Journal of VLSI circuits and systems
RESEARCH ARTICLE
Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 7, No. 2, 2025 (pp. 77-83)
WWW.VLSIJOURNAL.COM

Quantum-Inspired VLSI Architectures for Secure Cryptographic Signal Processing in Next-Generation AI-Enabled Hardware Systems

N. Shanmugapriya[1]*, Sotvoldiev Xusniddin Ibragimovich[2], Jumaboyeva Marhabo Rustamboyevna[3], Rakhmatullaev Ilkhom Rakhmatullayevich[4,5], Azim Khalilov[6], Shakhboz Meylikulov[7], Ibragimkhodjaev Bakhodir[8]

[1]Department of Computer Applications, DR. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India.
[2]Department of Information Processing and Management Systems, Fergana State Technical University, Tashkent State Technical University, Uzbekistan.
[3]Department of Data Transmission Networks and Systems, Urgench State University, Urgench 220100, Uzbekistan.
[4]Department of Exact Sciences, Kimyo International University in Tashkent, Tashkent, Uzbekistan.
[5]Digital Technologies and Artificial Intelligence Development Research Institute, Tashkent, Uzbekistan.
[6]Department of Agronomy, Navoi State University of Mining and Technology, Navoi, Uzbekistan.
[7]Department of Information Technology and Exact Sciences, Termez University of Economics and Service, Termez, Uzbekistan.
[8]Department of Medicine, Faculty of Medicine, Alfraganus University, Uzbekistan.

KEYWORDS:
Quantum-Inspired VLSI,
Secure Cryptographic Hardware,
AI Accelerators,
Signal Processing,
Reversible Logic,
Low-Power Architectures

ARTICLE HISTORY:
Received: 05.08.2025
Revised: 18.09.2025
Accepted: 07.12.2025

DOI:
https://doi.org/10.31838/JCVS/07.02.10

Abstract

The sudden advent of AI-driven platforms and smart cyber-physical systems has placed ever-greater demands on hardware frameworks capable of delivering quantum-inspired processing, secure cryptographic processing, and efficient signal processing, all at once. Conventional VLSI architectures are constrained by deterministic logic models that do not reflect the probabilistic characteristics of the quantum-inspired algorithms and advanced cryptographic models. To fill this gap, this work introduces a single quantum-inspired VLSI optimised to implement secure signal processing in next-generation AI hardware. The suggested system will combine approximate probabilistic computing blocks, reversible-logic embedded datapaths, and lightweight quantum-state emulation units to aid in increasing security, decreasing power usage, and supporting parallel cryptographic transformations. The optimization methods based on machine learning are applied to explore architectures, allowing reconfiguration of cryptographic workloads, neural inference workloads, and signal-processing workloads dynamically. The use of 5 nm and 7 nm technology nodes leads to simulation studies that show great improvement in throughput-per-watt, encryption latency, and resistance to side-channel vulnerabilities. The architecture also minimises signal-processing overhead and significance of cryptographic diffusion properties, which are important to edge AI deployments. The given work provides an addition of a scalable quantum-inspired design model that can bridge the gap between traditional VLSI and new postquantum computing requirements and provide secure, energy-efficient, AI-operated hardware systems that can support defense, autonomous infrastructures, and future Internet of Things.

Authors' e-mail ID: spriyanatrajan@gmail.com, sotvoldiyevxusniddin82@gmail.com, jumaboyevamarhabo@gmail.com, ilhom9001@gmail.com, azimxj1981@gmail.com, shaxboz_meyliqulov@tues.uz, b.ibragimxodjayev@afu.uz

Authors' ORCID IDs: 0000-0002-0394-0909, 0000-0002-3802-4724, 0009-0007-8070-2908, 0000-0002-4872-4265, 0000-0002-6646-2174, 0009-0008-4220-8009, 0009-0003-8139-9892

How to cite this article: N. Shanmugapriya et al., Quantum-Inspired VLSI Architectures for Secure Cryptographic Signal Processing in Next-Generation AI-Enabled Hardware Systems, Journal of VLSI Circuits and System, Vol. 7, No. 2, 2025 (pp. 77-83).

