2025 International Conference on Data Science, Agents, and Artificial Intelligence (ICDSAAI 2025)
28-29 March 2025, Chennai, India

2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) | 979-8-3315-3755-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICDSAAI65575.2025.11011628

Synergizing Quantum Cryptography and Post-Quantum Cryptography: A New Era of Ultra-Secure Data Transmission

A.R Kavitha*
Dept of Information Technology,
Chennai Institute of Technology,
Anna University,
Kundrathur,
Chennai-600069, India
kavithaar@citchennai.net

Balachandhar R
Dept of Information Technology,
Chennai Institute of Technology,
Anna University,
Kundrathur,
Chennai-600069, India
balachandharr@citchennai.net

Harikrishna K
Dept of Information Technology,
Chennai Institute of Technology,
Anna University,
Kundrathur,
Chennai-600069, India
harikrishnak.it2023@citchennai.net

Abstract—**Quantum Cryptography (QC) is a newer method of ultra-secure key transmission that relies more on Quantum Key Distribution (QKD) protocols. On the contrary, Post-Quantum Cryptography (PQC) is concerned about the high-security encryption of data that uses algorithms like the Kyber algorithm. However, both face unique challenges: QC requires costly QKD hardware, offers limited scalability due to point-to-point communication, and is vulnerable to physical attacks like side-channel and denial-of-service exploits, while PQC is resource-intensive, prone to latency issues, and faces uncertainties regarding future quantum algorithms that may compromise its security. Some challenges that QC and PQC face are overcome by merging both of them for the hybrid approach. This review explores synergy between QC and PQC, proposing a hybrid solution for combining QKD-based secure key exchange with the PQC quantum-resistant encryption capability. This integration delivers robust, future-proof communication with protection against both classical and quantum threats.**

Keywords—Quantum cryptography, Quantum mechanics, Superposition, Entanglement, Qubit.

I. Introduction

Quantum Key Distribution (QKD) protocols such as BB84 and E91 are the basic building blocks of Quantum Cryptography (QC). Such QC can provide an unbreakable security guarantee for the distribution of keys, in theory. However, this concept is plagued by serious problems, such as the cost of hardware in QKD and a severe issue related to scalability because of its point-to-point nature of communication as well as vulnerabilities to side-channel and denial-of-service exploits [1]. Post Quantum Cryptography (PQC), as its name suggests, is the development of quantum-resistant algorithms or those based on lattice-based cryptography implemented on classical infrastructure. Although offering resistance to quantum attacks, PQC algorithms are computationally intensive, which can lead to higher latency and uncertainty about long-term security as quantum computing advances [2].

To overcome these limitations, a hybrid approach combining QC and PQC has emerged. By combining the secure key distribution from QKD with PQC algorithms for encryption, this solution offers an enhanced security that provides immunity to both classical and quantum attacks. Moreover, the method addresses the issue of QC's scalability due to compatibility with the underlying classical infrastructure and provides an additional protection layer against physical attacks. This hybrid model is a promising solution for protecting sensitive data, including financial transactions and government communications, in the quantum era [1,2]. This review discusses the complementary roles of QC and PQC, points out their respective challenges, and shows that the hybrid approach can provide a robust framework for cryptographic security against both current and emerging quantum threats.

II. PRINCIPLES AND CHALLENGES OF QUANTUM CRYPTOGRAPHY

A. Core Principles of Quantum Cryptography (QC):

QC is an area of revolutionary secure communications that relies upon the quantum principles: entanglement, superposition and no-cloning theorem, to secure promises beyond what is achieved by classical cryptography.

1) Quantum Superposition: The superposition principle tells us that the qubit could be in many states at one time (that is 0, 1, or both 0 and 1). Superposition can represent a few classical states all at once. For example, a couple of qubits have four states: |00|, |01|, |10|, and |11|. In quantum cryptography, superposition is put to work in protocols; for example, Quantum Key Distribution (QKD) transfers qubits in their superposition state, with the disturbance of the attacked qubit indicating the appearance of the attacker [3].

