Study on Practical Quantum-based Security for 6G RAN

Anjar Priyatna
The Center of Excellence AICOMS
Telkom University
Bandung, Indonesia
anjarpri@student.telkomuniversity.ac.id

Khoirul Anwar
The Center of Excellence AICOMS
Telkom University
Bandung, Indonesia
anwarkhoirul@telkomuniversity.ac.id

Gelar Budiman
The Center of Excellence AICOMS
Telkom University
Bandung, Indonesia
gelarbudiman@telkomuniversity.ac.id

***Abstract*—Advancements in mobile network technologies have quickly led to the 6G era, increasing data rates and connectivity for future communications. However, implementing quantum security technology to existing devices is not straightforward, particularly in the area of Radio Access Networks (RAN). This paper studies on practical quantum-based security solutions for 6G RAN by exploring three key objectives: (i) analyzing various documents and standards for Quantum Key Distribution (QKD) in International Telecommunication Union (ITU), (ii) analyzing possible infrastructure and fronthaul system model of quantum-based security for 6G RAN, (iii) comparing different QKD protocols in terms of its strengths, weakness, security features and possible applications to identify whether it is possible for integration into 6G infrastructures and (iv) proposed scheme for QKD deployments for Indonesia case study. This paper aims to contribute to the development of a secure, quantum-resistant RAN for 6G by incorporating insights from the latest standards in various documents.**

***Index Terms*—Quantum Key Distribution, Security, Radio Access Network, Sixth-Generation Wireless Network (6G).**

I. Introduction

Advancements in telecommunications are steering us towards the rollout of sixth-generation (6G) wireless networks, specifically Radio Access Networks (RAN), which are poised to offer extraordinary data transfer rates, ultra-reliable low-latency communication, and expansive connectivity. These capabilities enable a range of applications, from augmented reality and autonomous vehicles to the Internet of Things (IoT). As these networks evolve and integrate more deeply into critical infrastructures, ensuring robust security becomes crucial. Quantum Key Distribution (QKD) emerges as a vital solution, enhancing the security of 6G RAN by securely generating and distributing encryption keys. This integration promises to elevate the security measures to unprecedented levels, safeguarding the privacy and integrity of data across increasingly interconnected environments, thereby addressing the crucial demand for advanced security mechanisms as the world transitions towards more sophisticated and wide-ranging applications supported by 6G networks [1]–[3].

This research is in part supported by Collaboration Research Center for Quantum Technology 2.0 – PKR Kuantum 2024 with ITB Bandung and National Research and Innovation Agency (BRIN).

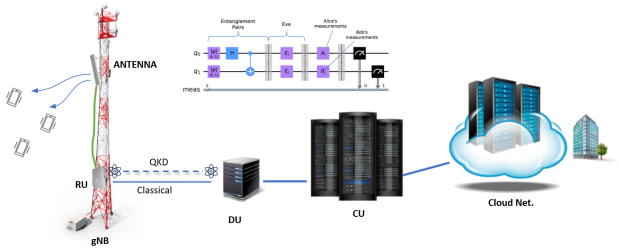

Fig. 1: The system model of Quantum-Based Security for 6G RAN.

Quantum Key Distribution (QKD) enhances 6G telecommunications security by utilizing quantum mechanics principles to generate unbreakable encryption keys, addressing the advanced threats posed by quantum computing. This ensures secure data transmission vital for protecting sensitive information across diverse platforms such as the 6G Radio Access Network (RAN), while also enhancing trust and authentication mechanisms essential for technologies like IoT, foundational to modern infrastructure [4]–[7]. The integration of QKD into 6G networks significantly improves the confidentiality of communications and strengthens overall network resilience, safeguarding critical infrastructures like healthcare and financial services against sophisticated cyber threats [8]–[10].

Latest progress in Quantum Key Distribution (QKD) technology showcases promising prospects for integration with both current and emerging 6G infrastructures. Active research has concentrated on the enhancement and thorough evaluation of diverse QKD protocols, such as BB84 and E91, which are targeted at boosting the efficiency and robustness of key distribution over expansive distances and in fluctuating conditions. Moreover, the development of hybrid cryptographic frameworks that merge classical and quantum approaches signifies a pivotal evolution in the field. These innovative systems aim to provide comprehensive security measures, thus bolstering the operational robustness of 6G networks against the spectrum of real-world challenges and threats [11]–[13].

