Securing Next-Generation Quantum IoT Applications using Quantum Key Distribution

Basudeb Bera, Ashok Kumar Das, *Senior Member, IEEE*, and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—The next generation of Quantum Internet of Things (QIoT) has the potential to revolutionize various sectors, including smart homes, healthcare, and smart cities, by enabling more sophisticated and interconnected systems. These applications incorporate advanced features, such as autonomous decision-making based on Quantum Artificial Intelligence and Machine Learning (QAI/ML) and context-aware functionality. The security of the data in these applications relies on traditional cryptographic techniques, which, however, face a growing threat due to the significant advancements in quantum computing, especially with the Shor's algorithm. This algorithm poses a substantial risk of breaking conventional cryptographic methods within a feasible timeframe. To address these emerging security challenges in the quantum realm, we propose a Quantum Key Distribution (QKD) based on the BB84 protocol. This approach aims to provide robust authentication using certificates through a classical channel and secure quantum key exchange via a quantum channel in a public environment. The proposed QKD scheme is implemented using a client-server model in Python and Qiskit, demonstrating its practicality in real-world applications. The obtained results showcase the successful establishment of a secure session key between IoT smart (sensor) devices and gateway nodes, effectively mitigating potential threats such as eavesdropping.**

***Index Terms*—Quantum key distribution, Internet of Things (IoT), security, key exchange, Qiskit implementation.**

I. Introduction

The Internet of Things (IoT) refers a network of interconnected smart sensor devices, machines, and objects that communicate and share data with each other through a wire or wireless Internet without requiring direct human involvement [1]. As per Statista's data presented in Fig. 1, the current count of interconnected IoT devices stands at 15.14 billion in 2023. This figure represents nearly twice the global population, estimated at eight billion. The forecast suggests a continuous annual increase, projecting the number to exceed 29.35 billion in the coming decade, driven by advancements like 5G and other evolving technologies [2].

The Quantum IoT (QIoT) refers to the evolution and integration of quantum technologies within the realm of the IoT and it encompasses the use of quantum mechanic principles and quantum communication methods to exchange information by enhancing the capabilities and performance of IoT devices and networks. The next generation QIoT is able to create more sophisticated, efficient, and interconnected systems that will impact diverse sectors, including smart homes, healthcare, smart cities, industrial automation, agriculture, and beyond. It is anticipated to enable intelligent such as autonomous decision-making using Artificial Intelligence and Machine Learning (AI/ML) and context-aware applications. These intelligent devices primarily communicate through a wireless Internet on public channels, sharing private and confidential information. Consequently, ensuring security becomes a major concern to uphold data privacy, encompassing integrity, access control, confidentiality, and authentication. Integrity serves to protect information against any alterations during transmission, while confidentiality hides information from unauthorized persons. Authentication ensures that the communicating parties are legitimate and authorized to share sensitive information, while access control resists unauthorized access. To address the mentioned security concerns, various symmetric and asymmetric cryptographic techniques are employed, including the Advanced Encryption Standard (AES) and elliptic curve cryptography (ECC) for ensuring confidentiality, ECC-based digital signature (ECDSA) for integrity and authentication, and the use of public-key based Rivest, Shamir, and Adleman (RSA), Diffie-Hellman (DH) key exchange, and elliptic curve-based DH key exchange protocols. The public-key based security protocols rely on the complexity of solving mathematical number-theoretic problems, such as integer factorization problem (IFP), discrete logarithm problem (DLP), and elliptic curve DLP (ECDLP) [3], [4].

The significant advancements in quantum computing, particularly with the Shor's algorithm [5], have revealed that the traditional cryptographic techniques mentioned can be feasibly broken by solving problems such as IFP, DLP, and ECDLP. Consequently, there is a need for new approaches that are resistant to compromise by quantum computers. To counter this threat, post-quantum cryptography (PQC) and quantum key distribution (QKD) have been introduced. The BB84 protocol is one of the earliest and most well-known QKD protocols, developed by Bennett and Brassard in 1984 (hence, the name is BB84) [6]. It provides a method for two parties, traditionally referred to as Alice (the sender) and Bob (the receiver), to establish a shared secret key over a potentially insecure communication channel, such as an optical fiber or free space. The security of the BB84 protocol relies on the principles of quantum mechanics, specifically the impossibility of measuring a quantum state without disturbing it. Any attempt by an adversary, say Eve, to intercept and measure

Basudeb Bera is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: b.bera26@nus.edu.sg).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in).

