Design and Development of Quantum and ML-Based Cryptography System for SoC Applications

V L Prasanna Dhulipudi, G. Sivaradje

Department of Electronics and Communication Engineering, Puducherry Technological University, India
Email: prasannadhulipudi14@gmail.com

Abstract: In recent decades, quantum computing-based cryptography has become the latest and more secure for sending of data through different protocols that could be wired or wireless in communications. To optimize power dynamic and static utilization in digital circuits, Machine Learning (ML) and Quantum computing are playing a major role in designing and implementing cryptography systems. The combination of these two techniques will increase the security level and be used for key authentications and integrity. Quantum Key Distribution (QKD) along with ML enables the communicating parties to detect the side channel effects and protection of keys from noisy channels. To guarantee two parties have access to significant sections of the key, the QKD creates random keys for private and public data transmission. The SHA-256 generates 256-bit hash values that are used for authenticating the signatures and data on the fly so that encryption and decryption can process their operation without waiting for hash values as private and public keys. The proposed design has been validated using benchmarking the overhead and measured performance degradation and shown their suitability for SoC and FPGA systems.

Keywords: ML, QKD, SoC, SHA-256 and Cryptography.

1. Introduction

From cutting-edge developments in QML and explores their unique applications in wireless communications. Beginning with a foundational exploration of quantum computing principles, proceeds to dissect various operations and techniques essential for QML implementations. Special attention is devoted to distinctive methods inherent to quantum computing, such as quantum search algorithms, and their potential contributions to enhancing the performance of wireless systems. The complexity of electronic control systems in quantum computing has surged alongside the advancement of qubit technologies, which now employ larger qubit arrays with heightened fidelity targets. This delves into assessing efficacy of modern SoC architectures in meeting intricate control demands inherent in executing quantum gates on trapped-ion qubits, with a keen emphasis on intra- SoC communication [1]. The sophistication of electronic control systems in quantum computing has seen a remarkable rise alongside the progress in qubit technologies. Today, these systems utilize larger arrays of qubits with higher fidelity targets [2]. This piece explores the effectiveness of modern SoC architectures in meeting the intricate control demands involved in executing quantum gates on trapped-ion qubits, with a particular focus on intra-SoC communication [3].

Quantum machine learning represents a pioneering approach wherein quantum computers harness data for learning purposes. Although still in its nascent stages, this field holds promise for surpassing classical machine learning algorithms in efficiency [4]. One of its primary strengths lies in lever- aging the immense parallelism inherent in quantum computers. Consequently, quantum machine learning algorithms stand poised to glean insights from data at a significantly accelerated pace compared to classical counterparts [5]. Additionally, they exhibit prowess in handling datasets of staggering size or

complexity, scenarios where classical algorithms falter. For instance, quantum algorithms could grapple with datasets too expansive to be accommodated within the memory of classical computers [6]. Despite facing numerous hurdles before practical application, the potential rewards are substantial. Success in quantum ML could potentially transform landscape of ML and exert far-reaching impacts across diverse realms of science and technology [7].

ML endeavors to craft models that glean insights from past experiences without explicit programming. The applications of machine learning are boundless, encompassing tasks such as pattern recognition, trend prediction, and decision-making, all adept at handling vast amounts of multi-dimensional data represented as large vectors and tensors [8]. However, executing these operations on classical computers demands substantial time and computational resources [9]. In contrast, Quantum Computers (QCs) leverage qubits, capable of simultaneously holding combinations of 0 and 1 through superposition and entanglement [10]. This attribute empowers QCs to efficiently handle and process large tensors, rendering them ideal for implementing ML algorithms. While many ML models for QCs draw from concepts of their classical computing counterparts, harnessing the potential of QCs often elevates them to superiority [11]. This provides an overview of current landscape of ML applications on QC, examining the acceleration and complexity advantages afforded by quantum machines. The rapid advancement of machine learning technology is driving the autonomy of devices within industries. However, the proliferation of sensors in industrial settings generates massive amounts of data, which machine learning algorithms leverage to enhance the performance of autonomous devices [12]. Nevertheless, traditional machine learning algorithms and hardware setups struggle to efficiently process this vast data for real-time applications. Consequently, researchers have turned to QC hardware systems and QML algorithms to accelerate processing. This study offers review of QC mechanisms and QML algorithms deployed for image classification. Through performance evaluations, various QML algorithms were compared, demonstrating their ability to classify images faster than classical ML algorithms in terms of processing time.