This study adopts a comprehensive qualitative analysis method, which includes reviewing existing literature, relevant standards, and practical Quantum Key Distribution (QKD) implementations. Additionally, it

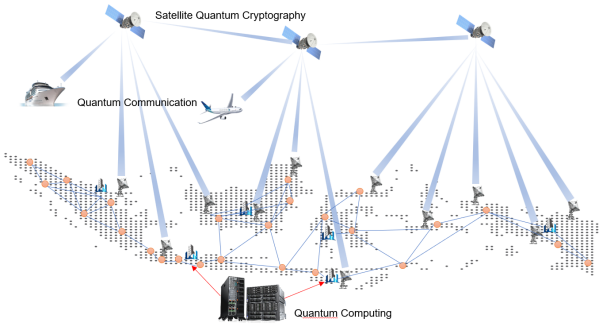

Fig. 2: Grand Design QKDN Indonesia Emas 2045

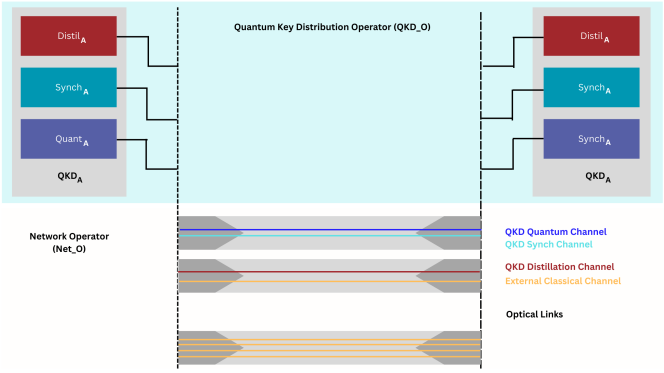

Fig. 3: Dedicated-link architecture.

conducts a comparative analysis of various QKD protocols to determine their practicality and effectiveness in strengthening the security frameworks of 6G RAN environments. The results aim to inform and shape the strategic security decisions in Indonesia's telecommunications sector, supporting the nation's objectives in digital security and transformation. This paper contributes to the field of quantum communications by outlining a practical framework for integrating quantum security technologies and by providing a financial analysis to elucidate the economic implications of these technologies at the national level.

The rest of this paper as follows. Section II introduces the possible system model. Section III analyzes the QKD Standards proposed model designs. Section IV explains qualitative analysis for Indonesia case study QKD Networks. Section V consists of the conclusions.

II. The System Model

The design depicted in Fig. 1 presents an advanced integration of Quantum Key Distribution (QKD) into a 6G Radio Access Network (RAN), enhancing security through a combination of classical and quantum communications. At the forefront are Radio Units (RUs) situated at the network's edge, crucial for converting radio signals into digital data and equipped with QKD to secure transmissions to Distributed Units (DUs). These DUs act as relay points that further process and safeguard the data before sending it to the Central Unit (CU). The DUs not only ensure the encryption of the data through quantum keys but also facilitate the seamless integration of quantum and classical communications. The CU, central to network management and data processing, coordinates the extensive key management tasks, reinforcing network security from end to end. Additionally, the Cloud Network extends beyond the CU, offering necessary computational resources and storage to handle the demands of 6G applications while utilizing quantum encryption to enhance data security and privacy.

The provided image in 2 outlines an advanced network model that incorporates Quantum Key Distribution (QKD) using satellite quantum cryptography to establish a secure global communication system across various mediums, including ground nodes, ships, and airplanes. This system utilizes quantum mechanics—specifically, quantum entanglement and superposition—to enable ultra-secure communications that instantly reveal any interception attempts by altering the quantum states involved. Satellites play a crucial role by distributing quantum keys to various receivers, essential for the encryption and decryption processes that protect sensitive information across large Indonesian islands such as Sumatra, Java, Kalimantan, Sulawesi, and Papua. Each island, with its strategic economic and geographical significance, could utilize this secure network to safeguard vital communications in government, business, and environmental monitoring.