Biplab Sikdar is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: bsikdar@nus.edu.sg).

the qubits would introduce errors into the transmission, which can be detected by Alice and Bob during the comparison of measurement bases. As a result, the BB84 protocol provides a method for secure key distribution that is resistant to eavesdropping attempts. Moreover, certain research [7], [8] has demonstrated that the BB84 protocol is an example of an unconditional security protocol. This indicates that the session key distributed through the BB84 protocol pertains to unconditional security keys. In classical cryptography, only a one-time pad (OTP) is capable of qualifying as an unconditional security cipher and AES-256 is also considered as quantum safe [4]. According to Statista's forecast, the QKD market revenue is projected to reach 527 million USD in 2023, with an anticipated increase to 2506 million USD, as shown in Fig. 2 [9].

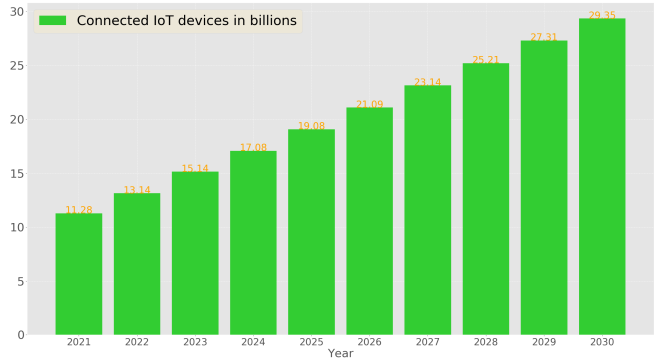

Fig. 1. Number of connected IoT devices forecast.

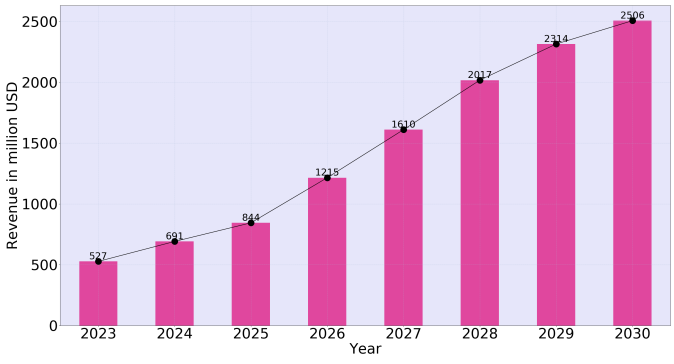

Fig. 2. Quantum key distribution market revenue forecast.

PQCs, also referred to as quantum-safe or resistant algorithms, are deemed secure cryptographic approaches against quantum computers. PQCs encompass various systems, including: 1) code-based, 2) lattice-based, 3) hash-based, 4) multivariate, and 5) isogeny-based cryptosystems (for more details, please see European Telecommunications Standards Institute (ETSI) White Paper No. 8 – "Quantum Safe Cryptography and Security") [10]. A brief description of the aforementioned cryptography is as follows.

- *Code-based cryptosystems:* This method is computationally difficult to reverse, whether by means of a classical or quantum computer, as it relies on a mathematical challenge known as syndrome decoding or error-correcting codes, such as the McEliece and Niederreiter encryption algorithms along with the associated Courtois, Finiasz, and Sendrier Signature scheme. This problem is recognized to be NP-complete when the number of errors is unbounded. The initial McEliece signature, utilizing random Goppa codes, has proven resilient over a span of 40 years under various examinations.
- *Lattice-based cryptosystems:* The focus on lattice-based problems over the past decade has highlighted their fast algorithms, offering quantum-resistant security. This systems relying on lattice hardness called Shortest Vector Problem (SVP) which involves finding the shortest non-zero vector within a lattice, and hsa been proved to be NP-hard. This approach includes systems like learning with errors (LWE), Nth order Truncated Polynomial Ring Unit (NTRU), and ring learning with errors (ring-LWE), each demonstrating strong resistance to attacks, with some schemes offering security proofs related to worst-case scenarios [11].
- *Hash based cryptosystems:* This approach provides one-time signature systems employing hash functions like Lamport-Diffie or Winternitz signatures. The security of these one-time signature systems hinges entirely on the collision-resistance property of the selected cryptographic hash function. Extended Merkle Signature Scheme (XMSS) is a contemporary hash-based scheme currently in the standardization process that leverages Merkle Trees for its structure.
- *Multivariate cryptosystems:* This comprises the Rainbow scheme, employing the complexity of solving sets of multivariate equations. Among the most favorable multivariate encryption methods is the Simple Matrix (or ABC) encryption scheme. Here, all calculations occur within a single finite field, and the decryption involves resolving linear systems, resulting in a highly efficient scheme.
- *Isogeny cryptography:* Supersingular elliptic curve isogeny cryptography involves cryptographic schemes derived from the unique properties of supersingular elliptic curves and supersingular isogeny graphs. It belongs to the family of elliptic-curve cryptography and is distinguished by its reliance on the problem of determining an explicit isogeny between two specified supersingular elliptic curves over a finite field $GF(q)$, q being a large prime. However, given an elliptic curve $E_{GF(q)}$ in Weierstrass form over a finite field and an elliptic curve point $G \in E_{GF(q)}$ of order k, it is possible to compute a cyclic separable isogeny of degree k using Velu's formulas. As of now, quantum computers do not appear to significantly simplify the task of finding isogenies.