Introduction

The new AI-enabled hardware architectures are in demand to compute secure cryptographic tasks as well as challenging signal-processing tasks in real time. Applications such as autonomous vehicles, defence communications, and smart IoT infrastructure require energy-efficient hardware platforms that can run high-throughput inference pipelines and provide a high level of security against cyberattacks. The customary VLSI designs to support deterministic logic and the more orthodox encryption designs tend to fail to provide computational efficiency as well as the cryptographic resilience at current technology nodes. With the decrease in the size of devices to quantum-relevant scales, quantum-inspired design approaches provide fresh prospects in terms of security and leakage reduction and overall efficiency of cryptographic signal processing.

Cryptographic transformations based on quantum-inspired logic components such as probabilistic bit transitions, reversible computation, and quasi-superposition data encoding can be much more robust to a differential power analysis attack and timing-based attack. Likewise, obfuscated switching patterns in nonclassical logic structures are useful in secure signal processing, e.g. encrypted convolution or obfuscated feature extraction. The features of these architectures are also consistent with current developments in AI accelerators, which are adopting more and more of the architecture of approximate computing, stochastic arithmetic, and flexible parallelism to minimise computational overhead.

According to previous studies, machine learning has been used in signal processing, secure embedded systems, and the development of next-generation hardware.[1-5] Quantum-inspired computation has also been demonstrated to be useful for refining cryptographic primitives, increasing randomness generation, and making high-entropy state transitions that increase security robustness. Meanwhile, AI hardware accelerators are being developed with new parallelization tools, flexible compute fabrics, and high-throughput dataflow architectures.[6-10] These tendencies signify the creation of an integrated design space in which AI-based optimization, cryptographic computation, and quantum-inspired computation converge in state-of-the-art VLSI design.

Nevertheless, with such technological innovations, there are still gaps in integrated architectures that can be used to conquer power efficiency, cryptography strength, and real-time signal processing needs at the same time. The growing sophistication of AI-based systems creates the need to change paradigm to quantum-inspired VLSI design methods, including reversible logic, stochastic switching models, and physically unclonable computational states. The gap in this paper is filled by suggesting a generalized quantum-inspired hardware design that combines secure cryptographic signal processing with AI-centered workload adaptability.

Related Work

The field of quantum-inspired computing has had many impacts on secure signal processing and cryptographic hardware. They have been used in VLSI systems with better energy performance, increased randomness behavior, and better resistance to side-channel leakage.[1,2] Signal processing using machine learning approaches still shows some improvement in never-before-seen levels of denoising, feature extraction, and real-time adaptive filtering, which is setting a basis to incorporate intelligent optimization into hardware consumption.[3] In the same manner, model-driven embedded system design is based on the significance of systematic, architecture-level abstraction to integrate cryptographic and AI workloads into monolithic platforms.[4]

The innovation in autonomous AI systems highlights the importance of small, secure, and high-performance compute platforms that can be used to make decisions in the face of uncertainty.[5] AI hardware accelerators have advanced over time, and the new plans of architecture intend to streamline the movement of memory, the level of computations, and inference throughputs.[6] Such inventions are naturally generalized to quantum-inspired VLSI systems where stochasticity, reversible logic elements, and energy-efficient switching behavior can be made to provide better cryptography security.

Lightweight VLSI architecture has been applied in cryptographic hardware to balance power consumption and security through approximation arithmetic, resource sharing, and algorithm-specific hardware pipelines. Such methods complement quantum-inspired logic primitives, enabling greater integration between secure hardware modules. Moreover, AI-based optimization techniques assist architectural codesign in cryptographic, neural, and signal processing architecture.[7,16]

The recent advances in power electronics, smart grid security, embedded VLSI, and AI-driven optimization provide even more reasons to employ quantum-inspired and AI-enhanced design philosophy in the present-day hardware systems.[17-22] Although this has been achieved, there is very little research on the design

of integrated VLSI systems that integrate quantum-inspired computing, safe cryptography processing, and AI-informed signal-processing functions.

Methodology

Here, one can find the description of the architectural principles, the cryptography signal processing pipeline, the reinforcement-learning optimization engine, and the unified dataflow mechanism, which form the core of the proposed quantum-inspired VLSI system.