The dedicated-link architecture, depicted in Fig. 3, is recommended for detailed terrestrial connections due to its ability to provide strong isolation for the QKD channel, thereby protecting it from noise interference from the QKD distillation channel and other external classical channels. This architectural choice is crucial for enhancing the integrity and security of quantum communications by reducing the risk of signal degradation and eavesdropping. In this architecture, dedicated links are specifically assigned to QKD Quantum and QKD Synchronization channels, ensuring that these critical communications are segregated from QKD Distillation and other channels, which are routed through separate links.

Operational roles within this architecture are clearly defined; the QKD Operator (QKD_O) handles the technical operations of the QKD Modules, including monitoring quantum channel parameters and managing the key buffer status. This operator is instrumental in planning and estimating QKD performance, leveraging their deep understanding of the communication channel characteristics. Conversely, the Network Operator (NET_O) oversees the broader optical network infrastructure, responsible for channel allocation and ensuring that the specialized needs of QKD communication—covering Quantum, Synchronization, and Distillation channels—are adequately met. This dual-operator model facilitates efficient management of both the physical and quantum layers of the network, optimizing the overall security and functionality of the system.

III. Analysis

This section provides protocol, regulation, strength and financial analysis for future QKD Networks for Indonesia case study.

A. Protocol Analysis

Table I provides a comparative analysis of the protocols in terms of their security features, efficiency, and practical implementation. For instance, BB84 and SARG04 demonstrate strong resistance to eavesdropping and photon-number-splitting attacks, making them suitable for foundational and secure deployments. However, protocols like DPS02 and ESSP02 show significant efficiency in high-loss environments due to phase modulation mechanisms, which is particularly advantageous in metropolitan-scale networks. On the other hand, E91 and BBM92, while offering higher security through entanglement, face challenges in infrastructure complexity, which may limit their widespread adoption. The table emphasizes the trade-off between security and practical implementation, with protocols like IB20 emerging as a flexible and scalable option for next-generation networks.

B. Regulation Analysis

Quantum Networks have not only been actively developed but also require new protocols tailored to quantum repeaters and an entanglement-based framework. Entanglement is deemed essential for the effective functionality of Quantum Key Distribution Networks (QKDN), including satellite integration. It was agreed that these networks would represent the next generation of ICT infrastructure. Suggestions to ITU-T emphasized the need for standardizing Quantum Network protocols to meet the evolving requirements of new network technologies and to ensure consistency across documentation and study groups, particularly under the leadership of JCA-QKDN.

Moreover, the importance of continuous activity in the field of QKDN was highlighted, with recommendations for further study items on quantum-related technology enhancements. The need for an in-depth understanding of quantum physics and collaborative efforts among standards development organizations was noted as crucial for progress. A roadmap-based approach to collaboration was suggested to streamline efforts and leverage collective expertise. The workshop recognized the successful development of QKDN protocols and security measures, indicating that the network is primed for ongoing and future advancements.

C. Qualitative Analysis

1) Strengths: Indonesia benefits from its strategic location, a booming tech sector, and a young, tech-savvy population, providing a strong foundation for adopting and developing quantum security technologies.
2) Weaknesses: The country faces challenges such as limited local expertise in quantum technologies, inadequate existing infrastructure for quantum integration, and insufficient funding for quantum research and development.
3) Opportunities: Opportunities for Indonesia include potential international collaborations to enhance local quantum capabilities, the possibility of increased government support for quantum initiatives, and the development of specialized education programs to build expertise.
4) Threats: Indonesia must navigate potential political instability, competition from established security technologies, and evolving cybersecurity risks that could threaten the deployment and effectiveness of quantum security systems.

D. Timeline

The Fig 4 shows a comprehensive roadmap for the implementation of Quantum Key Distribution (QKD) networks across Indonesia from 2025 to 2045, detailing a phased strategic plan. The plan kicks off in 2025 with foundational trials and proof of concept to test and standardize quantum network technologies in select locations, with significant research support expected from leading technological institutions by 2026. This initial phase aims to assess the effectiveness and security enhancements of QKD over traditional communication methods, establishing the groundwork for a nationwide rollout. By 2030, the roadmap anticipates the full-scale launch of the QKD network, dubbed QKDN Nation, designed to extend quantum-safe communication protocols across all major Indonesian cities, with significant investments in quantum satellite technologies and ground stations to develop a resilient and secure network capable of supporting secure data transmission immune to emerging cyber threats.