QKD and PQC are both cryptographic approaches, but they address different aspects of cryptography and leverage distinct principles of quantum mechanics. QKD is a method of securely distributing cryptographic keys between two parties using a quantum communication channel. QKD protocols, such as BB84 and Ekert E91, utilize the principles of quantum mechanics, such as the no-cloning theorem and the uncertainty

principle, to ensure that any attempt to eavesdrop on the communication will be detectable. The security of QKD relies on the laws of physics, particularly the principles of quantum mechanics, rather than computational complexity. Whereas, PQC is designed to secure against attacks by quantum computers leveraging algorithms like the Shor's algorithm to efficiently factor large numbers, known as integer factorization problem (IFP) and solve the discrete logarithm problem (DLP). Therefore, QKD is a method for securely distributing cryptographic keys using the principles of quantum mechanics, while PQC encompasses a broader range of cryptographic algorithms designed to withstand attacks from both classical and quantum computers.

The motivation of this work is that the next-generation quantum IoT applications brings forth an urgent need for robust security measures to safeguard sensitive data and communications in IoT networks. Traditional cryptographic algorithms utilized by IoT devices are increasingly susceptible to attacks from quantum computers, posing significant vulnerabilities. QKD offers a promising solution by leveraging the principles of quantum mechanics to distribute cryptographic keys securely. Unlike classical cryptography, QKD provides unconditional security based on the fundamental laws of physics, ensuring detectability of any eavesdropping attempts on the quantum communication channel. With its efficiency in key distribution, strong guarantees of privacy and data integrity, and future-proofing capabilities against quantum threats, QKD emerges as a crucial tool for securing the next generation of quantum IoT applications, enabling organizations to build resilient and secure IoT networks in the face of evolving technological landscapes.

II. Operational Process of Quantum Key Distribution

Quantum cryptography involves transmitting random keys between two devices (sender and receiver) using photons via fiber optic cables or open air. These keys are distributed through QKD methods and followed by conventional cryptography for secure communication. QKD is a cryptographic protocol leveraging the principles of quantum mechanics to facilitate information sharing between devices. Employing both classical and quantum channels, it establishes a secret key. The quantum channel utilizes optical fibers or free space/satellite links to transmit polarized photons (referred to as quantum states of light). Simultaneously, an authenticated classical channel is employed to compare specific measurements pertaining to these quantum states. Subsequent post-processing steps are performed to refine a valid and confidential key. Both these channels operate as public channels.

Consider a scenario where a sender (S) and a receiver (R) possess specialized optical equipment to establish a quantum channel while utilizing a classical channel for exchanging specific measurements to establish a quantum key and mutually authenticate. S employs a QKD transmitter to send a stream of polarized photons to R via the quantum channel, with each photon representing one bit of information and using randomly chosen bases. At the receiver's end, R utilizes a QKD receiver to capture the photons via the quantum channel and measures each one, using his/her own randomly selected bases. Subsequently, they utilize the classical channel to exchange the bases employed for measuring each photon. They then consider the measurement values for each photon that was measured using the same basis as a secret session key, whereas the photons measured with different bases are discarded and not included in the final session key.

In the above example, we consider the use of four bases or polarized filters to create and measure photon streams, where each photon can have one of these polarizations. The bases consist of diagonal polarizations at $45°$ or $135°$ and rectilinear polarizations at $0°$ or $90°$. As a result, the choice of basis corresponding to a bit "1" or "0" can be made randomly. Similar to [12], for the bit "0", we select the $0°$ or $135°$ polarizations, while for the bit "1", we opt for the $45°$ or $90°$ polarizations. Photons with rectilinear bases that pass through the rectilinear filter (+) remain unchanged, while a diagonally polarized photon that passes through this filter changes randomly with equal probability. Similarly, when diagonally polarized photons pass through the diagonal filter (x), they remain unaltered, whereas the state of photons polarized in a rectilinear fashion randomly switches with equal probability to one of the diagonal polarizations upon passing through this filter. Initially, S starts the process by generating random bits and converting them into a photon stream or quantum states, also known as qubits, by randomly choosing bases. Subsequently, S transmits these qubits to R, who receives and measures them, without prior knowledge of the polarizations of each of S's photons. Upon receiving and computing the bits, they derive their secret key. Figure 3 illustrates the QKD process without the presence of an attacker. It is observed that the session key between S and R, represented in binary, is 01110.