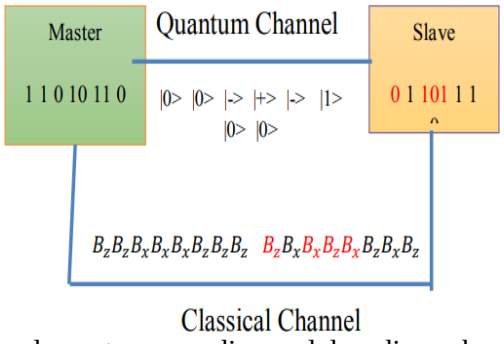

Fig. 1: Proposed quantum encoding and decoding schematic diagram

2. ML AND QUANTUM CRYPTOGRAPHY FOR SOC APPLICATIONS

ML has emerged as a powerful tool in enhancing cyber- security, including applications in SOCs. Here's how ML can be used in SOC applications are Anomaly Detection, where ML algorithms can analyze massive amounts of data to identify abnormal patterns and activities that may indicate a security breach or cyber-attack. This helps SOC teams in early threat detection and response. Predictive Analysis, ML models can be trained to predict potential security threats based on historical data, enabling proactive measures to be taken to mitigate risks. Behavioral Analysis, ML algorithms can continuously learn and adapt to normal network and user behaviors, enabling the identification of deviations that may signal security issues. Automation of Routine Tasks, ML can automate repetitive tasks in the SOC, such as filtering false positives, prioritizing alerts, and optimizing incident response processes, thereby allowing security analysts to focus on more complex tasks.

Quantum cryptography leverages principles of quantum mechanics to create secure communication channels, offering an innovative approach to securing data. Here's how quantum cryptography can be applied in SOC environments are QKD enables the creation of encryption keys with provable security guarantees based on quantum properties. This can be used to secure communication channels within the SOC and between different entities, ensuring confidentiality and integrity of the exchanged data Post Quantum Cryptography deals with the looming threat of quantum computers breaking traditional

cryptographic schemes, post-quantum cryptography, which includes quantum-resistant algorithms, is becoming increasingly relevant in SOC applications to ensure long- term security of sensitive information. Quantum cryptography offering a new level of protection for sensitive SOC communications and data transfers. Quantum cryptography techniques can be used to detect unauthorized tampering with transmitted data, providing an additional layer of security for critical information in SOC environments.

The master and slave want to share important information other than random numbers like secret photos, important passwords, and any other useful information, to provide security to them, required a lot of memory, and area and uses more power, hence hybrid approaches like ML and QKD are used to optimize. The QKD-based encryption uses module 2 addition between information and key, the key is generated by quantum computing. To increase the security level, each bit of the private key is encrypted with each bit of information i.e. master and slave can run out of bits from the key so they can exchange a new key to increase maximal privacy, the new key is nothing but One Time Programming (OTP) key. The analysis also extends to the practical applications of these quantum algorithms and their implications for ongoing research in machine learning. Additionally, the challenges and advantages of implementing ML algorithms on quantum computers are discussed, with quantum computers characterized by their unique capability to perform operations on large tensors and vectors efficiently, thanks to qubit superposition and entanglement. This attribute is in stark contrast to classical computers that require exponentially more time and resources for the same tasks as shown in Fig.1.

Finally, the text touches on PQC and the efforts to standardize these technologies to safeguard against the im- pending quantum threat. It gives particular attention to the implementation of lattice-based PQC solutions, showcasing enhanced performance through multicore processing architectures. In summary, the text weaves an intricate narrative about the convergence of quantum computing, machine learning, and enhanced security frameworks, presenting a forward-looking view of how these advanced technologies are poised to reshape digital and computational landscapes. It underscores the progressive strides being taken across various sectors to harness the power of quantum computing in addressing some of the most pressing computational challenges of modern times in Fig 2.