2) Quantum Entanglement: It is a phenomenon that takes place only in quantum systems where the two or more qubits are so entangled that one qubit's state relies on the other qubit's state, independent of the distance between those qubits. This nonlocal phenomenon permits using entanglement in quantum cryptographic protocols, for instance, E91 in secure key distribution. If an eavesdropper tries measuring any of the entangled qubits, it would collapse the shared state and disturb the entanglement, thus revealing their presence [4].

3) Heisenberg's Uncertainty Principle: It states that both the momentum and position of a particle/object cannot be precisely measured at the same time. If one is measured more accurately, the other may be measured less accurately. It gives a view of how in quantum mechanics there is always a limitation in observation. It brings out the probabilistic nature of particles at the quantum level [5].

4) No-Cloning Theorem: It states that it is impossible to clone an unknown quantum state with complete accuracy. Cloning an unknown quantum state is no longer determinate and cannot be reproduced precisely without altering the state itself. Thus, quantum cryptography is naturally immune to eavesdropping since any action to intercept or measure quantum information necessarily interferes with the systems; hence, detection is possible [4].

B. Quantum Key Distribution:

Quantum Key Distribution (QKD) allows sharing a cryptographic key between two devices in such a way that these keys are imparted securely using quantum properties of superposition and entanglement. However, if we try to eavesdrop on any classical cryptographic protocols, then the act will go unnoticed. We have two foundational protocols, BB84 and E91, which form the understanding towards developing secure quantum communication.

- **BB84 Protocol:**

The basic concept of the BB84 protocol depends on the quantum superposition principles and measurements. It uses qubits (quantum bits), consisting of photons encoded in either one of the four polarization states,

0: Horizontal polarization represented as |0|,

1: Vertical polarization represented as |1|,

+: Diagonal polarization represented as |+| = (1/sqrt (2)) * (|0| + |1|),

−: Anti-diagonal polarization represented as |-| = (1/sqrt (2)) * (|0| - |1|).

1) ***Encoding Qubits***: Sender encodes a bit (b) using one of the two bases:

If b=0, the sender chooses |0| or |+|.

If b=1, the sender chooses |1| or |-|.

2) ***Transmission:*** The sender transmits the encoded qubits to the receiver. The qubit's state is one of four possible polarization states.

3) ***Measurement:*** Receiver measures the received qubits. If the sender and receiver share the same basis, the measurement outcomes would be the same as the encoded bits; otherwise, the measurement outcomes are random.

4) ***Sifting:*** Sender and receiver publicly reveal their basis choices. They retain only those bits in which the two bases were the same and discard those in which the bases were different. Mathematically, for any such pair of qubits, when sender and receiver select the same basis, their shared key bits will be correlated as [4]:

|ψ| = (1/sqrt (2)) * (|0| + |1|) or |ψ| = (1/sqrt (2)) * (|0| - |1|).

- **BB84 Protocol's Security:**

BB84 provides security in a guaranteed manner by using the uncertainty principle and no-cloning theorem. No-cloning theorem ensures that the eavesdropper cannot prepare an identical/exact copy of a quantum state, whereas uncertainty principle ensures that measurement of a quantum state will disturb it. This disturbance creates errors/anomalies in the key detected by the sender and receiver.

C. Challenges of Quantum Cryptography:

Quantum cryptography promises seemingly unbreakable security, but its applications have proven difficult to achieve in practice, primarily due to hardware and scalability.

- **Hardware Requirements:**

Hardware components in quantum cryptography include photon sources, detectors such as avalanche photodiodes, and quantum channels such as optical fibers or free-space links. These components have to preserve high fidelity in order to avoid eavesdropping. The problem in quantum transmission is that photon loss causes the quantum signal to be weak over distance; this limits the range of currently available QKD systems. Although still in experimental stages, quantum repeaters aim to extend this reach by reducing photon loss while preserving quantum coherence. Several factors including temperature, vibration, and even electromagnetic interference, impact performance that requires controlled operating conditions [6].

