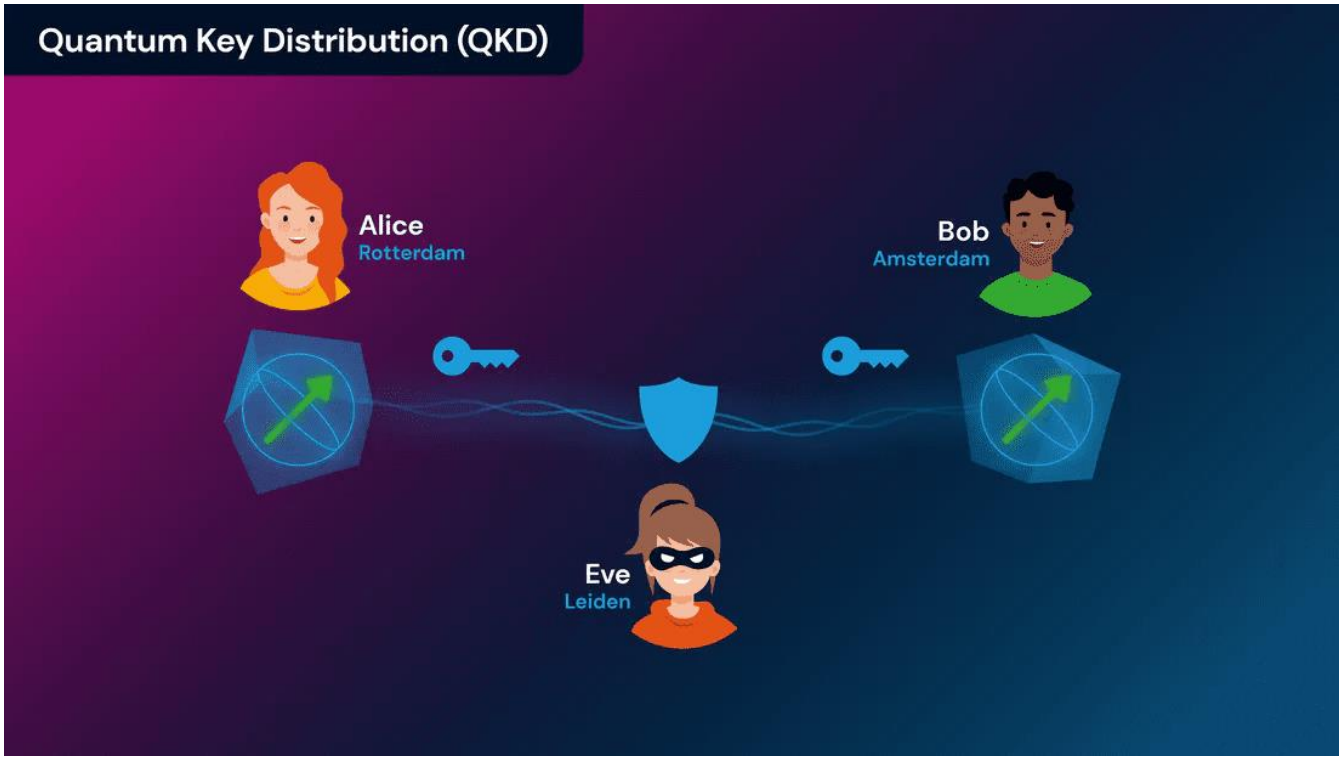


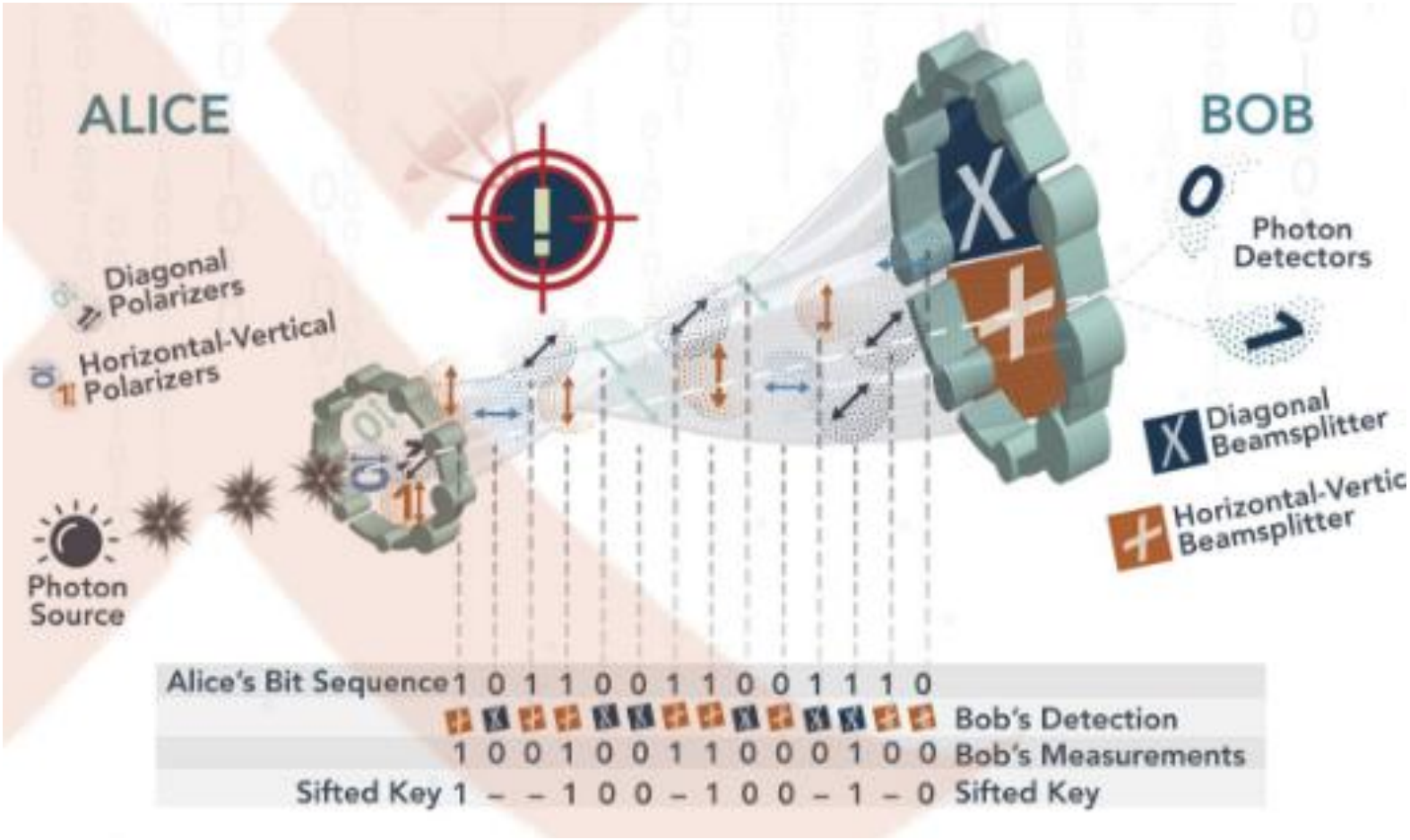
FIGURE 3. Diverse concepts of quantum cryptography

❖ Quantum Key Distribution (QKD)

- QKD establishes a public key between two parties using quantum communication, ensuring third parties cannot learn the key.

- Quantum states are disrupted if an eavesdropper attempts to intercept, allowing detection of intervention.




ALICE
BOB
Diagonal Polarizers
Horizontal-Vertical Polarizers
Photon Source
Photon Detectors
Diagonal Beamsplitter
Horizontal-Vertic Beamsplitter
Alice's Bit Sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's Detection
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's Measurements
Sifted Key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted Key

❖ Quantum Entanglement:

Quantum entanglement is a phenomenon observed at the subatomic level.
Where entangled particles remain connected in a way that actions on one particle affect the other, regardless of their distance.

❖ Quantum Superposition:

Quantum superposition is a fundamental concept in quantum theory, stating that two or more valid quantum states can be combined (superposed) to generate another valid quantum state.
In quantum computing, a qubit can be in a superposition of 0 and 1, allowing for simultaneous computation in both states.

