Enhancing Wireless Sensor Network Security with Quantum-Enabled Elliptic Curve Cryptography

1st Sathish Krishna Anumula
Digital Tranformations Architect
IBM Corporation
Detroit, USA
sathishkrishna@gmail.com
[0009-0009-0613-4863]

2nd Ranganath Taware
Chief Architect,
Capgemini America Inc
Atlanta, USA
ranganath.taware@gmail.com
[0009-0008-4774-1515]

3rd Ohm Hareesh Kundurthy
Director, Application Development
Santander Bank
Boston, MA, USA
ohk609@g.harvard.edu
[0009-0000-9880-475X]

4th Ram Ghadiyaram
Independent Researcher
Celina,TX, USA
ram.ghadiyaram@gmail.com
[0009-0006-3730-0914]

5th Jaya Eripilla
Independent Researcher
Little elm , Texa, USA
jaya.eripilla@gmail.com
[0009-0005-4422-2523]

6th Shruthi Raghavendra
Independent Researcher
Santa Clarita, USA
shruthi.raghavendra@utdallas.edu
[0009-0006-6581-2159]

***Abstract*— Wireless sensor networks (WSNs) are systems made up of sensor nodes that communicate wirelessly over short distances, with adaptability and functionality at their core-essence. These networks have traits. Face challenges in devising effective strategies for identifying and thwarting attacks due to limitations, in individual sensor node processing power and the essence of wireless communication. Securing WSN poses a challenge given the constrained processing abilities of sensor nodes and the inherent nature of communication while facing various security threats that have emerged alongside the widespread adoption of these networks. To protect against these dangers it's crucial to put in place the security measures Encryption's key, to keeping data safe from unauthorized users Nevertheless not all encryption methods are equally strong as some are vulnerable Elliptic Curve Cryptography (ECC) is considered the best option due to its smaller key sizes offering strong security with efficiency in space and energy As technology advances conventional encryption techniques are seen as inadequate, for ensuring data privacy and security Utilizing principles from physics to ensure data transmission, between the sender and receiver is a groundbreaking advancement in network security known as quantum cryptography. Quantum Key Distribution (QKD) combined with ECC is highlighted in this study, for authentication processes, key management and energy efficiency. A novel method called QKD ECC has been put into practice. Compared against ECC and other encryption methods to bolster the security of WSN and safeguard the confidentiality of data exchange.**

Keywords*— *Elliptical Curve Cryptography ECC, Wireless Sensor Network WSN, Quantum Key Distribution QKD

I. INTRODUCTION

Utilizing quantum enhanced Elliptic Curve Cryptography (ECC) to bolster the security of Wireless Sensor Networks (WSNs) presents a strategy that tackles efficiency and resilience in the face of emerging quantum threats effectively. WSNs consist of sensor nodes that have limited processing capabilities and energy resources; hence conventional security measures are often not feasible, due to these constraints. ECC stands out as a favored encryption technique, in WSN setups because of its capacity to offer security with key sizes; this results in decreased computational burden and lower energy consumption when compared to alternative cryptographic methods. Maintaining effectiveness is crucial, to extending the lifespan of sensor nodes all while upholding the confidentiality and integrity of data, in communication systems. Traditional error correction codes (ECC) however effective they may be, in securing data transmissions are at risk when faced with attacks from computers that excel in solving ECCs mathematical challenges quickly through algorithms such as Shor's algorithm. To address this vulnerability and enhance security measures against threats, like eavesdropping attempts Quantum Key Distribution (QKD) techniques are combined with ECC to ensure a secure distribution of cryptographic keys utilizing the principles of quantum mechanics. This unique approach not fortifies the distribution process but also aids in establishing reliable authentication and managing keys efficiently within the constraints of Wireless Sensor Networks (WSN).QKD implementations enhanced by ECC have demonstrated energy efficiency and security results when compared to using ECC alone.The integration of both methods enables effective data transfer to address risks, in WSN environments where quantum computing threats are a concern [1] [2].

Moreover research is being conducted into encryption methods, for communications in wireless sensor networks (WSNs) such as lattice based cryptography. Despite this exploration of postquantum cryptography protocols like lattice-based cryptography for securing WSN communications, elliptic curve cryptography (ECC) remains dominant due to its efficiency and ability to use key sizes making it well suited for the limited resources of sensor nodes. New studies have looked into incorporating postquantum protocols into mechanisms using approaches like DTLS showcasing the possibility of integration without negative impacts, on energy efficiency. Implementations, like utilizing caching certificates as part of optimization tactics can effectively lower the computational workload and enhance communication efficiency in real world scenarios involving advanced security protocols, for wireless sensor networks. Quantum enhanced ECC emerges as an approach to boost WSN security. It combines the efficient features of ECC with the secure key exchange methods of quantum cryptography. This advancement signifies a step, towards

security setups for sensor networks, in the era of quantum technology [3].

II. Related Work - Encryption Methods in WSN Security

A. Conventional Cryptographic Approaches

Traditional cryptographic methods encounter challenges in WSNs due to the resource constraints of sensor nodes, including limited processing power and battery life [3]. The increasing number of resource-constrained devices in IoT environments further complicates data privacy, necessitating strong and efficient cryptographic solutions [4]. This creates a trade-off between security complexity and energy consumption, where enhanced security measures often lead to increased battery drain [5]. Relying solely on conventional encryption and key management becomes impractical given the dynamic nature of WSNs. To address these security limitations, researchers are exploring energy-efficient and algorithm cryptographic hardware, with domain-specific configurability, hence providing the necessary flexibility [6]. Certain Hybrid approaches, like combining a Hash-Function (HF) along with Elliptic Curve Cryptography (ECC), has a promising avenue for optimizing both security and energy efficiency in WSNs [7].