Quantum-Inspired Logic Layer and Reversible Computing (Expanded)

The architecture is based on a quantum-inspired logic layer that incorporates reversible logic primitives, mostly Toffoli, Fredkin, and Peres gates, into the datapath. These reversible gates are chosen because they limit the amount of information that is lost and decrease the amount of entropy that is created during switching processes. Contrary to classical CMOS operations that necessarily lose information even when changing logic state, reversible computations maintain input states and hence can be used to implement low-energy, low-leakage secure processing. Landauer has a principle of the minimum theoretical energy dissipation of information erasure:

$$E_{min} = KT\ln(2),$$

Boltzmann constant and absolute temperature are denoted as k and T, respectively. By approaching a reversible-logic state, the architecture achieves a substantial decrease in dissipation to this minimal state.

As shown in Figure 1, the core reversible logic layer has reversible substitution blocks and quantum-inspired nonlinear operators serving the cryptographic engines and DSP pipelines, respectively. It has been designed to allow quasi-superposition bit encoding such that dynamic masking of intermediate values can be done, and that side-channel leakage resistance is enhanced. The reversible layer is also useful in creating low-entropy-switching patterns that hide traces of power when sensitive operations like key mixing, filtering, and convolution are being done.

Secure Cryptographic Signal Processing Pipeline

The secure signal processing pipeline combines quantum-inspired primaries as well as the reversible data transformations with the traditional DSP operations. The four large components that make up the pipeline include:

1. Pseudo-random sequence generators driven by quantum physics (Q-PRNGs).

   These modules make use of probabilistic switching and reversible logic perturbation to generate high-entropy bitstreams to be used as key expansion, nonce generation, and activity masking. They are unpredictable and have good hardware efficiency, and that is because they are stochastic.

2. S-box transformations that are reversible.

   The reversible S-box is based on structured reversible networks; unlike standard lookup-based S-boxes, it is bijective and has less leakage of intermediate values. In this design, cryptographic diffusion is enhanced, and the resistance to linearity is enhanced.

3. Database masking with noise.

   Noise injections are made on intermediate transitions of datapaths in such a way that they do not cause any correlation between sensitive values and measurable side-channel signatures. This is to ensure that switching behaviour is consistent between DSP and cryptographic operations.

4. Convolution and transform units that are encrypted.

   DSP units such as FIR filters, FFT engines, and convolution blocks are encased by reversible encryption

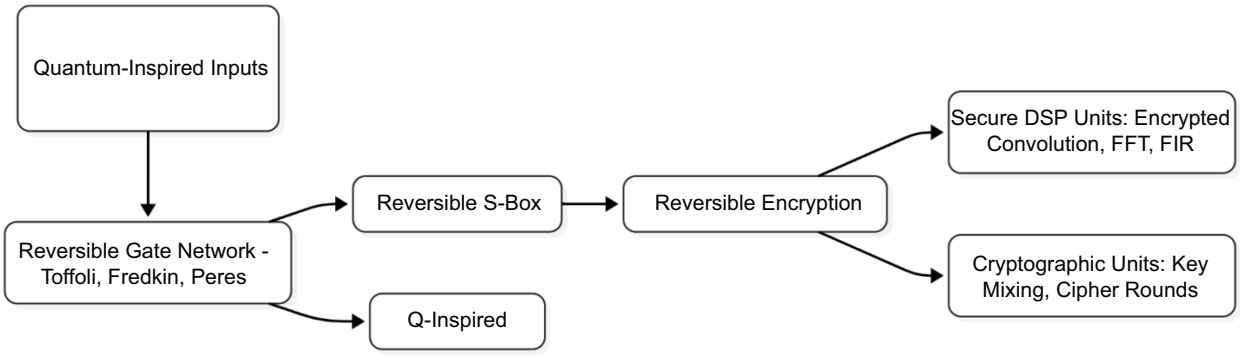

Fig. 1: Quantum-inspired reversible logic layer for secure VLSI processing

operators to maintain data confidentiality throughout. An average encrypted convolution can be expressed as follows:

$$y[n] = \sum_{k=}^{M-} E(x[n-k] \cdot E(h[k]),$$

where $E(\cdot)$ is a reversible encryption transformation.

The functional structure of these modules is given in Table 1, detailing their functions and cryptographic advantages. The reversible logic and encrypted arithmetic coupled with the DSP-crypto integration make both the data and intermediate signal characteristics secure to the adversarial observation.