THE PROPOSED QUANTUM CRYPTOGRAPHY-BASED SOLUTION

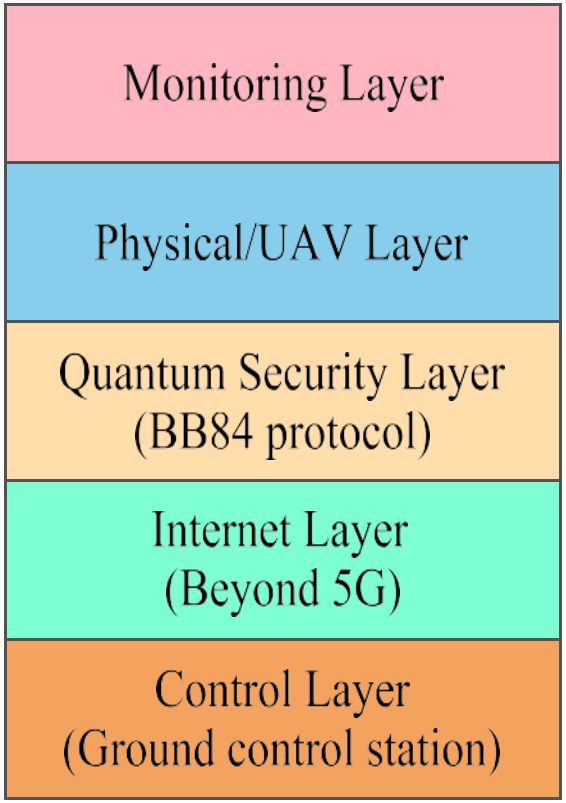


FIGURE 5. The proposed layered architecture.

A. Monitoring Layer:

- Focuses on capturing data from various designated locations (entities) such as cities, water bodies, forest areas, etc.
- The layer employs UAV cameras for data capture, eliminating the need for manual intervention.

B. UAV Layer:

- Houses the actual UAVs physically deployed at specific locations for data generation.
- They can form chains or swarms for synchronized tasks.
- Cybersecurity concerns are crucial in this layer, as cyber-attacks can pose significant risks to data integrity and confidentiality.

C. Quantum Layer:

- Utilizes a quantum key distribution paradigm for secure key exchange, employing existing QKD protocols like the BB84 protocol.

D. Internet Layer:

- Facilitates both quantum and classical communication channels mentioned in the quantum layer, using the 5G wireless network.

E. Control Layer:

- The final layer in the architecture stack, comprising a centralized data and control center for UAV operations.

- Enables Quantum Key Distribution (QKD) between arbitrary UAVs (Ua and Ub) using actual quantum computers present at the control station.

- Manages and controls the operations of UAVs deployed on the ground.

BB84 PROTOCOL

1. BB84 protocol involves the transmission of data using the polarization of a single photon state.
2. A quantum communication channel connects the sender (U1) and receiver (U2), allowing the exchange of quantum states.
3. The protocol assumes that an adversary may interfere with the quantum channel, emphasizing the need to verify the classical channel.
4. Encryption of data in non-orthogonal states ensures protocol security, leveraging quantum uncertainty.
5. The polarization of photons is determined by random bit selection and basis choice (rectilinear or diagonal).