B. Elliptic Curve Cryptography (ECC) for WSNs

ECC helps in securing WSNs, its ability to provide robust security with smaller key sizes, making it suitable for resource-constrained devices [8]. In IoT-enabled WSNs, ECC is an essential for ensuring data integrity and privacy during transmission [8], and researchers are exploring Two-Factor Authentication (2FA) techniques that integrate ECC with fuzzy verifiers to overcome the limitations of current authentication methods [8].In IoT-enabled WSNs, ECC is essential for ensuring data integrity and privacy during transmission [8], and researchers have explored Two-Factor Authentication (2FA) techniques that integrate ECC with fuzzy verifiers to overcome the limitations of existing authentication methods [8]. This integrated approach leverages the flexibility of fuzzy verifiers with the cryptographic strength of ECC, creating a user-friendly authentication system that balances robust security with computational efficiency, which is critical for WSNs given their limited processing capabilities and vulnerability to various attacks [8]. D. Malan et al. demonstrated the practical viability of ECC in WSNs through its implementation on the MICA2 mote [9], showing that public-key infrastructure, previously deemed impractical, could be used for distributing TinySec keys; however, despite these benefits, existing ECC techniques raise security concerns related to computational costs and potential vulnerabilities, leading to the exploration of hybrid approaches, such as combining a Hash-Function (HF) with ECC, to optimize both security and energy efficiency. In some of the applications like smart grids, where communication between smart meters and neighborhood area networks is susceptible to attacks, ECC-based authentication schemes can be developed to provide privacy-preserving and lightweight security [10], security-enhanced user authentication protocols using ECC to reduce resource consumption and bolster security in WSNs [11] can be employed. The algorithm can be explained with an *elliptic curve* as a plane over a finite field (with real numbers) which consists of the points satisfying the equation $y^2 = x^3 + ax + b,$ (an elliptic curve representation)

along with a distinguished point at infinity which is denoted ∞. The coordinates are chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation would be somewhat more complicated.

This set of points, combined with the group operation of elliptic curves, is an abelian group, with the point at infinity as an identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety: $\mathrm{Div}^0(E) \to \mathrm{Pic}^0(E) \simeq E.$ where E represent the Identity element.

The gap highlights limitations in existing ECC-based approaches for WSNs particularly with respect to high computational delays, inefficient power consumption, poor bandwidth optimization, and network congestion. There are several research are adequately addressing these ineffectiveness, avoidance of WSNs vulnerable for encryption attacking and not able to meet practical performance demands. This research seeks to bridge these gaps by introducing enhanced authentication by QKD scheme with ECC. It integrates quantum mechanism with ECC as hybrid asymmetric cryptography may generate high secure, efficient solution tailored to WSNs.

C. Quantum Key Distribution (QKD) Application in WSN Security

- *Fundamentals of Quantum Key Distribution*

Quantum Key Distribution (QKD) offers a method for secure communication through the principles of quantum mechanics, establishing cryptographic keys with theoretical unbreakability, which addresses the increasing need for robust security in wireless networks [12]. By utilizing quantum mechanics, this approach aims to provide enhanced key security, surpassing the capabilities of traditional cryptography [12]. While QKD provides security, Post-Quantum Cryptography (PQC) focuses on algorithms designed to withstand attacks from both classical and quantum computers [13]. R. Bedington, J.J et al. proposed a hybrid security model, integrating post-quantum cryptography with quantum cryptographic techniques to enhance resilience against both classical and quantum computing threats [14]. However, the implementation of QKD encounters challenges, including technological limitations, integration complexities with existing network infrastructure, and cost considerations [12], [14], which must be addressed for its widespread adoption in WSNs and other applications. The integration of QKD with ECC leverages the strengths of both methodologies, presenting an approach to address security challenges in WSNs while maintaining efficiency [7]. A Work Flow Method of QKD-ECC combination can is shown in Fig 1.

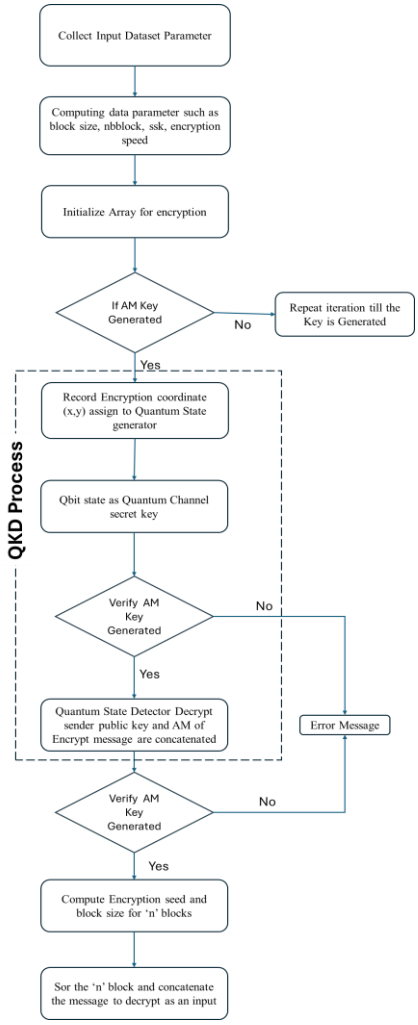

Fig. 1. Workflow of hybrid cryptography method QKD-ECC in Wireless Sensor Networks

D. *Practical Implementations and Field Tests of QKD*

Real-world applications of QKD are demonstrated through field tests, such as the urban, open-air implementation using entangled light from a semiconductor nanostructure, showcasing the potential of quantum-dot entangled photon sources beyond laboratory environments [14]. N. Walenta et al. presented a 625 MHz clocked coherent one-way QKD system that employs wavelength multiplexing [15]. Moreover, the integration of six QKD systems into a mesh-type network in a metropolitan area facilitated secure TV conferencing over a distance of 45km, demonstrating features such as eavesdropper detection and secure path rerouting [16]. These implementations highlight QKD's capacity to enhance security in communication infrastructures [12], and researchers are exploring its integration with emerging technologies like 6G networks to improve overall security [17]. Although challenges, such as cost, distance limitations due to atmospheric losses [14], and integration with existing networks [18], remain, these advancements are crucial for future secure communication networks. An Algorithm in the context of users can be shown in the Fig. 3 below.