Here, the focus is particularly on the efficiency of modern SoC architectures, which are crucial for the functioning of these quantum systems, analyzing their intra-SoC communication, latency, and throughput as shown in Fig.3. In the context of ML, the text breaks down the distinctions between classical ML on traditional computers and quantum machine learning on quantum computers. The latter are posited as superior due to their ability to handle massive data sets through quantum parallelism and entanglement, potentially outperforming classical algorithms that struggle with similar loads. The narrative transitions into a discussion of how quantum computing significantly expedites data processing capabilities necessary for today's industrially autonomous devices arrays and meet increasingly rigorous fidelity requirements.

Fig.4 illustrates the calculation method for each neuron within the dense layers. The weights used are specified in the Jupyter notebook. Denoted as wnk where 0¡k¡n-1 and n are the number of neurons; these weights correspond to the inputs xk originating from the previous layer. The output of a neuron is determined by computing a weighted sum of its input values from the previous layer, augmented by a bias term. Subsequently, this sum undergoes an activation process, which involves applying an activation function. In this case,

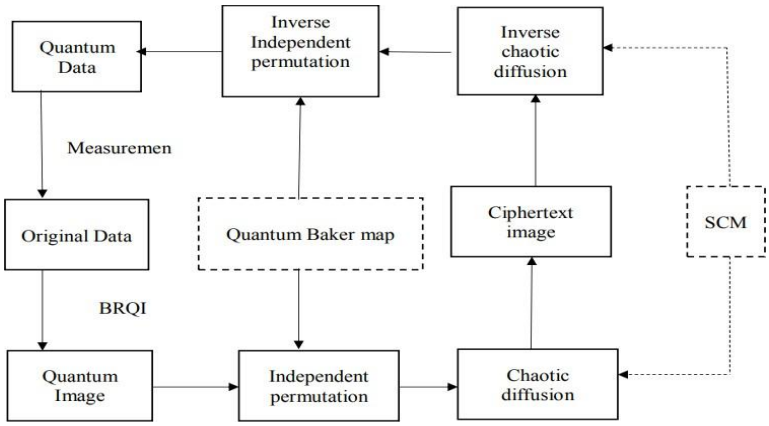

Fig. 2: The block diagram of proposed quantum cryptosystem

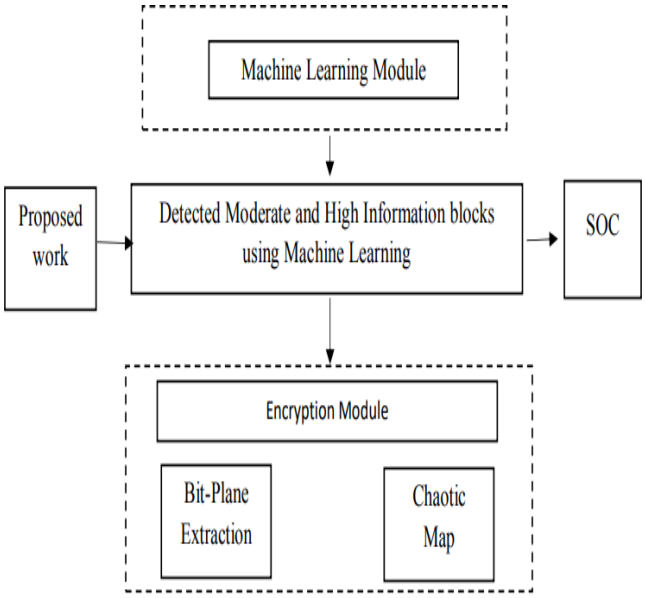

Fig. 3: Machine Learning Encryption for SoC Applications

the activation function employed is the ReLU (Rectified Lin- ear Unit) function. Specifically, the ReLU function outputs the same integer if the neuron's computed value is positive. Conversely, if the computed value is negative, the output of the neuron after activation is zero.