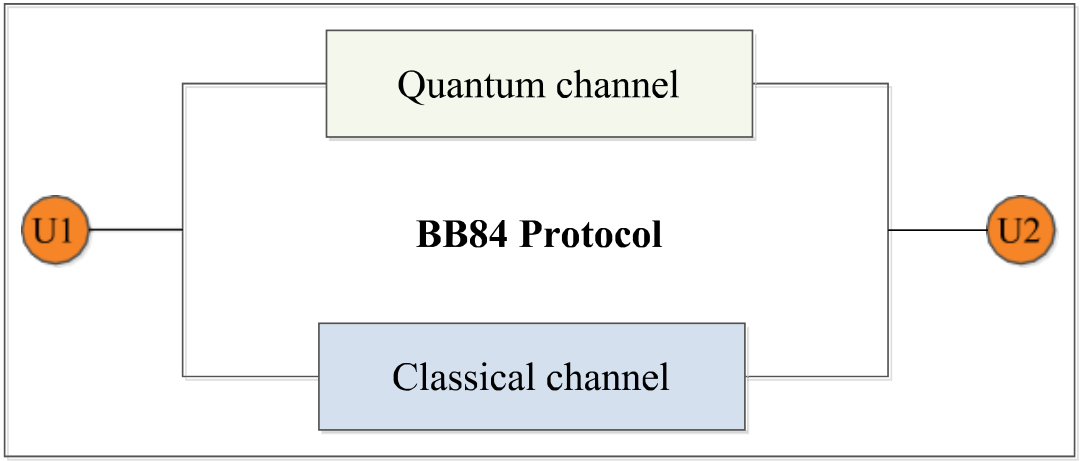
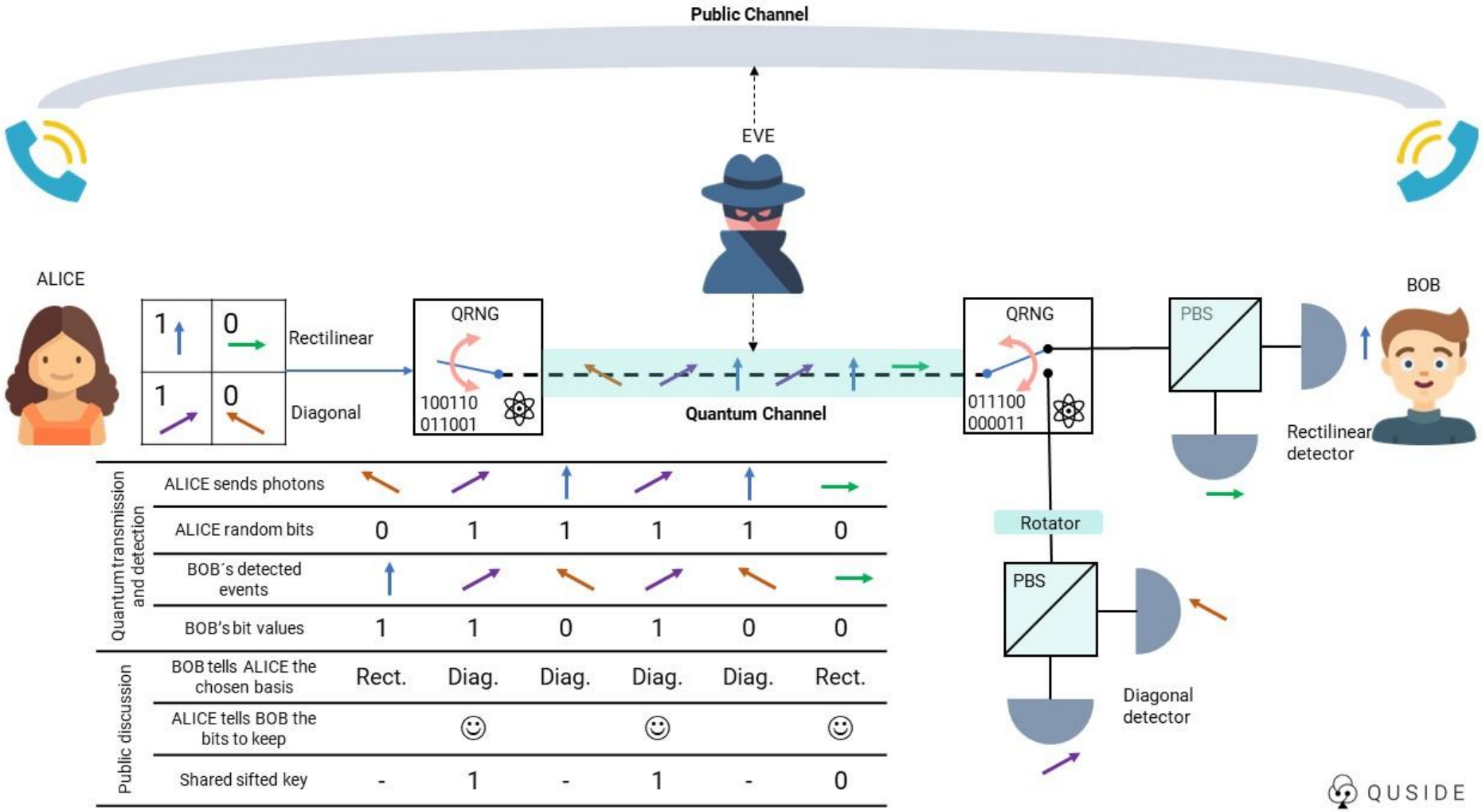