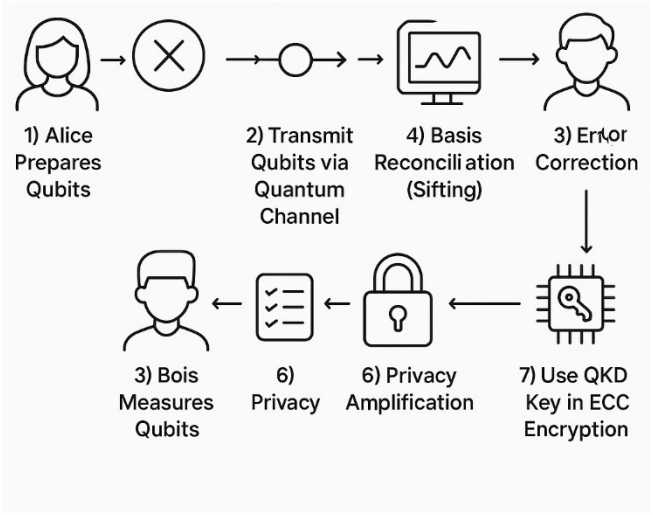

Fig. 3. User Interaction of BB84 QKD Protocol Integrated with ECC for WSNs

E. *Challenges in QKD Implementation*

Despite the potential of QKD, its practical application, particularly within WSNs, faces challenges [14]. These challenges include limitations in secret key rate, distance, size, and cost, which impede its widespread adoption [14]. Ground-based QKD systems are further constrained by atmospheric losses and in-fiber attenuation, restricting their feasibility for global distribution networks [14]. Deploying QKD in specific contexts, such as smart grids, presents difficulties due to the distances between control centers [18].

III. METHOD - INTEGRATION OF QKD WITH ECC: TOWARDS ENHANCED WSN SECURITY

A. *Quantum Key Distribution Principles*

Quantum cryptography is often linked with a protocol, within the wider scope of cryptography fieldwork. Due to its role in ensuring communication channels Quantum Key Distribution (QKD) is commonly linked with symmetric encryption methods. Typically, the quantum key generated through QKD can serve as a session key in systems employing algorithms like AES. The encrypted nature of the key transmitted via QKD enhances the security of cryptosystems by safeguard it against potential attacks, from quantum adversaries. Technological progress, in Quantum Key Distribution (QKD) is seen as the cornerstone of quantum cryptography and cybersecurity technology advancements using principles to generate communication keys between trusted parties without the need for traditional quantum assets like channel preparation and measurement equipment often involving polarization at both ends of the communication link between Alice and Bobs devices. In order for QKD to work effectively specific assumptions about the devices used by the communicating parties are essential with two assumptions playing a role, in this process. The tools used to create and assess quantum states must be dependable which is essential, for systems that engage with long distance quantum communication methods like scaling quantum networks, teleportation and repeaters.

Photon measurements play a role, in the BB84 protocol requiring implementation to ensure strong artificial randomness, for security purposes.The various methods proposed for generating numbers basedon quantum states offer an opportunity to improve security in this context.
The steps involved in Quantum Key Distribution (QKD) are as outlined below.

The generation of keys begins during the generation process.

- The process of creating a key involves leveraging the principles of quantum mechanics to generate the initial quantum key.
- The quantum key has undergone refinement to enhance its security incorporating measures such, as privacy amplification and error correction to ensure its integrity and protection, against threats.
- The use of authentication methods guarantees that communication is both secure and error free.
- An extra layer of security has been added to safeguard the content due, to the sensitivity of the key.

B. Final Encryption:

The final symmetric key is derived from the quantum key. Is used for encryption purposes. Final Encryption refers to the encryption of data using keys, which's a conventional method that ensures a secure communication channel is established. The Quantum Key Distribution (QKD) process involves stages starting with creating qubits and then moving to assessing and comparing them among users. Moreover Recurrent, in the procedure is the detection of errors in data reconciliation leading to the creation of a key. The fundamental principle of quantum mechanics forms the basis for QKD making it inherently resistant to threats posed by quantum computers. While conventional methods such as RSA are vulnerable to attacks by quantum computing techniques QKD maintains its security, in these scenarios. QKD enables two users to securely swap keys. Typically when two parties engage in communication they use a designated channel and a pre agreed upon authentication key to ensure the security of transmitting each quantum packet. This process results in the creation of a quantum cryptography key which is then further processed using methods to produce a single key that is theoretically secure, from a data perspective. The security of Quantum Key Distribution (QKD) lies in its ability to detect and respond to any attempts, at eavesdropping by changing the state of particles when interfered with. Ensuring that authorized users can create the most secure key possible.

C. Potential Benefits of Combined Approaches

The convergence of QKD and ECC offers a strategic advantage in reinforcing the security of WSNs, without sacrificing operational efficiency [7]. This synergy capitalizes on the distinct strengths inherent to each cryptographic approach. QKD introduces a layer of unconditional security rooted in the fundamental principles of quantum physics [12], effectively addressing vulnerabilities at the key exchange level. Complementing this, ECC contributes computational efficiency through its utilization of smaller key sizes [8], an essential attribute for resource-constrained WSN environments. The open nature of wireless communication makes WSNs susceptible to eavesdropping and malicious attacks [19], necessitating robust security measures. By integrating QKD with ECC, a more fortified and streamlined security framework can be realized for WSNs.