3. RESULTS & DISCUSSION

For each qubit, Alice randomly chooses between the standard basis and the Hadamard basis to encode it. She records the basis used for each qubit but does not disclose this information to Bob. Alice sends the encoded qubits to Bob over a quantum communication channel as shown in Fig.5. Due to quantum principles (like the uncertainty principle), any attempt by Eve to measure these qubits introduces errors that Alice and Bob can detect. Upon receiving each qubit, Bob randomly chooses to measure it in either the standard basis or the Hadamard basis. Bob records his measurement basis for each qubit. After the transmission phase, Alice and Bob communicate publicly (over a classical channel) to reveal which bases they used for each qubit. They discard qubits where they used different bases and estimate the error rate caused by Eve's potential interference. From the remaining qubits where Alice and Bob used the same basis, they extract a secure cryptographic key. By comparing a subset of their bits to estimate the error rate (due to Eve's interference), they can apply error correction techniques to obtain a final secure key. The provided data outlines in Table.1 various performance metrics and resource utilization for different components within a hardware design or system. For instance, the" uut (QKD BB84 8bit)" component demonstrates a significant allocation of resources, with 7850 Slice LUTs and 5155 Slice Registers indicating robust logic and register utilization. It also features 773 F7 Muxes and 8 F8 Muxes, highlighting its complexity in routing and multiplexing tasks. Moreover, it utilizes 42 Block RAM Tiles and 42 DSPs, indicative of its data processing and storage capabilities. In contrast, the" NN (neural network)" component focuses heavily on Slice LUTs (5903) and Slice Registers (1501), crucial for neural network computations, with minimal reliance on F8 Muxes (0) and Block RAM Tiles (0), suggesting a different architectural emphasis. It does, however, utilize 725 F7 Muxes, essential for managing connectivity within the neural network model. Similarly," ip ila (ila 0)" and" dbg hub (dbg hub)" exhibit varying resource distributions, with" ip ila" using a significant number of Slice Registers (2125) and" dbg hub" focusing more on Slice LUTs (463) and Slice Registers (723), reflecting their respective functionalities in debugging and interfacing logic analysis as shown in Fig.5. Each component's specific resource al- location underscores its role and operational characteristics within the overall system design. These metrics are vital for optimizing FPGA designs, ensuring efficient use of resources while meeting design constraints. They provide insights into how components distribute across FPGA resources, guiding designers in refining designs for better performance and resource utilization. Monitoring these percentages helps maintain FPGA stability and performance, allowing for adjustments to enhance overall system efficiency and functionality. Understanding these utilization patterns aids in achieving optimal FPGA implementation for diverse application requirements. The power consumption of proposed work is0.144 Watts as shown in Fig 6&7.

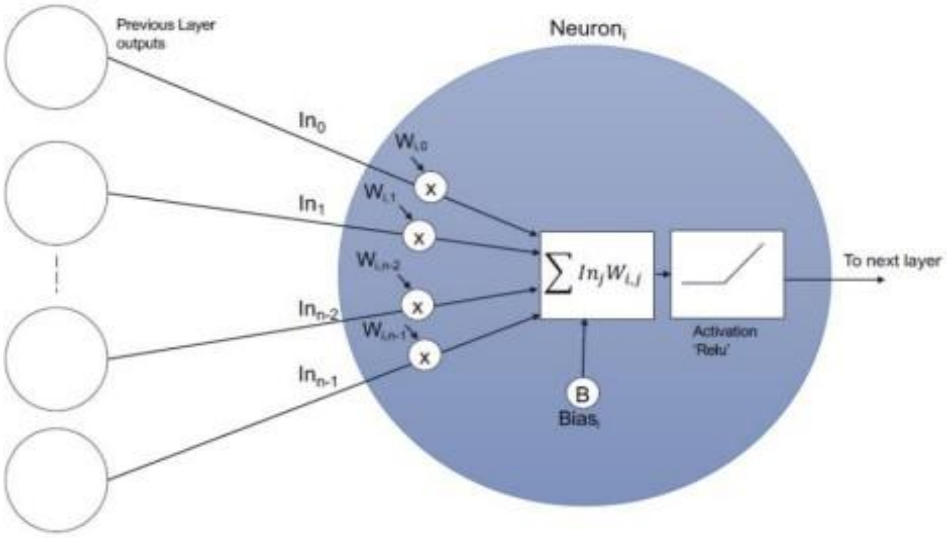

Fig. 4: Architecture of ML based neural network for training and testing of data bases