Bit number	1	2	3	4	5	6	7	8	9
S's random bits	1	0	1	1	1	0	0	1	0
S's chosen bases	+	x	+	x	x	+	x	x	+
Polarized photons of S	↕	↘	↕	↗	↗	↔	↘	↗	↔
R's chosen bases	x	x	+	+	x	x	+	x	+
Polarized photons measured by R	↗	↘	↕	↔	↗	↘	↔	↗	↔
R's measured key	0	0	1	1	1	0	1	1	0
Session key		0	1		1			1	0

Fig. 3. An example of QKD process without presence of an attacker.

III. Securing QIoT Applications using QKD

In this section, we propose an architecture for IoT applications, where each IoT application is equipped for quantum computing with its smart devices for communications. We also demonstrate the establishment of an unconditionally secure quantum key between a smart device (SD) and its associated gateway node (GN). To illustrate this framework, several phases are considered, including the network model, threat model, and the quantum key exchange (QKE) protocol between SD and GN.

A. Network Model

Figure 4 presents a generalized network model for various IoT applications capable of quantum computing. Before the deployment of IoT devices, a trusted registration authority (RA) registers all SDs and GN for a particular application by providing distinct identities and quantum-resistant certificates. Two public channels are used for communication between SD and GN: a classical channel and a quantum channel. The classical channel is used for mutual authentication of the two parties and sharing bases that will be used to establish a quantum key between them. The quantum channel is used only to share polarized photons or quantum states between them. After the successful registration is complete, the entities can deploy their application and communicate to share sensing information. After collecting information from SD, GN can forward this information to the quantum servers for further processing and storage.

B. Threat Model

In this threat model, we discuss security threats that arise during quantum communication through the quantum channel, as well as threats for the classical channel. During QKE, an adversary $\mathcal{A}$ can eavesdrop on the quantum communication channel and gain a certain level of quantum information. $\mathcal{A}$ can launch a Trojan-horse attack to probe smart devices with light to gain information about the device settings and conduct a bright-light attack to manipulate the photon detectors by sending bright light to the participating devices [13]. Additionally, we consider the Dolev-Yao (DY) [14] threat model, where $\mathcal{A}$ possesses the ability to not only eavesdrop on communication messages but can also manipulate, delete, or insert malicious content into the classical communication channel. In quantum key distribution (QKD), despite its enhanced security compared to classical cryptography, there are still potential vulnerabilities in communication via the quantum channel. Some of the attacks that can be encountered include: 1) Intercept-resend attack (also known as the man-in-the-middle attack), where an attacker intercepts quantum states sent by the sender, measures them, and then resends altered states to the intended receiver; 2) Photon number splitting attack, in this attack, the attacker captures the quantum states sent by the sender, splits the photons (particles of light) into multiple copies, and measures each copy individually; and 3) Entanglement-breaking attack, where the attacker intercepts and measures one or more entangled particles in the quantum channel, thereby destroying their correct entanglement.

In addition to the specific attacks mentioned earlier, there are broader threat models and considerations that must be addressed when using the quantum channel in quantum communication protocols like QKD. These include environmental noise and channel imperfections, as quantum systems are highly sensitive to noise and disturbances from the environment. Factors such as temperature fluctuations, electromagnetic interference, and optical losses can introduce errors or compromise the security of the communication. To mitigate these threats, cryptographic techniques such as post-processing of quantum key material and error correction codes are employed to enhance the security and reliability of quantum communication protocols.

C. Quantum Channel Establishment

Establishing a quantum channel between a SD and the GD typically involves several steps including:

- *Initial Setup:* SD and the GD need to be equipped with suitable quantum communication devices capable of generating, manipulating, and detecting quantum states. These devices often include sources of entangled photons, quantum memories, optical components for state manipulation, and single-photon detectors.
- *Entanglement Generation:* The first step is to generate entangled photon pairs at each node. Entanglement is a fundamental property of quantum mechanics where the state of one particle is correlated with the state of another, regardless of the distance between them. This entangled pair forms the basis for establishing secure quantum communication.
- *Quantum Transmission:* Once entangled photon pairs are generated, one photon from each pair is sent to the other node through a quantum communication channel. This channel could be based on various physical mediums, such as optical fibers or free-space.
- *Quantum State Measurement:* Upon receiving the photons, the nodes perform measurements on them. These measurements typically involve bases chosen randomly for each photon, which are later disclosed to check for potential eavesdropping attempts.
- *Key Distillation:* After performing measurements, the nodes compare the bases used for measurement. A subset of the measurement results, for which the bases match, are used to generate a raw key. This raw key contains bits that can be used as cryptographic keys.
- *Error Correction and Privacy Amplification:* The raw key undergoes error correction and privacy amplification protocols to remove errors introduced by noise in the quantum channel and to ensure that the final key is secure against eavesdropping attempts.
- *Establishment of Quantum Channel:* The error-corrected and privacy-amplified key serves as the basis for establishing a secure quantum channel between SD and the GN. This channel can be used to transmit sensitive information or to authenticate classical communication channels.
- *Key Refreshment:* To maintain security over time, keys are periodically refreshed using new entangled pairs and the same process described above.