The timeline progresses to 2045, targeting the final milestone of achieving 'QKDN Indonesia Emas,' which envisions a mature and fully operational quantum communication network throughout the country. This phase will witness a substantial rollout of quantum technology equipment and the integration of QKD systems into a broad spectrum of digital communication channels, including terrestrial and non-terrestrial networks like the Radio Access Network (RAN), Internet of Things (IoT) devices, and general internet services. Strategic placement of key relay nodes and management systems throughout the network is planned to ensure optimal security and efficiency, solidifying Indonesia's position as a global leader in quantum-safe communications by mid-century.

E. Security Challenges

1) Eavesdropping and Interception in QKD
Eavesdropping is a major threat in communication networks, but Quantum Key Distribution (QKD) leverages quantum mechanics to enhance security. The principles of the no-cloning theorem and Heisenberg uncertainty principle mean any interception attempt alters qubits and introduces detectable errors, though real-world issues like imperfect detectors and environmental noise

TABLE I: Comparison of QKD protocols in terms of security features, efficiency and practical implementation.

Protocol	Security Features	Efficiency	Practical Implementation
BB84	Strong resistance to eavesdropping; detects interception.	Moderate key rates.	Requires single-photon sources and detectors.
E91	Provides higher security through quantum correlations.	Lower key rates compared to BB84.	Complex; requires entanglement generation and management.
BBM92	Resistant to eavesdropping, provides error correction.	Moderate efficiency for practical networks.	Requires quantum entanglement infrastructure.
B92	Lightweight; simple to implement.	Less robust than BB84.	Suitable for low-resource environments.
SSP99	High error tolerance and resilience.	Moderate efficiency.	Scalable for large network deployments.
DPS02	Resistant to photon-number-splitting attacks.	High key rates for short distances.	Simple; does not require single-photon sources.
ESSP02	Stronger security than DPS02.	Moderate efficiency.	Advanced infrastructure for real-world QKD.
KB02	Improved security and key rates.	High efficiency in real-world scenarios.	Simple implementation with classical systems.
SARG04	Strong resistance to photon-number-splitting attacks.	Moderate efficiency.	Similar implementation to BB84.
COW	High transmission rates with simple detectors.	Moderate security.	Suitable for high-speed quantum communication.
AKI05	Adds flexibility in dynamic networks.	Moderate efficiency.	Suitable for time-varying network conditions.
IB20	Ensures compatibility with classical cryptography.	High efficiency and scalability.	Hybrid systems for quantum-safe networks.