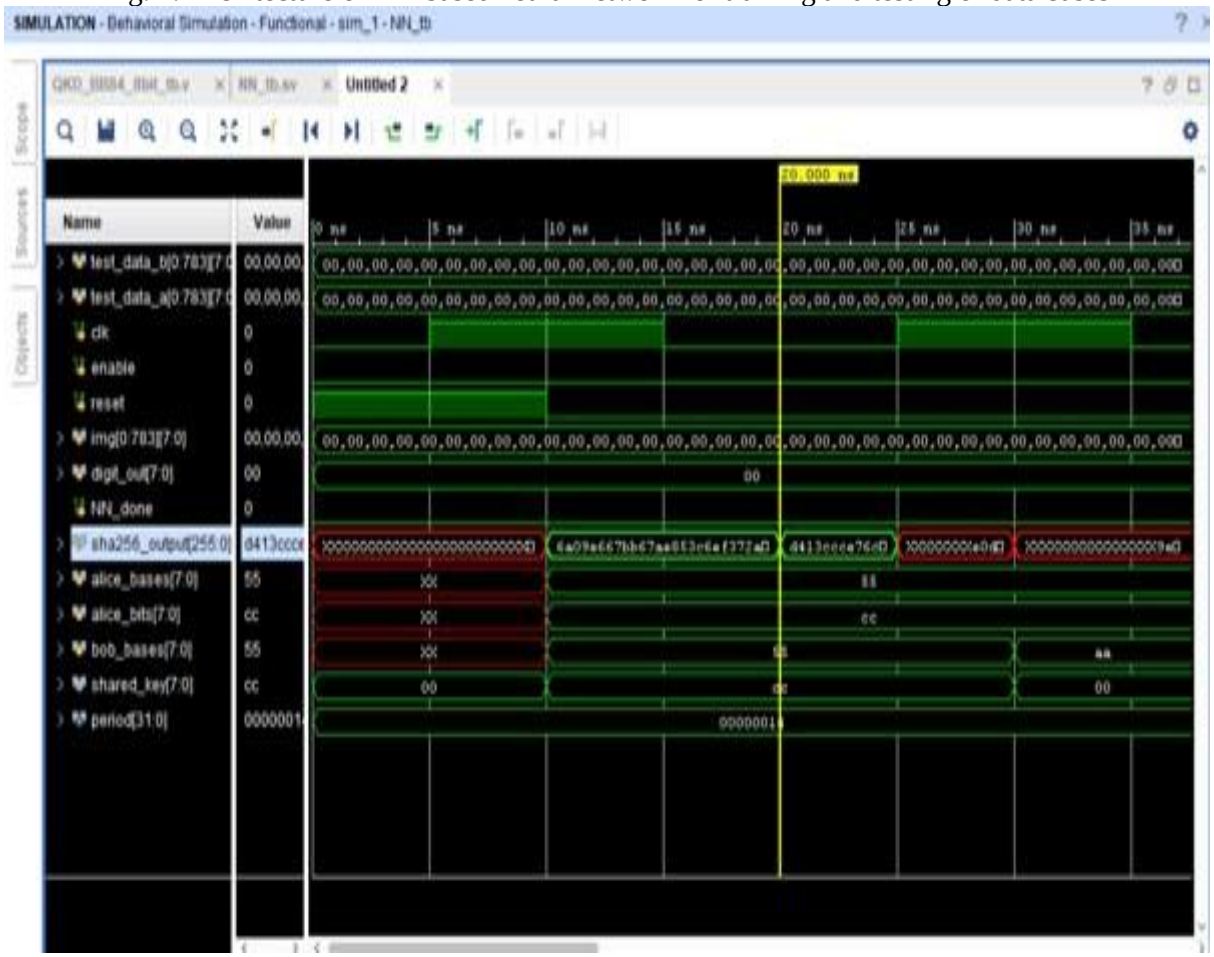

Fig. 5: Simulated results of proposed QKD and SHA-256 at SoC level.