D. Registration Process

RA registers all SD and GN prior to deployment with the following process through a secure channel or offline phase.

- *RGP 1:* The RA picks a unique and distinct identity ID_i, a certificate $Cert_i$ for a SD, and $Cert_j$ for a GN.
- *RGP 2:* The RA selects a Gaussian distribution over the polynomial ring $Q_p = \frac{Z_p[x]}{x^n+1}$ with standard deviation δ

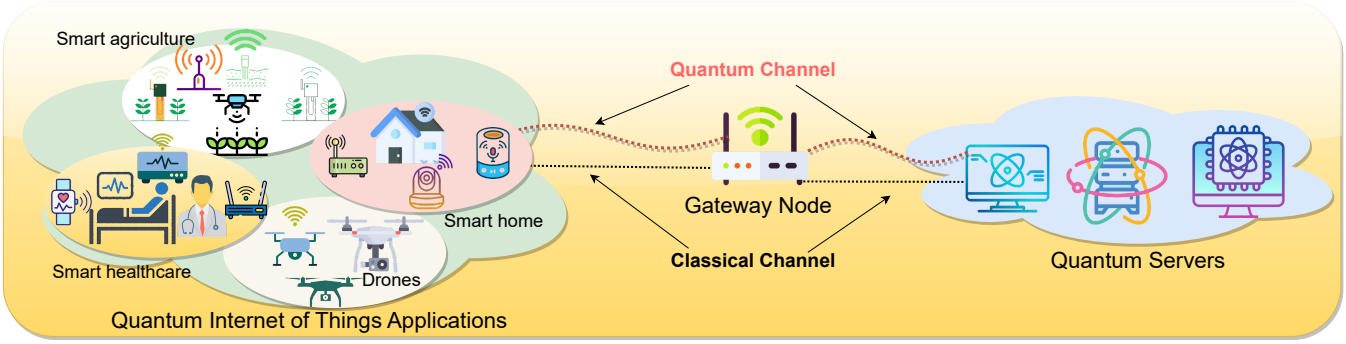

Fig. 4. Various QIoT applications.

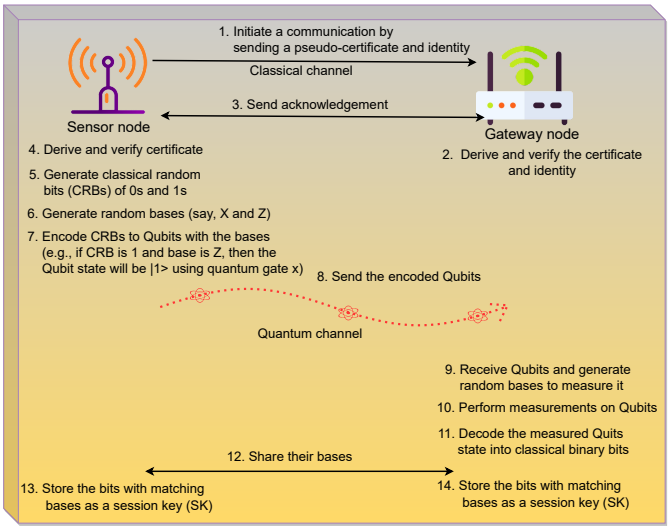

Fig. 5. Overall process for QKE between SD and GN.

denoted as χ_δ, where p is a large prime number and n is an integer n with power of two.

- *RGP 3:* The RA then randomly chooses a sample s_i for SD from χ_δ and a cryptographic hash function $h : \{0,\ 1\}^* \rightarrow \{0,\ 1\}^\gamma$, where γ denotes output length (here, SHA-256 algorithm is considered as it is quantum safe [11]).

Finally, the RA loads $\{Cert_i,\ h,\ ID_i,\ s_i\}$ into SD's memory and sends $\{ID_i,\ s_i,\ Cert_j\}$ to GN securely.