D. Implementation Considerations and Energy Efficiency

When integrating QKD and ECC into WSNs, a primary challenge is maintaining energy efficiency due to the limited power resources of sensor nodes [5]. Traditional security measures can significantly complicate essential WSN operations, such as data aggregation, due to increased energy consumption [3]. Therefore, optimizing energy usage is crucial for the practical deployment of these advanced cryptographic techniques in WSNs.

Implementing cryptographic functions requires performing operations across various mathematical domains, including integers modulo N, binary Galois fields, and non-super singular elliptic curves, all with programmable parameters [6]. J. Goodman and A. Chandrakasan noted that energy consumption is a critical design parameter, with some processors consuming up to 75 mW at 50 MHz and 2V, while energy usage can be reduced to as little as 525 μW in ultralow-power mode [6]. Efficient key management is also essential for secure and energy-effective data transfer within WSNs, particularly in resource-constrained environments [7]. The need for energy-efficient solutions has driven research into algorithm-agile cryptographic hardware that provides the required flexibility without incurring high overhead costs [6]. Furthermore, hardware implementations of security protocols, such as DTLS (Datagram Transport Layer Security), can significantly improve energy efficiency compared to software implementations, enabling end-to-end security for IoT devices with minimal energy consumption [20].

E. Security Enhancements through QKD-ECC Integration

The convergence of QKD and ECC offers a calculated method to reinforce WSN security without undermining operational efficiency [7]. QKD employs quantum mechanics to establish cryptographic keys, providing theoretical unbreakability and addressing vulnerabilities during key exchange [12]. Complementarily, ECC contributes computational efficiency through its utilization of smaller key sizes, an essential attribute for resource-constrained WSN environments [8]. Given the open nature of wireless communication, WSNs are susceptible to eavesdropping and malicious attacks [19]; therefore, integrating QKD with ECC creates a more resilient security framework.

The rising demand for robust security measures has driven exploration into technologies like QKD to bolster security in emerging networks, such as 6G [17]. Moreover, integrating PQC with quantum cryptographic techniques presents a hybrid security model designed to withstand both classical and quantum computing threats [13]. Classical cryptographic methods, including RSA and Elliptic Curve cryptography, face potential vulnerabilities to cyberattacks from quantum computers, highlighting the importance of PQC algorithms in safeguarding inter-node communication in WSNs [4].

Advanced secure wireless communication protocols can be achieved by integrating post-quantum cryptography, specifically Kyber's key encapsulation method [5].

F. Elliptic Curve Triangulation

The non-singular elliptic curve that allowed for certain parametrization with rational point is illustrated in equation 1

$$y^2=x(x-r1)(x-r2) \quad (1)$$

Area S of triangle include side "a, b, c" considered in the elliptic curve is illustrated in equation 2.

$$S=\sqrt{sp(sp-a)(sp-b)(sp-c)} \quad (2)$$

The semi-perimeter sp is represented as formulae in equation 3.

$$sp=a+b+c2 \quad (3)$$

Figure 2 illustrate the parameter T that introduced and illustrated in equation 4.

$$T=sp-asp \quad (4)$$

Simplify by dividing S2 by sp2 in elliptic curve is represented in equation 5.

$$y^2 = x[x^2+Ax+B] = x(x-r1)(x-r2) \quad (5)$$

We have for coordinates (x, y) of a point on elliptic curve shown in equation 6.

$$\begin{cases} x = tbc = \frac{p-a}{p}bc \\ y = \frac{S_{abc}}{p^2} \end{cases} \quad (6)$$

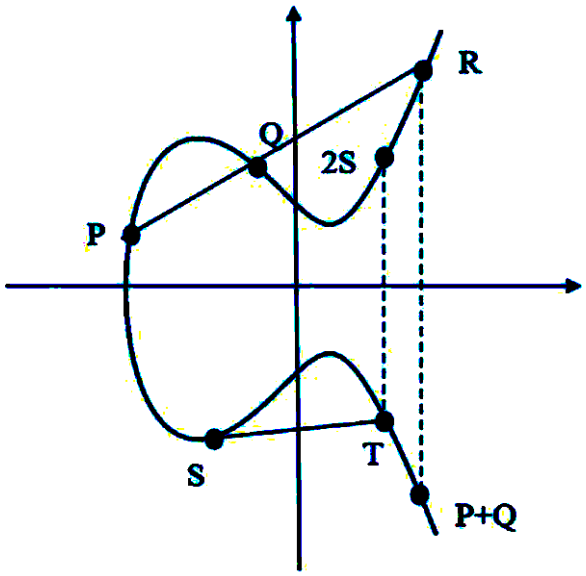

Figure 3. Elliptical Curve Triangulation

Elliptic curve roots, coefficients and triangle sides are related through is represented in equation 7.

$$\begin{cases} r1r2 = B = (a-b)(a-c) \\ r1+r2 = -A = 2bc - a(b+c) \end{cases} \quad (7)$$

This represents the triangle rational sides and area S whereas the rational points on the curve with coordinates (x, y) are available in equation 3.6. Let we initiate the triangle with rational sides by expressing side b and c functions, of curve coefficients A and B that keep side a of triangle (a,b,c) as free parameter. Based on the first equation from equation 7 assist in determining root and curve coefficients derived is shown in equation 8.

$$\begin{cases} b = \frac{A-ac}{a-2c} \\ b+c = \frac{A-2c^2}{a-2c} \end{cases} \quad (8)$$

Moreover, second equation of equation 7 is used to find the equation for c is shown in equation 9.