- **Scalability and Integration with Classical Systems:**

Another equally important thing is the compatibility of quantum cryptography with any existing classical communication networks. Quantum cryptographic systems need to be compatible with existing classical cryptographic systems so that hybrid solutions can be built to secure data at all network layers. The transition to quantum networks poses not only technological but also logistical barriers, such as new infrastructure in the form of quantum repeaters and quantum-safe hardware for end-users [7].

III. POST QUANTUM CRYPTOGRAPHY FOR QUANTUM RESISTANCE

Post-Quantum Cryptography (PQC) does create any cryptographic algorithms that are resistant to quantum attacks. Classical systems of cryptography, for example, Rivest-Shamir-Adleman (RSA), are insecure against quantum algorithms (Example: Shor's algorithm), in particular since it factors extremely large numbers in a reasonable number of steps [4, 8, 9]. That is, the aim of PQC is to create cryptosystems that classical quantum computers break with reasonable resources [10, 11].

A. Kyber Algorithm:

Kyber algorithm is a lattice-based public-key encryption algorithm (PKE). It is a Key Encapsulation Mechanism (KEM) for PQC. Kyber algorithm's security is built upon the variant of the Learning with Errors problem, known as Module-LWE. It is built to be hard for both classical and quantum attacks [12]. Kyber depends on the M-LWE problems, variants of LWE that organize small-dimensional lattices as modules for compact representation of data. The problem lies in that noisy linear equations are complicated to solve computationally for a classical and quantum computer when the dimensions get very high [13].

- **Working of Kyber Algorithm:**

  The Kyber algorithm works on three primary phases: Key-generation, Encapsulation, and Decapsulation.

- *Key Generation:*
  - Objective: To generate key pairs–one public key and one private key.
  - Process: This algorithm generates random values that help strengthen security. Encryption is done by using a public key, while the private key kept secret for decryption.
- *Encapsulation:*
  - Objective: Encrypt a message to obtain a shared secret key.
  - Process: Receiver's public key is used by the sender to encrypt a random secret. This creates a ciphertext that is sent to the receiver.
- *Decryption:*
  - Objective: Decrypt the shared message and regain the shared secret key.
  - Process: By using the private key, receiver decrypts the ciphertext obtaining the shared secret key for secure communication [12,13].

B. *Challenges in PQC:*

i) Efficiency and Performance:

For the most part, PQC schemes typically require more processing power and memory as compared to their classical counterparts. Some lattice-based cryptosystems are reported to be computationally expensive-a characteristic that makes it harder for their implementation in resource-constrained devices [6, 14].

ii) Key Size and Overhead:

Quantum-resistant schemes, especially code-based ones, in general have larger key sizes compared to the traditional cryptographic methods. The additional storage and transmission overheads will present practical challenges in several applications involving IoT and mobile devices [13, 15].

iii) Transition to Quantum-Resistant Systems:

It takes much labor to adapt the available infrastructures for PQC as the prevailing standard must be preserved. The transition requires concerted effort from industries because security must be provided without interfering with running systems [6, 9, 16].

IV. INTEGRATION OF QUANTUM CRYPTOGRAPHY AND POST QUANTUM CRYPTOGRAPHY

Countermeasures to quantum computing threats come through a combined approach of Quantum Cryptography (QC) and Post-Quantum Cryptography (PQC). QC has its strengths through quantum key distribution, wherein any attempt at eavesdropping is detected because of quantum principles. Whereas PQC focuses on developing quantum computers-resistant algorithms and protects information against both classical and quantum attacks. This hybrid system therefore, by combining the strengths of these two fields, enhances security in guaranteeing confidentiality, integrity, and authenticity of data. This multi-layered security framework safeguards current communication systems but readies them for the future, where quantum adversaries would pose a potential threat, making this phase a very necessary step in securing sensitive data in the quantum age [8, 17]. The steps involved in the hybrid approach are shown in Fig: 1.