E. Proposed Quantum Key Exchange Protocol

In this section, we propose a BB84-type quantum key exchange scheme to share a quantum-secure secret key between an SD and GN. To establish this session key, the following steps are executed:

- *Step 1.* SD initiates a communication process over classical channel by picking a fresh timestamp TS_1 and generating a pseudo-certificate $Cert_i^*$ as $Cert_i^* = Cert_i \oplus h(s_i\ ||TS_1)$. Next, SD sends $\{ID_i, Cert_i^*, TS_1\}$ to the attached GN.
- *Step 2.* After receiving the message from SD, GN checks its freshness by verifying the attached timestamp. If the timestamp is verified, GN derives $Cert_i = Cert_i^* \oplus h(s_i\ ||TS_1)$ and then verifies the certificate and identity for authenticity. If all verifications are successful, GN considers SD as the authenticated party. GN picks a fresh timestamp TS_2 and generates pseudo-certificate $Cert_j^*$ as $Cert_j^* = Cert_j \oplus h(s_i\ ||TS_2\ ||TS_1)$. GN then sends its pseudo-certificate, timestamp, and verification status as an acknowledgment to SD.
- *Step 3.* SD receives the message from GN, derives the original certificate $Cert_j$ as $Cert_j = Cert_j^* \oplus h(s_i\ ||TS_2\ ||TS_1)$ and verifies its freshness and authenticity by checking its certificate. Once this verification is completed, they mutually authenticate each other.
- *Step 4.* SD then generates classical random bits (CRBs) and selects random bases (here, X and Z). Next, SD encodes the CRBs into qubits (quantum states) using one of these bases. For example, if CRB is "1" and the basis is "Z", then SD applies a quantum gate "x" and converts it to a quantum state $|1\rangle$. After that, SD sends the encoded qubits to GN over the quantum channel using a fiber optic cable or airspace.
- *Step 5.* After receiving the qubits from SD, GN generates its own random bases to measure them. GN then measures the received qubits with its own bases and decodes the quantum states into binary bits.
- *Step 6.* SD and GN now share their bases through the classical channel with each other to finalize the quantum key. After receiving their bases, each calculates the binary bits according to the matching basis and stores it as a session key. This quantum secret session key can be used in the future for AES encryption to share secret information related to QIoT applications.

A detailed description of this process is provided in Fig. 5.

IV. Security Analysis

The security of QKD relies on the fundamental principles of quantum mechanics rather than computational power. Two key concepts, the superposition principle and the no-cloning theorem, underpin the unconditional security of QKD. The superposition principle allows qubits to exist in two states simultaneously, providing a more efficient storage of information compared to classical bits. This principle enables secure quantum exchange for encryption keys over an untrusted network, making QKD virtually unbreakable. Any attempt

to eavesdrop on the communication is detectable, as the act of measuring polarized photons, which represent qubits, disturbs the information they carry. Heisenberg's uncertainty principle states that once a photon is measured or disturbed, its information is destroyed. This principle contributes to the detection of eavesdropping attempts, as any observation of the photon by an adversary ($\mathcal{A}$) results in changes that can be identified. The no-cloning theorem in quantum mechanics prohibits the perfect copying of an unknown quantum state. If an eavesdropper tries to intercept and clone quantum states, errors are introduced, revealing the intrusion.

Detection of an attacker's presence on the quantum communication channel can be achieved using the fundamental principles of quantum mechanics. In quantum communication, the act of measuring or observing a quantum state inherently disturbs the state. The receiver can utilize the *No-Cloning Theorem*, which states that it is impossible to create an identical copy of an arbitrary unknown quantum state. According to Heisenberg's uncertainty principle, measuring any quantum state changes the position and momentum of a quantum particle simultaneously. Therefore, when an attacker tries to eavesdrop on the transmitted quantum states, it induces changes. Upon receiving the altered quantum states, the receiver verifies them using shared bases, which may result in mismatches. Consequently, the receiver can easily detect the presence of an attacker in the network. In the proposed scheme, any $\mathcal{A}$ attempting to eavesdrop on the quantum communication channel can be easily detected. $\mathcal{A}$ cannot directly observe the photons without changing them, and any attempt to indirectly observe the photon through the measurements of sender (SD) and receiver (GN) is futile. SD and GN only disclose the basis used for measurement, not the final result, making it impossible for $\mathcal{A}$ to gain useful information. Consider a scenario where $\mathcal{A}$ attempts to infiltrate the system and measure SD's photons. Due to the uncertainty introduced by Heisenberg's principle, the information carried by the measured photons is destroyed, resulting in a mismatch between the measurements of SD and GN. By analyzing the traffic of transmitted photons, GN can detect eavesdropping attempts. Even if $\mathcal{A}$ tries to create and send photons to GN, it can be easily detected by verifying their bases.

$\mathcal{A}$ also cannot reveal any information from the classical channel, as the certificates are not communicated directly as plaintex form and instead of original certificates, pseudo-certificates are communicated. The original certificates are generated by the trusted authority's private key. Therefore, $\mathcal{A}$ cannot generate a fake certificate without knowing the original private key. As a result, the proposed scheme also provides security for authentication through the classical channel. The original certificate is not transmitted to prevent untraceability attacks. Instead, a pseudo-certificate is communicated over the public classical channel. Upon receiving the pseudo-certificate, the receiver can extract the original one and verify the sender's authenticity. Therefore, to mitigate the risk of untraceability attacks, we utilize pseudo-certificates during communication.