$$ac^2+c(A-2(a^2-B))-a(A+B)=0 \quad (9)$$

For discriminant D, the equation 10 is formulated as

$$D=(A+2B)^2+(2a)^2(1-2A-3B) \quad (10)$$

Hence, the side C formulated is shown in equation 11.

$$C = \frac{2a^2-2B-A\pm\sqrt{D}}{2a} = f(a, D(A,B)) \quad (11)$$

Similarly, the side b is formulated as shown in equation 12.

$$b = \frac{A-ac}{a-2c} = g(a, D(A,B)) \quad (12)$$

Thus, the term A and B is expressed with respect to triangle side (a, b, c) and obtain the following for the discriminant D is shown in equation 3.13

$$D= 4a^3(b+c)-8a^4+7a^2(b^2+c^2)-20a^2bc+4a^2-12a(b+c)+16bc \quad (13)$$

Given side a is rational and D is a square of integer or rational number, sides c and b will be rational too, thereby giving us triangle △(a,b,c) with rational sides.

- Algorithm of QKD-ECC method
  - Key generation and raw quantum key
  - Implementing AM
  - Verifying AM
- Enhanced authentication of encryption process
  Entity P is linked to a specific elliptic curve set of domain parameters as *D = (a, b, n, D, G, l, FR)*, where *E* (F_{qf}) denotes the elliptic curve *E* in the quantum finite field F_{qf} with prime order *l*. Point P then follows these steps.
  Step 1: Selection of value to *d in the* range [1, *n*−1].
  Step 2: Computing $S=dP_k$,
  Where,
  P_k= private key
  S = public key
- Improved Nonce Management
  Step3: Use a secure random number generator to ensure the nonce k is unique and unpredictable for each signing operation.
  Step4: Consider using a deterministic approach (like RFC 6979) where *k* is generated based on the private key and the message hash:
  Compute $k = HMAC_K(H(m))\bmod n$, where *K* is derived from the private key.
- Key generation of AM in encryption process
  The domain parameters *Q*, entity *P and* message m are defined as *Q= (FR, a, b, n, D, G, q)* Steps required to be considered for entity *P*
  Step 1: Selection of k value from the range [1, *n*−1].
  Step 2: Computing $K_P= (X_1,Y_1)$, g=$X_1 \bmod n$. When *g* = 0, return to Step 1.
  Step 3: Calculate $k^{-1} \bmod n$.
  Step 4: Computing $s=k^{-1}(Q(m)+dg) \bmod n$; when *h*=0, return to Step 1.
  The integer pair (*g, h*) generates the authentication for the message *m*.

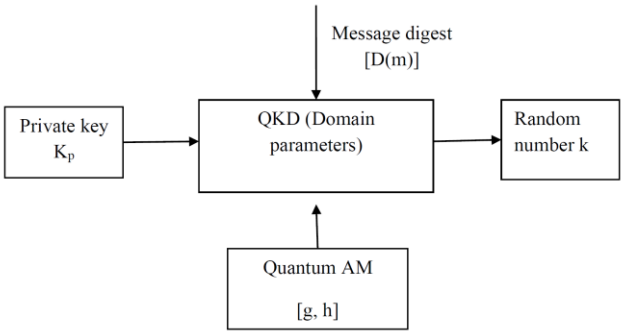

Figure 4: Generation of Quantum AM

- Quantum AM of decryption process

Verifying AM key (*g, h*) for message (*m)* using entity *P* 's signature, entity *R* will utilize the public key *S* as well as domain parameters *D = (FR, b, a, h, n, G).* The verification process is as follows:

Step 1: Ensure that the values *g, h* are within the range [1, $n-1$].

Step 2: Compute $\omega=h^{-1}$ mod n, $D(m)$.

Step 3: Calculate $u_1= D(m).\omega$ mod n.

Step 4: Calculate $u1= g \ . \ \omega$ mod n.

Step 5: Determine the point $(X_0,Y_0)= u_1P_k+u_2S$ and compute $v=X_0$,mod n.

If $v=g$, authentication key get accepted as valid.

- Given multiple signatures $\sigma_i=(g_i,h_i)$ messages m_i:
  - Compute

$$\omega i= h_i^{-1} mod\ n$$

$$u_{1i} = \mathrm{D}\ (m_i)\ \omega_i mod\ n$$

$$u_{2i} = g_i\omega_i mod\ n$$

- Compute the aggregated elliptic curve point

$$V= \sum_{i=1}^{m}(u_{1i}G + u_{2i}S)$$

- Verify by checking $r' = xV$ mod n

If g′ = gi for all authentication key and get valid.

- Multi-Signature Schemes
  - Implement a multi-signature scheme where a message must be signed by *t* out of *n* participants.
  - The aggregate signature can be constructed as:

$$h = \sum_{j=1}^{t} h_j \bmod n$$

- Each participant computes their own signature, and a final verification can check if: $g' = x_V$ mod n

The whole process is represented in figure 4 – for enhanced Authentication.

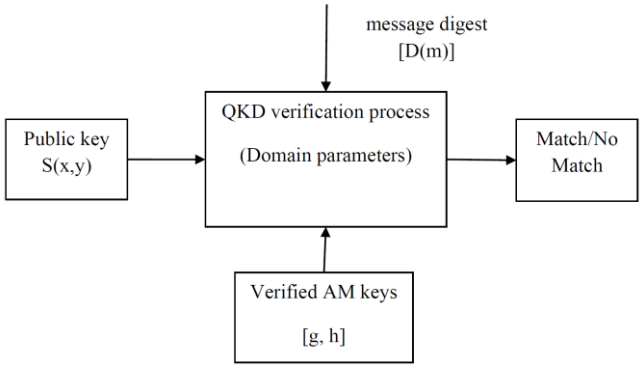

Figure 5 Enhanced authentication Digital Signature Verification

IV. Result and Discussion

The NS3 simulator was used in evaluation of EAECC technique within IEEE 802.15.4 Zigbee networks, sme of the key metrics focused were: encryption and decryption time, throughput, and energy consumption. The results confirmed EAECC's performance advantage over RSA and Sengupta's technique, particularly in throughput and congestion management. EAECC optimizes security and efficiency, with strong throughput and minimal encryption and decryption time consumption, hence making it a suitable choice for secure and high-performance communication in IEEE 802.15.4 networks.