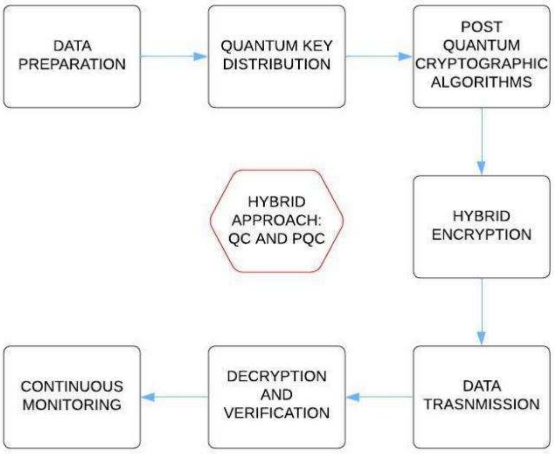

Fig:1 Steps in Hybrid Approach

A. *Key exchange with Quantum Key Distribution:*

Quantum Key Distribution (QKD) depends on quantum mechanics principles for secure exchange of keys. BB84 is the best-known QKD protocol. The key exchange between sender and receiver is shown in Fig 2.

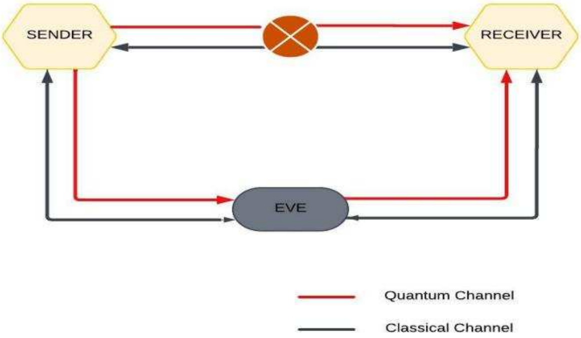

Fig:2 Key Exchange between Sender and Receiver

i) Preparation of Quantum State: The sender encodes classical bits (0 or 1) onto quantum states using two bases:

Rectilinear Basis: {|0|, |1|}

Diagonal Basis: {|+|, |-|}, where

|+| = (1/sqrt (2)) * (|0| + |1|) and

|-| = (1/ sqrt (2)) * (|0| - |1|) [3, 17].

ii) Quantum Transmission: Qubits are transmitted through a quantum channel. Any attempt by an intruder to intercept will introduce measurable changes since an ideal copy of unknown quantum states is hidden by the No-Cloning Theorem [4].

iii) Measurement and Basis Reconciliation: The receiver receives each qubit in a randomly chosen basis. Sender and receiver use a public classical channel to compare bases. Only bits measured in the same basis are retained as the raw key [6, 16].

iv) Error Reconciliation: The errors that arise due to the noise as well as due to eavesdropping are corrected with the help of classical error correction codes. It includes Low-Density Parity-Check (LDPC). LDPC can be represented as:

$$H \cdot s = e \ (\text{mod } 2)$$

where H is a parity check matrix, s is the raw key, and e is the error vector [18, 19].

v) Privacy Amplification: Privacy amplification reduces partial information that could have been acquired by Eve through hashing on the reconciled key followed by the creation of a secure final key [12, 19].

B. *Data Encryption with Post Quantum Cryptography Algorithms:*

PQC relies on problems which are challenging for quantum attacks. Lattice-based cryptography is the most popular among other cryptography. It includes the Kyber algorithm, which relies on the LWE problem.

$$A \cdot s + e \equiv b \ (\text{mod } q)$$

where A is a randomly chosen matrix, s is the secret key, e is the error vector, and b is a public key's component. Security comes as it is hard to find s given A, b, and noise e [9,12]. The Shortest Vector Problem (SVP) of lattice-based cryptography is quantum-resistant. The issue underlying which is that of the determination of the shortest nonzero vector in a high-dimensional lattice, challenging for quantum algorithms. Other difficult problems are module-LWE and NTRU, forming the basis for schemes like Kyber [9, 12, 21].