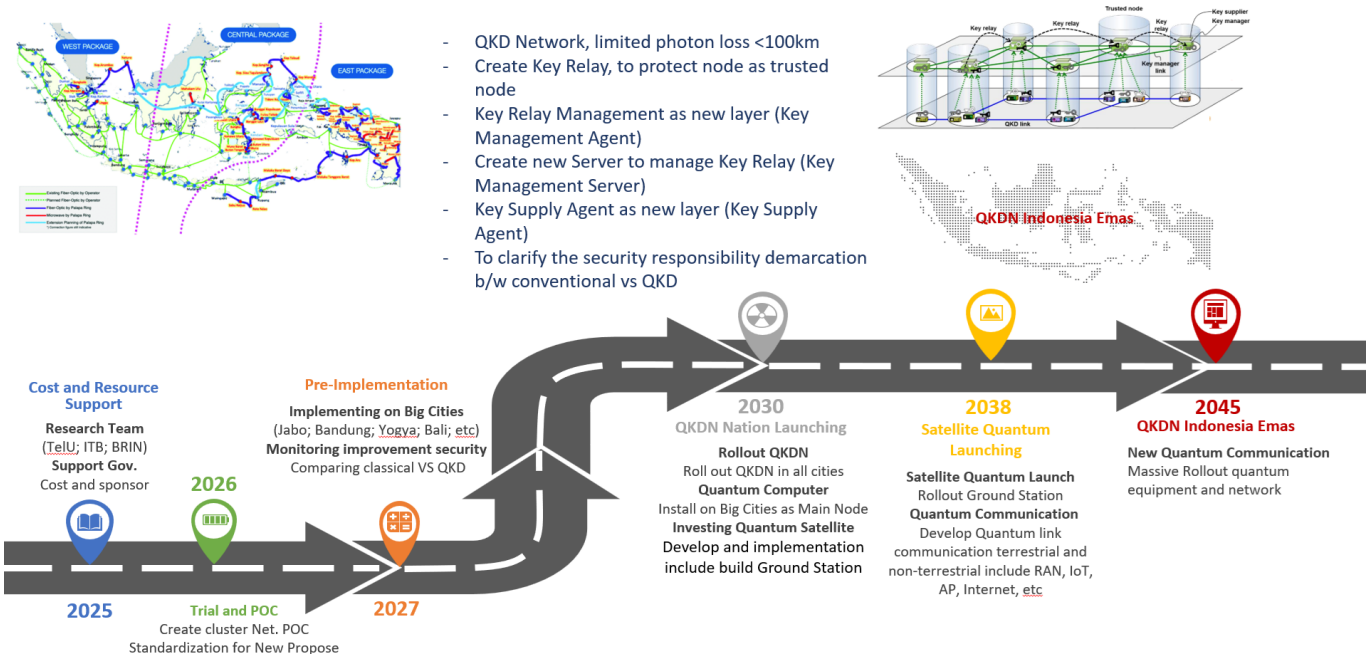

Fig. 4: Timeline of expected Indonesia quantum networks deployment.

could still allow for covert data extraction by advanced eavesdroppers.

2) Man-in-the-Middle Attacks in QKD
In QKD systems, Man-in-the-Middle (MitM) attacks involve an adversary intercepting and altering communications. QKD's quantum properties help detect such intrusions by noticing errors and quantum correlation losses. The use of protocols like Ekert91, which employs entangled particles, helps ensure any attacker interference is detectable through disrupted entanglement.
3) Denial of Service Attacks Against QKD
Denial of Service (DoS) attacks target QKD systems by overwhelming them with noise or excessive requests, reducing key generation rates and disrupting communications. Effective countermeasures include advanced error correction and filtering mechanisms to differentiate between legitimate signals and interference, essential for maintaining system integrity.
4) Side Channel Attacks on QKD Systems
Side-channel attacks in QKD exploit leaks from physical system attributes like power consumption or electromagnetic emissions. These attacks could allow an attacker to infer key information by analyzing such emissions during the key generation process. Designing QKD systems to minimize these leaks is crucial to safeguard against the extraction of sensitive information.

F. Issues

1) Limited Scalability of Current QKD Systems
Current quantum key distribution (QKD) systems face significant scalability challenges, primarily due to their reliance on complex quantum technologies. This limits their deployment in large-scale networks such as those required for 6G RAN, where numerous end-user devices must be efficiently secured.
2) Integration with Existing Network Infrastructure Integrating
QKD solutions with existing network infrastructure poses a substantial challenge. Many current systems are not designed to operate within traditional network environments, requiring significant modifications or complete overhauls of the existing technology, which can be both time-consuming and costly.
3) Need for Standardization
The lack of standardized protocols for QKD complicates interoperability between different sys-

tems and vendors. This fragmentation can hinder widespread adoption, as organizations may hesitate to invest in technology that lacks industry-wide support and compatibility.

4) Cost Implications of QKD Deployment
The high costs associated with the deployment of QKD systems remain a barrier to their adoption. This includes not only the initial investment in quantum technology but also ongoing operational expenses, which can deter organizations from fully committing to QKD solutions.

G. Financial Analysis

No	Description	Qty	Unit	Unit Price ($)	Total Price ($)
1	**Quantum Satellites**				60,000,000
	Satellite Manufacturing	3	Unit	15,000,000	45,000,000
	Launch Services	3	Unit	5,000,000	15,000,000
	Design Engineering	3	Unit	2,000,000	6,000,000
	Testing and Validation	3	Unit	2,000,000	6,000,000
	Project Management	-	-	-	3,000,000
2	**Ground Stations**				100,000,000
	Construction and Infrastructure	10	Unit	7,000,000	70,000,000
	Quantum Receivers	10	Unit	3,000,000	30,000,000
	Security Systems	10	Unit	1,500,000	15,000,000
	Integration Software	10	Unit	1,000,000	10,000,000
	Installation & Integration	10	Unit	1,000,000	5,000,000
3	**Quantum Routers**				50,000,000
	Router Hardware	50	Unit	800,000	40,000,000
	Installation Services	50	Unit	200,000	10,000,000
4	**Encryption Systems**				50,000,000
	Encryption Hardware	100	Unit	400,000	40,000,000
	Key Management Software	100	Unit	100,000	10,000,000
5	**Network Infrastructure**				30,100,000
	Site Preparation	-	-	-	5,000,000
	Network Integration	-	-	-	10,100,000
	System Testing	-	-	-	15,000,000
Total					**290,100,000**