QKD-ECC has consistently achieved higher throughput than RSA and EAECC method that calculated as the data size divided by the total time for encryption and decryption. This improvement was evident across various data sizes (115 to 1150 bytes), highlighting QKD-ECC ability has efficiently handle larger data packets without sacrificing speed.

Total throughput=Data size (bytes) / Time taken for encryption and decryption process (S) (14)

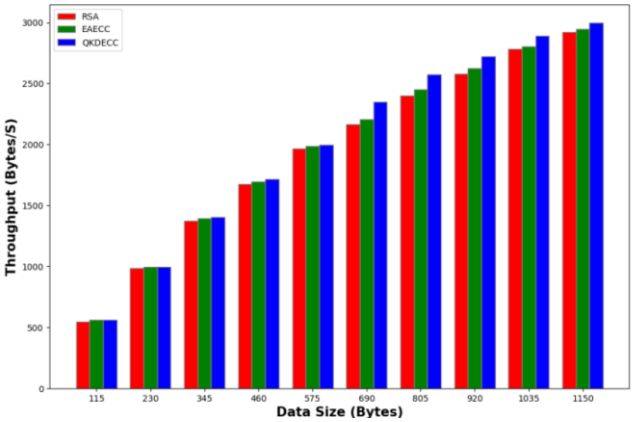

Figure 6 Throughput comparison of QKD-ECC with other cryptography technique

Figure 6 shows a comparison of throughput (in bytes per second) for proposed QKD-ECC with other cryptography technique such as EAECC and RSA across different data sizes. QKD-ECC consistently outperforms than other two methods, particularly as data size grows indicating higher efficiency in data transmission with very minimum loss of packets

- **Encryption and Decryption performance**

QKD-ECC demonstrated lower encryption and decryption times compared to the other techniques. This reduction translates into lower computational demand which is crucial for power-constrained networks like Zigbee, and ensures the network's overall efficiency.

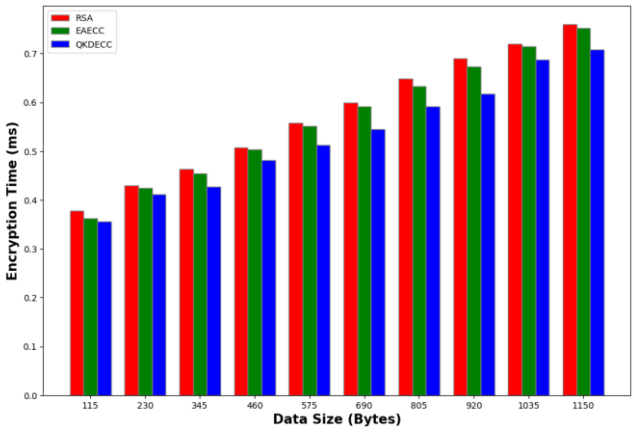

Figure 7 Encryption time comparison of QKD-ECC other cryptography techniques

Figure 7 illustrates the encryption time of proposed QKD-ECC with existing EAECC and RSA in which encryption time consumed for all data sizes are very low in QKD-ECC while compared to other existing EAECC and RSA. Hence, the safer data transmission is done with less time consumption.

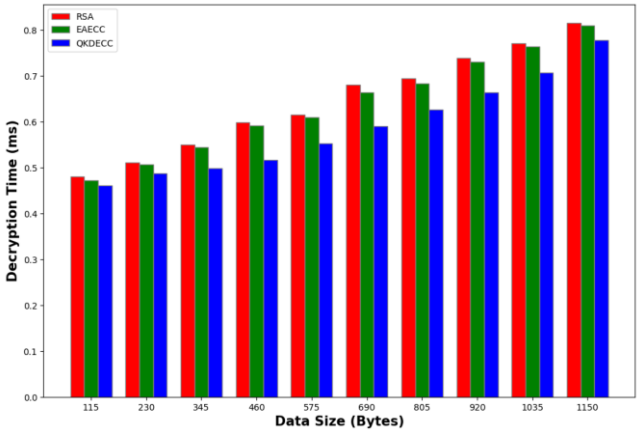

Figure 8 Decryption time comparison of QKD-ECC other cryptography techniques

Figure 8 illustrates the decryption time of proposed QKDECC with existing EAECC and RSA in which decryption time consumed for all data sizes are very low in QKD-ECC while compared to other existing EAECC and RSA. Hence, the safer data transmission is done with less time consumption.

V. Future Directions and Research Gaps

A. Post-Quantum Cryptography

The potential of quantum computers to compromise network security by solving complex cryptographic problems has spurred research into PQC, which focuses on developing encryption methods resistant to both classical and quantum computing attacks [6]. One promising approach is lattice-based cryptography (LBC), which employs computationally challenging lattice problems to establish robust cryptographic functions, offering resistance to quantum attacks, high performance, and parallelism [6]. Looking ahead to the development of 6G wireless networks, expected around 2030, Shimaa A. B.Tharani et al. note that PQC is slated for integration alongside artificial intelligence and machine learning [7]; such integration will necessitate a re-evaluation of current security methods, emphasizing novel authentication, encryption, and access control mechanisms to ensure trustworthiness and privacy in future networks [8], and also the integration of quantum-resistant methods alongside machine learning algorithms [9]. S. A. Chaudhry highlights that QKD offers a revolutionary method to secure communication by leveraging quantum mechanics to ensure the theoretical unbreakability of cryptographic keys [10].