C. *Hybrid System for Secure Key Exchange Using Quantum Key Distribution and Post-Quantum Cryptography:*

- ***Layered Defence Strategy:***

i) Quantum Key Exchange with Quantum Key Distribution: It establishes a quantum-secure channel for key distribution. The final secure key obtained from QKD is used as a symmetric key in classical encryption schemes. [13, 22].

ii) Data Encryption with Post Quantum Cryptography Algorithms: Once a secure key has been established using Quantum Key Distribution (QKD), it encrypts sensitive information through Post Quantum Cryptography (PQC) algorithms, for instance, Kyber. This would ensure that even when some emerging quantum computers break the traditional encryption, data remains safe. [9, 12, 20].

- ***Practical implementation example:***

a) **Quantum Key Distribution for Secure Key Exchange:** Critical infrastructure data centers, such as financial industries, can generate common symmetric keys with entangled photons using Quantum Key Distribution (QKD). Here are the entangled states:

$$|\Phi+| = (1/ \text{sqrt}\ (2)) * (|00| + |11|),$$

provide a secure channel [13,23].

b) **Post Quantum Cryptography for Encryption:** Encrypted messages use a lattice-based scheme such as NTRU or Kyber:

$$C = P \cdot H \ (\text{mod } q)$$

where C is the ciphertext, P is the plaintext, and H is a polynomial-based public key [20,21,24]. The entire workflow of the hybrid approach is shown in Fig 3.

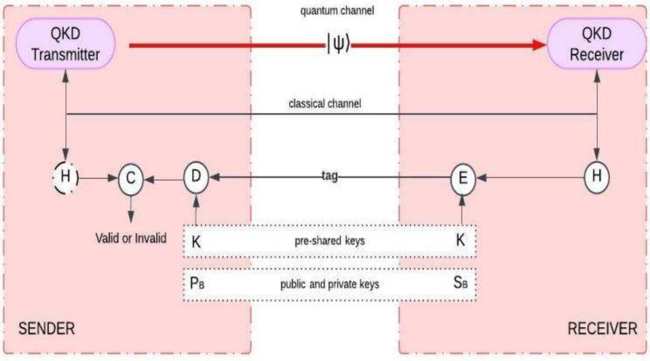

Fig: 3 Workflow of the Hybrid Approach

V. REAL WORLD APPLICATIONS AND PRACTICAL USE CASES

i) Secure Communication:

The combination of QC and PQC provides better security assurances for sensitive sectors like government, healthcare, and finance. Quantum Key Distribution (QKD) protocols of QC are already proving to be robust against eavesdropping attacks on communication networks by exploiting quantum mechanics [10, 25, 26]. On the other hand, lattice-based PQC schemes offer robust defenses against attacks from quantum computers, so encrypted data will be safe post-quantum as well [6, 24, 27].

ii) Quantum Networks:

Quantum networks will work toward establishing a global quantum internet to enable secure data transfer via entangled states. Developments in Quantum Key Distribution (QKD) systems and satellite-based quantum communication open up the prospects for these networks [6, 20, 28]. Practical feasibility of such systems has been demonstrated by experiments involving entangled photons for long-distance transmission, such as those conducted in the China Micius satellite project [18,28,29].

iii) Sensitive Data Protection:

QC and PQC combination gives a long-term solution for secure protection of data, especially on classified high-value information. PQC algorithms, like NTRU Encrypt and CRYSTALS-Di lithium, work on complex mathematical problems that cannot be solved even on a very powerful quantum computer [12,30,31].

iv) Emerging Technologies:

Applications of QC and PQC appear in emerging trends including blockchain, IoT, and cloud computing. In blockchain applications, quantum-secure protocols assure the integrity of a transaction, while PQC applies specifically to keying functions for cryptos involved in digital signatures [23,32,33]. In IoT applications, secure communication between devices depends directly upon PQC algorithms, used there to ensure that connected nodes do not permit quantum attacks upon vulnerable endpoints [1,26,34].