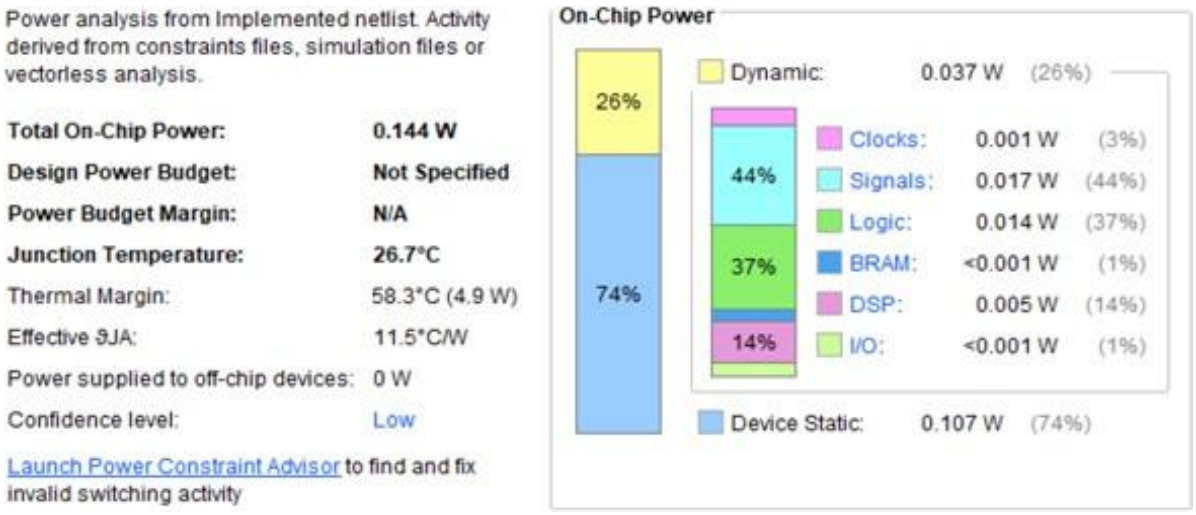

Fig. 6: Power consumption of proposed SoC system

TABLE I: Hardware Utilization Summary for Proposed and Existing Works

Component	Slice LUTs	Slice Registers	F7 Muxes	F8 Muxes	LUT as Logic	LUT as Memory	LUT Flip-Flop Pairs
top_SoC	7850	5155	773	8	3100	7499	351
uut (QKD_BB84_8bit)	486	806	0	0	197	480	6
NN (Neural Network)	5903	1501	725	0	2078	5903	0
ip_ila (ila_0)	998	2125	48	8	591	677	321
dbg_hub (dbg_hub)	463	723	0	0	244	439	24
Existing Work [3]	9802	6514	891	12	3801	8951	472
Existing Work [7]	9302	6401	982	13	3943	9320	563