B. Emerging Approaches for WSN Security

Machine learning (ML) presents a promising avenue for bolstering security services within WSNs through continuous monitoring and intelligent decision-making [11]. However, the implementation of ML algorithms is not without its challenges. A significant hurdle lies in the extensive training data and computational resources required, especially considering the resource-constrained nature of WSN nodes [12]. Traditional intrusion detection systems (IDS) are becoming less effective against increasingly sophisticated attacks [12]. Consequently, deep learning (DL)-based IDS are being explored, trained on specialized datasets to identify various denial-of-service (DoS) attacks, demonstrating promising results in experimental evaluations [12].

WSNs, integral to the IoT, face diverse cyberattacks, necessitating robust security measures [13]. Due to their unique limitations, including constrained power, storage, and processing capabilities, designing effective attack prevention and detection techniques is complicated [13]. To address these challenges, researchers are exploring the integration of ML and blockchain (BC) technologies to develop lightweight security frameworks that offer both cyberattack detection and prevention [14]. The goal is to create solutions that are less computationally demanding, ensuring the viability and longevity of WSNs in security-critical applications [14].

C. Research Gaps and Future Opportunities

Several research gaps exist in the integration of QKD with ECC for WSN security:

- *Implementation in Resource-Constrained Environments:*

Addressing the integration of QKD and ECC for WSN security necessitates further investigation into several key areas. Adapting QKD, which is generally designed for broader applications, to the resource-constrained environments of WSNs remains a significant challenge [18]. P. Kong suggests that there are considerable opportunities for tailoring QKD implementations to WSNs, given the limited research on specific applications such as smart grids. The complexity of QKD network technologies also highlights the need for precise and scalable simulation tools [15], with M Sasci et al. proposing that simulation environments with multiple links and nodes are crucial for thoroughly analyzing routing protocols and evaluating network performance. The necessity for robust defense mechanisms to reinforce wireless network security is paramount [16], including addressing authenticity, confidentiality, integrity, and availability. C. Wang et al. have proposed security-enhanced user authentication protocols leveraging ECC to minimize

resource consumption and strengthen security within WSNs [16], while Shaykhah S. Aldosari and Layla S Aldawsari emphasize employing PQC algorithms to safeguard inter-node communication in WSNs against potential cyberattacks from quantum computers [17]. Furthermore, P Kong et al. highlight the potential of quantum secure direct communication (QSDC) to defend against quantum computing threats [18], underscoring the importance of continued research into QSDC's theoretical underpinnings and experimental validation.

- *Scalability Challenges:*

As QKD networks expand in complexity, the need for robust simulation tools becomes increasingly apparent for assessing the practicality and anticipating the challenges associated with QKD implementations [19]. The highlights QKD's potential to revolutionize secure communications [19], and the importance of ongoing research to improve the security and efficiency of WSNs. Advanced simulation technologies facilitate the analysis of routing protocols and the evaluation of network performance, which is crucial for the advancement and secure operation of QKD networks [20]. These simulations aid in understanding the trade-offs between enhanced security measures and operational performance [21], which are essential for deploying secure and efficient WSNs, and they can also be used to examine security vulnerabilities and devise effective defense mechanisms for enhancing overall wireless network security [21]. S. S. Aldosari et al. note that the practical implementation of QKD technologies faces significant challenges, including technological limitations and the need for global standardization [21].

- *Practical Security Guarantees:*

In light of the potential vulnerabilities of conventional cryptographic methods like RSA and ECC to emerging quantum computing capabilities, the exploration and implementation of advanced security measures have become increasingly critical [22]. QSDC presents a promising avenue by enabling the secure transmission of secret messages through quantum channels, effectively mitigating inherent vulnerabilities in quantum computing [23]. Current research efforts are dedicated to establishing the theoretical underpinnings and practical validation of QSDC, with a focus on detailing communication protocols and secure information transfer methodologies [25]. Furthermore, the development of PQC algorithms is essential for protecting inter-node communication in WSNs against quantum threats [23], while the incorporation of QKD into future 6G systems demonstrates potential for bolstering security [23]. These advancements, underscored by ongoing research aimed at enhancing the security and efficiency of WSNs and the transformative potential of QKD, highlight the necessity for continued exploration and development in quantum-resistant security solutions.

- *Standardization and Interoperability:*

Wireless networks, characterized by radio propagation, inherently differ from wired networks, creating an open environment accessible to both authorized and unauthorized entities. This openness increases susceptibility to malicious activities, necessitating a thorough analysis of security vulnerabilities and the development of effective defense mechanisms [24]. Key security requirements encompass authenticity, confidentiality, integrity, and availability [24], and while traditional cryptographic methods, particularly those based on symmetric key cryptography, have been foundational, they may not fully address the complex security needs of WSNs, especially regarding secure node replenishment. E merging solutions, such as PQC, offer a promising avenue for safeguarding inter-node communication against potential cyberattacks from quantum computers, while the integration of ML, Quantum Computing and blockchain technologies is being explored to create lightweight security frameworks for attack detection and prevention [24]. The importance of ongoing research to improve the security of WSNs, and D. Pan highlights QKD's potential to revolutionize secure communications [25].