VI. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

i) Scalability of Quantum Cryptography:

Scaling QC systems, such as QKD to the global level will be possible only after overcoming problems like photon loss, decoherence, and the development of reliable quantum repeaters [9, 27, 35]. Current efforts are on error correction protocols and trying to enhance the entanglement distribution efficiency [28, 36, 37].

ii) Standardization of Post Quantum Cryptography:

Standardization of PQC is highly demanding in real environments as a result of several tests run on the algorithms. The standardization efforts are mainly directed toward discovering secure, efficient, and scalable approaches to PQC that can supersede traditional systems [18,24, 22].

iii) Integration with Classical Systems:

Integrating QC and PQC with existing infrastructure requires a phased approach, addressing compatibility, deployment costs, and transition complexities. Hybrid systems that merge classical encryption with PQC are under development to facilitate this transition while maintaining security [7, 16, 38, 39].

VII. CONCLUSION

Integration of QC and PQC provides data protection by a powerful defence mechanism through the quantum mechanical strength coupled with classical cryptographic resilience. That hybrid model addresses both short-term and long-term security concerns. Quantum communication and PQC standardization will profoundly impact secure data over all fields, bringing a new era in cryptographic standards. Further research and innovation across the globe need to be addressed to overcome the hurdles posed by a quantum-dominated landscape. The hybrid cryptographic model is speculated to abreast the technological change without compromising the sensitivity of the information regarding the quantum threats.

REFERENCES

[1] Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A review of the present cryptographic arsenal to deal with post-quantum threats. Procedia Computer Science, 215, 834-845. DOI: https://doi.org/10.1016/j.procs.2022.12.086 .

[2] Yu, Y. (2021). Preface to special topic on lattice-based cryptography. National Science Review, 8(9), nwab154. DOI: https://doi.org/10.1093/nsr/nwab154 .

[3] Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge university press.

[4] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE. DOI: 10.1109/SFCS.1994.365700.

[5] Svensson, S., & Bourennane, M. (2013). Testing Heisenberg's Uncertainty Principle with Polarized Single Photons.

[6] Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. Frontiers in Physics, 12, 1456491.DOI:https://doi.org/10.3389/fphy.2024.1456491 .

[7] Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS-a practical forward secure signature scheme based on minimal security assumptions. In Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4 (pp. 117-129). Springer Berlin Heidelberg.

[8] Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120–126. DOI: https://doi.org/10.1145/359340.359342 .

[9] Perlner, R. A., & Cooper, D. A. (2009, April). Quantum resistant public key cryptography: a survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet (pp. 85-93). DOI: https://doi.org/10.1145/1527017.1527028 .

[10] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[11] Micciancio, D., & Goldwasser, S. (2002). Complexity of lattice problems: a cryptographic perspective (Vol. 671). Springer Science & Business Media.

[12] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE. DOI: 10.1109/EuroSP.2018.00032.

[13] Peikert, C. (2016). A decade of lattice cryptography. Foundations and trends® in theoretical computer science, 10(4), 283-424. DOI: http://dx.doi.org/10.1561/0400000074 .

[14] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... & Xiong, N. (2023). Post-quantum security: Opportunities and challenges. Sensors, 23(21), 8744. DOI: https://doi.org/10.3390/s23218744

[15] Loidreau, P. (2017, June). A new rank metric codes based encryption scheme. In International Workshop on Post-Quantum Cryptography (pp. 3-17). Cham: Springer International Publishing.

[16] Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015, May). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In 2015 IEEE symposium on security and privacy (pp. 553-570). IEEE. DOI: 10.1109/SP.2015.40.

[17] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science, 560, 7-1. DOI:https://doi.org/10.1016/j.tcs.2014.05.025 .

[18] Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. DOI: https://doi.org/10.6028/NIST.IR.8413 .

[19] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.

[20] Peikert, C. (2014, October). Lattice cryptography for the internet. In International workshop on post-quantum cryptography (pp. 197-219). Cham: Springer International Publishing.

[21] Pöppelmann, T., & Güneysu, T. (2014, June). Area optimization of lightweight lattice-based encryption on reconfigurable hardware. In 2014 IEEE international symposium on circuits and systems (ISCAS) (pp. 2796-2799). IEEE. DOI: 10.1109/ISCAS.2014.6865754.