FIGURE 6:

Working of BB84 Algorithm:

1. The sender (U1) produces a random bit (0 or 1) and selects a basis (rectilinear or diagonal) to encode the photon's polarization.
2. U1 sends the single photon through a quantum channel to the receiver (U2), repeating the process for each photon.
3. Quantum physics allows discrimination between non-orthogonal polarization states, enabling measurements in an orthonormal basis.
4. U2 measures each photon's polarization, recording the basis and time of measurement.
5. U1 publicly broadcasts the basis used for encoding the bits, allowing U2 to verify the correctness of his measurements.
6. Both parties discard incorrectly measured photons, generating a shared random key between them.
7. A subset of the remaining bit strings is compared to ensure the key's security, rejecting it if a third party may have learned anything about the photons' polarization.



Quantum transmission and detection	ALICE sends photons	↖	↗	↑	↗	↑	→
	ALICE random bits	0	1	1	1	1	0
	BOB´s detected events	↑	↗	↖	↗	↖	→
	BOB's bit values	1	1	0	1	0	0
Public discussion	BOB tells ALICE the chosen basis	Rect.	Diag.	Diag.	Diag.	Diag.	Rect.
	ALICE tells BOB the bits to keep		☺		☺		☺
	Shared sifted key	-	1	-	1	-	0

Quantum Cryptography Applications

- UAV Communication.
- Cloud Computing Security
- Voting Security
- Future E-commerce
- Smart Card Security (QKarD)

Open Issues and Challenges

- Data Handling
- BB84 Vulnerability to MITM Attacks
- PNS Attack during Key Exchange
- Quantum Channel Breakdown
- Quantum are destroyed once measured
- Cost Efficiency
- Central Node Failure

DISCUSSIONS AND CONCLUSION

This study highlights the need for heightened security in UAV communication, The integration of quantum cryptography and beyond 5G networks emerges as a promising strategy to bolster drone communication and protect data.

1. Urgent Need for Enhanced UAV Communication Security:
   Driven by the widespread global use of drones and the high value of their generated data.
2. Mission-Specific Focus:
   Identifying challenges in securing data transfer in today's cryptographic landscape with a specific emphasis on mission-specific applications.
3. Quantum Cryptography and Beyond 5G Networks:
   Offer a promising approach to fortify drone communication and safeguard data.
4. Adoption of BB84 Quantum Cryptographic Algorithm:
   Represents a significant departure from conventional methods, ensuring a higher level of security.
5. Novel Architecture for Elevated Communication:
   Aims to enhance UAV-to-UAV and UAV-to-GCS communication, particularly beneficial for time-sensitive tasks and highly confidential data.

REFERENCES

[1] A. R. Hall and C. J. Coyne, "The political economy of drones," Defence Peace Econ., vol. 25, no. 5, pp. 445–460, Sep. 2014.
[2] S. P. Priyadharshini and J. Kalaivani, "A study on quantum cryptography," Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 3185–3191, 2018.
[3] R. Renner, "Security of quantum key distribution," Int. J. Quantum Inf. vol. 6, no. 1, pp. 1– 127, Feb. 2008.
[4] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," Phys. Rev. Lett., vol. 78, no. 17, p. 3414, 1997.
[5] R. Aggarwal, H. Sharma, and D. Gupta, "Analysis of various attacks over BB84 quantum key distribution protocol," Int. J. Comput. Appl., vol. 20, no. 8, pp. 28–31, Apr. 2011.
[6] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in Proc. 39th Annu. Symp. Found. Comput. Sci., 1998, pp. 503–509.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," 2020, arXiv:2003.06557.