VI. Conclusion

WSNs encounter a variety of security risks because of their limitations, in processing power and communication abilities. These inherent constraints make security methods like asymmetric cryptography less effective, in WSN settings. ECC has become a choice because it needs bits and offers better security, than other methods that use different keys for encryption and decryption processes; this makes it a good fit for places with limited resources available for use in their operations or activities. Several systems that focus on authentication and managing keys built around ECC have been created to increase security measures without compromising on energy efficiency. With the progress made in the field of quantum computing technology recently; there is concern that ECC based systems might not be as resistant to potential cyber-attacks, in the future. QKD provides a groundbreaking method, for enhancing security using principles of mechanics to develop encryption that's theoretically impenetrable. The BB84 protocol and its different versions have been thoroughly. Put into practice in networks to show the increasing sophistication of this technology. Despite its advancements QKD encounters hurdles in terms of application, scale up. Compatibility with current networks. Exploring the combination of QKD with ECC shows potential for improving security, in WSNs. By merging the efficiency of ECC with the safety of QKD, in this method can tackle the distinct obstacles in WSN environments effectively. The study, in this field is continuously progressing as different combined methods are suggested and tested.

We should concentrate on tackling the real-world obstacles of combining QKD and ECC in environments, with resources in studies and work towards creating standardized procedures for secure quantum WSN systems while also delving into how these technologies can impact different application fields as quantum computing progresses further, along the line.

References

[1] J. . Elfarahati, T. Pašić, E. Kurtanović, A. Ferhatović, E. Šabotić, and A. Abd Almisreb, “Review of Wireless Sensor Network security ”, Defense and Security Studies, vol. 6, no. 1, pp. 25–38, Feb. 2025.

[2] M. Faris, M. N. Mahmud, M. S. M. Salleh, A. Alnoor, "Wireless sensor network security: A recent review based on state-of-the-art works," International Journal of Engineering Business and Management, 2022. https://doi.org/10.1177/18479790231157220

[3] D. Kar, H. L. Ngo, G. Sanapala, "Applied Cryptography for Security and Privacy in Wireless Sensor Networks," International Journal of

Information Security and Privacy, 2009. https://doi.org/10.4018/jisp.2009100702

[4] D. A. F. Saraiva, V. Leithardt, D. D. Paula, A. S. Mendes, G. Villarrubia, P. Crocker, "PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices," Italian National Conference on Sensors, 2019. https://doi.org/10.3390/s19194312

[5] R. Ahmad, R. Wazirali, T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," Italian National Conference on Sensors, 2022. https://doi.org/10.3390/s22134730

[6] R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," IoT, 2021. https://doi.org/10.3390/IOT2010005

[7] B. Tharani, B. P. Devi, "Optimizing Energy Efficiency and Security in Wireless Sensor Networks with a Hybrid HF-ECC," 2024. https://doi.org/10.1109/ICACCS60874.2024.10716923

[8] T. Sudhakar, R. Praveen, V. Natarajan, "An efficient ECC and fuzzy verifier based user authentication protocol for IoT enabled WSNs," Scientific Reports, 2025. https://doi.org/10.1038/s41598-025-94550-9

[9] D. Malan, M. Welsh, M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," 2004. https://doi.org/10.1109/SAHCN.2004.1381904

[10] S. A. Chaudhry, K. Yahya, S. Garg, G. Kaddoum, M. M. Hassan, Y. B. Zikria, "LAS-SG: An Elliptic Curve-Based Lightweight Authentication Scheme for Smart Grid Environments," IEEE Transactions on Industrial Informatics, 2023. https://doi.org/10.1109/TII.2022.3158663

[11] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," Italian National Conference on Sensors, 2014. https://doi.org/10.3390/s140610081

[12] M. I. Alghamdi, "A Review on Quantum Key Distribution for Wireless Networks: Current Status and Future Prospects," Communications on Applied Nonlinear Analysis, 2024. https://doi.org/10.52783/cana.v32.2516

[13] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, A. Fabuyide, "Quantum Cryptography And U.S. Digital Security: A Comprehensive Review: Investigating The Potential Of Quantum Technologies In Creating Unbreakable Encryption And Their Future In National Security," 2024. https://doi.org/10.51594/csitrj.v5i2.790

[14] R. Bedington, J. M. Arrazola, A. Ling, "Progress in satellite quantum key distribution," 2017. https://doi.org/10.1038/s41534-017-0031-5

[15] N. Walenta et al., "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," 2013. https://doi.org/10.1088/1367-2630/16/1/013047

[16] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network.," Optics Express, 2011. https://doi.org/10.1364/OE.19.010387

[17] C. Wang, A. Rahman, "Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges," IEEE wireless communications, 2021. https://doi.org/10.36227/techrxiv.14785737.v1

[18] P. Kong, "A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security," IEEE Systems Journal, 2022. https://doi.org/10.1109/jsyst.2020.3024956

[19] Y. Zou, J. Zhu, X. Wang, L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," Proceedings of the IEEE, 2015. https://doi.org/10.1109/JPROC.2016.2558521

[20] U. Banerjee, A. Wright, C. Juvekar, M. Waller, .. Arvind, A. Chandrakasan, "An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications," IEEE Journal of Solid-State Circuits, 2019. https://doi.org/10.1109/JSSC.2019.2915203

[21] S. S. Aldosari, L. S. Aldawsari, "PQ-LEACH: A novel post-quantum protocol for securing WSNs communication," International Journal of Engineering Business and Management, 2024. https://doi.org/10.1177/18479790241301163

[22] V. Mavroeidis, K. Vishi, M. Zych, A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," arXiv.org, 2018. https://doi.org/10.14569/IJACSA.2018.090354

[23] S. A. A. Hakeem, H. H. Hussein, H. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," Italian National Conference on Sensors, 2022. https://doi.org/10.3390/s22051969

[24] S. S. Ismail, D. W. Dawoud, H. Reza, "Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review," Future Internet, 2023. https://doi.org/10.3390/fi15060200

[25] D. Pan et al., "The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet," IEEE Communications Surveys and Tutorials, 2023. https://doi.org/10.1109/COMST.2024.3367535