[22] Ding, J., Xie, X., & Lin, X. (2012). A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive.

[23] Xu, G., Mao, J., Sakk, E., & Wang, S. P. (2023, March). An overview of quantum-safe approaches: quantum key distribution and post-quantum cryptography. In 2023 57th Annual Conference on Information Sciences and Systems (CISS) (pp. 1-6). IEEE. DOI: 10.1109/CISS56502.2023.10089619.

[24] Weger, V., Gassner, N., & Rosenthal, J. (2022). A survey on code-based cryptography. arXiv preprint arXiv:2201.07119. DOI: https://doi.org/10.48550/arXiv.2201.07119 .

[25] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. Advances in optics and photonics, 12(4), 1012-1236. DOI: https://doi.org/10.1364/AOP.361502 .

[26] Wang, L. J., Zou, K. H., Sun, W., Mao, Y., Zhu, Y. X., Yin, H. L., ... & Pan, J. W. (2017). Long-distance co-propagation of quantum key distribution and terabit classical optical data channels. Physical Review A, 95(1), 012301. DOI: https://doi.org/10.1103/PhysRevA.95.012301 .

[27] Elkouss, D., Leverrier, A., Alléaume, R., & Boutros, J. J. (2009, June). Efficient reconciliation protocol for discrete-variable

quantum key distribution. In 2009 IEEE international symposium on information theory (pp. 1879-1883). IEEE. DOI: 10.1109/ISIT.2009.5205475.

[28] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). "NTRU: A Ring-Based Public Key Cryptosystem". DOI: https://doi.org/10.1007/BFb0054868 .

[29] Sidhu, J. S., Joshi, S. K., Gündoğan, M., Brougham, T., Lowndes, D., Mazzarella, L., ... & Oi, D. K. (2021). Advances in space quantum communications. IET Quantum Communication, 2(4), 182-217. DOI: https://doi.org/10.1049/qtc2.12015 .

[30] Teja, V., Banerjee, P., Sharma, N. N., & Mittal, R. K. (2007, August). Quantum cryptography: state-of-art, challenges and future perspectives. In 2007 7th IEEE conference on nanotechnology (IEEE NANO) (pp. 1296-1301). IEEE. DOI: 10.1109/NANO.2007.4601420.

[31] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238-268. DOI: https://doi.org/10.13154/tches.v2018.i1.238-268 .

[32] Jones, R. W. (2024). ΦBlockchain: A Quantum-Resistant, Immutable Blockchain Protocol.

[33] Darzi, S., Ahmadi, K., Aghapour, S., Yavuz, A. A., & Kermani, M. M. (2023). Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities. arXiv preprint arXiv:2310.12037. DOI: https://doi.org/10.48550/arXiv.2310.12037 .

[34] Samardjiska, S., & Gligoroski, D. (2014). Linearity Measures for Multivariate Public Key Cryptography.

[35] Manzalini, A. (2020). Quantum communications in future networks and services. Quantum Reports, 2(1), 221-232. DOI: https://doi.org/10.3390/quantum2010014 .

[36] Coles, P. J., Berta, M., Tomamichel, M., & Wehner, S. (2017). Entropic uncertainty relations and their applications. Reviews of Modern Physics, 89(1), 015002. DOI: https://doi.org/10.1103/RevModPhys.89.015002 .

[37] Martinez-Mateo, J., Elkouss, D., & Martin, V. (2013). Key reconciliation for high performance quantum key distribution. Scientific reports, 3(1), 1576. DOI: https://doi.org/10.1038/srep01576 .

[38] Huttner, B., Imoto, N., Gisin, N., & Mor, T. (1995). Quantum cryptography with coherent states. Physical Review A, 51(3), 1863. DOI: https://doi.org/10.1103/PhysRevA.51.1863

[39] Kuznetsov, A., Svatovskij, I., Kiyan, N., & Pushkar'ov, A. (2017, October). Code-based public-key cryptosystems for the post-quantum period. In 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 125-130). IEEE. DOI: 10.1109/INFOCOMMST.2017.8246365.