V. Implementation Results and Discussions

This section presents an implementation of QKE part of the proposed QKD protocol discussed in Section III-E using a client-server model, also known as socket programming, with the Python language. The protocol was implemented with the assistance of the available source code in [15] and utilizing well-adopted software tools such as Qiskit. Qiskit is a freely available software development kit designed for quantum computing tasks involving circuits, pulses, and algorithms. It offers functionalities for crafting and handling quantum programs, enabling their execution on prototype quantum devices via the IBM Quantum Platform or on local computer simulators (for more details, please see https://qiskit.org/).

To establish a quantum session key between the sensor and gateway nodes, they need to agree on the same quantum basis, which they share through the quantum channel. Once they have agreed on the same quantum basis, they measure and identify the matching bases. They then utilize these bases to convert the binary bits of $\{0, 1\}$ into the session key. If they encounter a measurement basis that does not match the received one, they immediately reject it and restart the process. Figure 6 shows the implementation result of the proposed scheme, where a sensor node (left side in Fig. 6), being a client, initiates the connection with a gateway node (as shown in the right side of Fig. 6), considered as a server. The sensor node generates random bits of 200 bits in length and random bases. Next, the sensor node encodes these with the bases and sends them to the gateway node. The gateway node receives and calculates accordingly and then shares its bases to finalize the session key. Finally, both establish their quantum secret key as a session key of 106 bits, as illustrated in Fig. 6. It is worth noting that the simulation produces an end-to-end latency of 0.42 seconds for establishing QKD between a sensor node SD and the gateway node GN.

VI. Conclusion

The proposed QKD in next-generation QIoT applications offers a promising avenue for ensuring the security and integrity of communication. The integration of QKD provides an unconditionally secure method for establishing a quantum key between a sensor device and a gateway node in QIoT applications, leveraging the principles of quantum mechanics to detect any potential eavesdropping attempts. The proposed QKD scheme successfully demonstrates the feasibility of its application in a client-server model for QIoT. Through the exchange of quantum states and classical information, the scheme enables the creation of a secure session key between a sensor node and a gateway node. The utilization of Qiskit and socket programming in Python showcases the practical implementation of the protocol. The scheme effectively addresses potential threats, including eavesdropping and unauthorized access, by leveraging the unique properties of quantum mechanics and adaptation of certificates. As quantum technologies continue to advance, the proposed approach sets a foundation for developing quantum-safe solutions that safeguard sensitive information in the evolving landscape of quantum-enabled IoT applications.