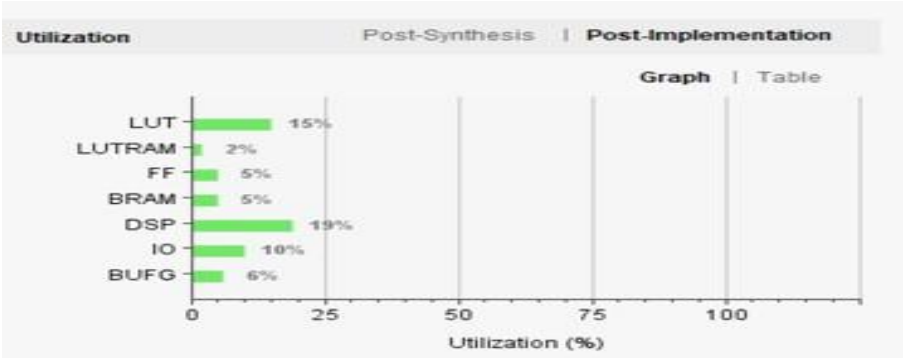

Fig. 7: Power consumption of proposed SoC system

4. CONCLUSION

The integration of quantum cryptography in SoC applications offers unprecedented levels of security by leveraging principles of quantum mechanics, such as QKD and quantum-resistant algorithms. This ensures that sensitive data transmitted within SoC systems remains secure against potential threats posed by quantum computing and traditional cryptographic attacks. The" uut (QKD BB84 8bit)" component demonstrates a significant allocation of resources, with 7850 Slice LUTs and 5155 Slice Registers indicating robust logic and register utilization. It also features 773 F7 Muxes and 8 F8 Muxes, highlighting its complexity in routing and multiplexing tasks. Moreover, it utilizes 42 Block RAM Tiles and 42 DSPs, indicative of its data processing and storage capabilities. ML in Cryptography Furthermore, the incorporation of machine learning in cryptography enhances the adaptability and robustness of security measures within SoC applications. ML algorithms can effectively detect anomalies, predict security breaches, and optimize cryptographic key management, thereby fortifying

the overall resilience of SoC- based cryptographic systems.

References

1. Design and Analysis of Digital Communication Within an SoC- Based Control System for Trapped-Ion Quantum Computing" in IEEE Transactions on Quantum Engineering, vol. 4, no. 01, pp. 1-24, 2023.
2. S. N. Pushpak and S. Jain," An Introduction to Quantum Machine Learning Techniques," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-6, doi: 10.1109/ICRITO51393.2021.9596240
3. B. Saju, M. K. Gopal, B. Nithya, V. Asha and V. Kumar," Analysis on Role of Quantum Computing in Machine Learning," 2022 Fourth International Conference on Cognitive Computing and In- formation Processing (CCIP), Bengaluru, India, 2022, pp. 1-8, doi: 10.1109/CCIP57447.2022.10058679.
4. S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi and A. Amirlatifi," Machine Learning Algorithms in Quantum Computing: A Survey," 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 2020, pp. 1-8, doi: 10.1109/IJCNN48605.2020.9207714
5. P. Kuppusamy, N. Yaswanth Kumar, J. Dontireddy and C. Iwendi," Quantum Computing and Quantum Machine Learning Classification – A Survey," 2022
6. M. T. N, A. Hiremath, N. M, S. -L. Peng, S. M. R and P. S. K," A Survey on Machine Learning Techniques Using Quantum Computing," 2022 Fourth IEEE 4th International Conference on Cybernetics, Cog- nition and Machine Learning Applications (ICCCMLA), Goa, India, 2022, pp. 200-204, doi: 10.1109/ICCCMLA56841.2022.9989137
7. J. -R. Jiang," A Quick Overview of Quantum Machine Learning," 2023 IEEE 5th Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2023, pp. 301-304, doi: 10.1109/ECICE59523.2023.10383149.
8. I. Manan, F. Rehman, H. Sharif, N. Riaz, M. Atif and M. Aqeel," Quantum Computing and Machine Learning Algorithms - A Review," 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS), Karachi, Pakistan, 2022, pp. 1- 6, doi: 10.1109/ICONICS56716.2022.10100452.
9. P. Kuppusamy, N. Yaswanth Kumar, J. Dontireddy and C. Iwendi," Quantum Computing and Quantum Machine Learning Classification – A Survey," 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Goa, In- dia, 2022, pp. 200-204, doi: 10.1109/ICCCMLA56841.2022.9989137.
10. A. Jhanwar and M. J. Nene," Enhanced Machine Learning using Quan- tum Computing," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2021, pp. 1407-1413, doi: 10.1109/ICESC51422.2021.9532638.
11. Savo G. Glisic; Beatriz Lorenzo," Quantum Machine Learning," in Artificial Intelligence and Quantum Computing for Advanced Wireless Networks, Wiley, 2022, pp.543-591, doi: 10.1002/9781119790327.ch12.
12. M. Ahmadian, M. Ruiz, J. Comellas and L. Velasco," ML-Aided SOP Compensation to Increase Key Exchange Rate in QKD Systems," 2023 23rd International Conference on Transparent Optical Net- works (ICTON), Bucharest, Romania, 2023, pp. 1-5, doi: 10.1109/IC- TON59386.2023.1020741