From the Table III-G Quantum satellites enhance secure global communications by using quantum entanglement to send encryption keys between any two points on the planet, a critical feature for developing a truly secure global communication network that transcends geographical and political boundaries. This system ensures data security across continents, positioning any investing nation or organization as a leader in cutting-edge telecommunications. The significant investments required for satellite manufacturing ($45,000,000), launch services ($15,000,000), and related engineering and validation efforts ($12,000,000) reflect the sophisticated and high-tech nature of these assets, which are vital for global quantum communications.

Ground stations serve as critical terrestrial endpoints for quantum signals from satellites, processing and integrating these signals into the existing networks. The construction of multiple ground stations enhances network redundancy and increases fault tolerance, improving overall network reliability. A substantial investment in these stations, including $70,000,000 for construction and infrastructure, $30,000,000 for quantum receivers, and $25,000,000 for security and software integration, underlines their role in maintaining the network's integrity and functionality. Moreover, quantum routers streamline the network by optimizing data routing, with significant funds allocated for router hardware ($40,000,000) and installation services ($10,000,000). Encryption systems within the network use quantum mechanics to generate unbreakable keys, with $40,000,000 spent on hardware and $10,000,000 on key management software, underscoring their crucial role in protecting data against espionage and cyber threats. This infrastructure is foundational for a scalable network, poised to grow as quantum technology advances, with substantial initial investments in site preparation, integration, and testing totaling $30,100,000.

IV. Conclusions

In this paper, we have studied several documents from ITU related to practical quantum-based security for 6G RAN. QKD provides an information-theoretical way to share secret keys between two parties. However, there is a signifcant gap between theory and practice. QKD requires hop-by-hop security relying on trusted intermediate nodes and QKD demands the deployment of new hardware. QKD Networks which can be regarded as a subset of a Quantum Internet has six stages of roadmap development. Quantum Internet is not anticipated to replace but rather to enhance the Classical Internet. Additionally, we classified 12 different QKD protocols to provide a comprehensive understanding of their underlying mechanisms and functionality. QKD based on the BB84 protocol has been commercially deployed and are in use today to distribute quantum safe keys in real networks. The SARG protocol has been used on the international Swiss Quantum network. Differential-Phase-Shift and the Coherent OneWay protocol enabling long-distance and high transmission rate QKD exceeded 250 km transmission distance in optical fibre. The forecasted budget of roughly USD 295.1 million, distributed across various sectors such as infrastructure, hardware, training, and research and development, marks a critical investment in safeguarding the telecom- munication future of Indonesia. The archipelago's distinct geographic challenges call for the launch of three quantum satellites, improvements to ground stations, and the extension of a secure fiber optic network to achieve extensive national coverage. Finally, we considered the practical implementation possibilities of these protocols in future communication systems.

References

[1] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5g era," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 90–96, 2014.

[2] S. P. et al., "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[3] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179.

[5] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[6] R. A. et al., "Using quantum key distribution for securing optical networks," in *Proceedings of the 2014 European Conference on Optical Communication*, 2014, pp. 1–3.

[7] T. G. et al., "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," *Nature Communications*, vol. 6, p. 8795, 2015.

[8] E. Diamanti and I. Kerenidis, "Quantum cryptography: From theory to practice," *Advances in Physics: X*, vol. 1, no. 1, pp. 1–24, 2016.

[9] Z. Z. et al., "Experimental demonstration of entanglement-based continuous-variable quantum key distribution," *Physical Review Letters*, vol. 124, no. 13, p. 130501, 2020.

[10] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.
[11] V. S. et al., "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, p. 1301, 2009.
[12] L. O. Mailloux and Z. Tang, "Hybrid classical-quantum cryptography for 6g networks," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 50–56, 2021.
[13] S. W. et al., "Practical security analysis of quantum key distribution with minor device flaws," *Physical Review X*, vol. 9, no. 4, p. 041012, 2019.