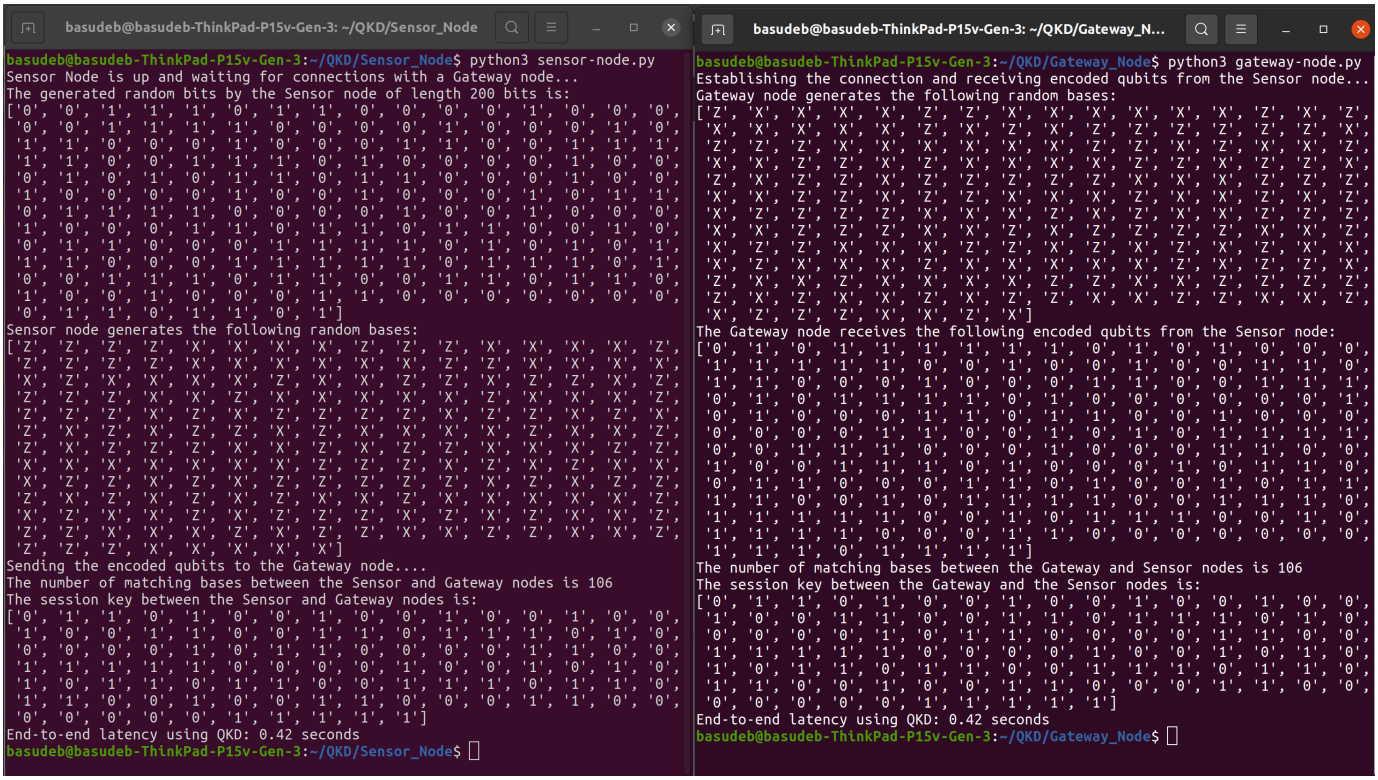

Fig. 6. Implementation of the QKD between a sensor node and a gateway node.

REFERENCES

[1] Z. Wang, D. Liu, Y. Sun, X. Pang, P. Sun, F. Lin, J. C. S. Lui, and K. Ren, "A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2292–2328, 2022.

[2] "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030," 2023, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Accessed on November 2023.

[3] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021.

[4] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116–120, 2017.

[5] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, 1997.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, Theoretical Aspects of Quantum Cryptography - celebrating 30 years of BB84.

[7] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000.

[8] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 457–475, 2003.

[9] "Quantum security market revenue worldwide from 2021 to 2030, by method," 2023, https://www.statista.com/statistics/1332840/quantum-security-market-revenue-by-method/. Accessed on November 2023.

[10] T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.

[11] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," 2016, https://doi.org/10.6028/NIST.IR.8105. Accessed on October 2023.

[12] H. A. Al-Mohammed, A. Al-Ali, E. Yaacoub, K. Abualsaud, and T. Khattab, "Detecting Attackers during Quantum Key Distribution in IoT Networks using Neural Networks," in *IEEE Globecom Workshops (GC Wkshps'21)*, Madrid, Spain, 2021, pp. 1–6, doi: 10.1109/GCWkshps52748.2021.9681988.

[13] L. Marco, S. Andrew, A. Romain, C. Christopher, I. Degiovanni, M. Gramegna, H. Atilla, H. Bruno, K. Rupesh, L. Andrew *et al.*, "Implementation Security of Quantum Cryptography-Introduction, challenges, solutions| ETSI White Paper No. 27," *ETSI*, 2018, https://hdl.handle.net/11696/59931.

[14] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[15] A. Andriievska, "Quantum Key Distribution," 2022, https://github.com/fomalhautn/Quantum-Key-Distribution/tree/main. Accessed on October 2023.

Basudeb Bera received a Ph.D. degree in computer science and engineering from International Institute of Information Technology, Hyderabad, India, in 2022. He also received his M.Sc. degree in mathematics and computing in 2014 from IIT (ISM) Dhanbad, India, and M.Tech. degree in computer science and data processing in 2017 from IIT Kharagpur, India. He is currently a post-doctoral fellow at the National University of Singapore (NUS), Singapore. His research interests are cryptography, network security, post-quantum cryptography, and blockchain technology. He has published over 34 papers in international journals and conferences in his research areas.

Ashok Kumar Das (Senior Member, IEEE) received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently a full professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He is also a visiting research professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA, in 2024.

He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate^{TM}) Highly Cited Researcher 2022 and 2023 in recognition of his exceptional research performance. His current research interests include cryptography, system and network security, blockchain, AI/ML security, and post-quantum cryptography. He has authored over 415 papers in international journals and conferences in the above areas, including over 345 reputed journal papers. He is/was on the editorial board of IEEE Transactions on Information Forensics and Security, IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), Journal of Cloud Computing (Springer), Cyber Security and Applications (Elsevier), IET Communications, and KSII Transactions on Internet and Information Systems.

Biplab Sikdar (Senior Member, IEEE) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He is a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he serves as the Head of Department of the Department of Electrical and Computer Engineering. He was a Systems Engineering at Rensselaer Polytechnic Institute from 2001 to 2013. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and an Associate Editor for the IEEE Transactions on Mobile Computing from 2014 to 2017. He is a member of Eta Kappa Nu and Tau Beta Pi.