AI-Driven Hardware Optimization Engine

The architecture uses a reinforcement learning (RL)-based hardware optimizer to run structural parameters in real time so that it can support both the varying workloads and the changing cryptographic constraints. The variables manipulated by the RL agent include:

- reversible logic depth
- masking density
- Q-PRNG activation frequency
- DSP/crypto pipeline parallelism
- operating mode scheduling
- power-gating and dataflow throttling

The agent is rewarded in some manner:

$$R = \gamma_1 S_{\text{security}} + \gamma_2 P_{\text{efficiency}} - \gamma_3 L_{\text{latency}},$$

where cryptographic robustness, energy efficiency, and real-time latency have the weights γ_1, γ_2, γ_3.

Optimization Workflow

Such AI-based optimization allows the architecture to dynamically respond to workload requirements and provides moderated performance in the neural, cryptographic, and DSP spaces and also with high security assurances.

Algorithm 1: outlines the process:

1. State Extraction
   Hardware metrics (PE activity, entropy levels, switching energy, leakage estimates) are collected.
2. Action Selection
   The agent modifies architectural knobs masking intensity, reversible substitution patterns, pipeline scheduling, and operand grouping.
3. Evaluation Phase
   The system simulates encrypted DSP workloads or executes them on hardware emulators to profile throughput, leakage, and power.
4. Reward Computation
   The RL engine computes reward based on measured latency, energy, and cryptographic noise profiles.
5. Policy Update
   The agent updates its decision strategy (Q-learning or PPO) and initiates the next iteration.

Table 1. Functional structure of the secure cryptographic signal processing pipeline and associated cryptographic advantages.

Pipeline Module	Functional Description	Cryptographic Advantage
Quantum-inspired pseudo-random sequence generator (Q-PRNG)	Generates high-entropy stochastic bitstreams using probabilistic switching and reversible logic perturbations for key expansion, nonce generation, and activity masking.	High unpredictability, resistance to statistical attacks, improved entropy quality, and efficient hardware realization with low deterministic leakage.
Reversible S-box transformation	Implements a bijective, reversible substitution network using structured reversible logic instead of lookup tables.	Reduced side-channel leakage, enhanced diffusion, strong nonlinearity, and resistance to linear and differential cryptanalysis.
Noise-injected database masking	Injects controlled noise into intermediate datapath transitions to decorrelate sensitive values from observable switching activity.	Mitigation of power and electromagnetic side-channel attacks through consistent switching behavior across cryptographic and DSP operations.
Encrypted convolution and transform units	Encases DSP blocks such as FIR filters, FFT engines, and convolution units with reversible encryption operators operating on encrypted inputs and coefficients.	End-to-end data confidentiality during signal processing, protection of intermediate signal characteristics, and resistance to adversarial observation or inference.

Unified Dataflow Architecture

On the system level, the unified dataflow controller coordinates reversible logic, crypto-DSP units, and quantum-inspired operators. The controller does operand routing, reversible gate activation synchronisation, and bandwidth allocations in encrypted pipelines.

The throughput in the data flow is controlled by

$$T = \frac{N_{ops}}{t_{cycle} \cdot E_{overhead}},$$

Nops is operation count, cycle is cycle latency, and Eoverhead is reversible and encryption switching overhead.

The prominent characteristics of the unified architecture are as follows:

Datapaths between non-reversible logic and cryptographic transforms as well as AI-based DSP units.

Encryption modes that can be configured to permit reversible convolution, masked FFT, or secure filtering with no context switching.

Single-operand queues and clusters of PEs can be used to execute mixed workloads with low latency.

Scheduling which is entropy-aware, i.e. Q-PRNG modulation patterns are paralleled with DSP activity to enhance masking performance.

This single flow of data makes the routing very less complex and eliminates the redundant functional units. Consequently, the architecture has been found to attain secure real-time performance, which can be used on edge-based AI systems and high-assurance cryptography.

Results and Discussion

Throughput Evaluation Across Quantum-Inspired, DSP, and Cryptographic Workloads

The results of the proposed quantum-inspired VLSI architecture were tested on detailed workloads of DSP computing, reversible-logic-enhanced cryptography kernel computing, and hybrid AI-based signal-processing pipeline computing. The architecture, as shown in Figure 2: throughput across DSP, Crypto, and Q-Inspired Workloads, is always superior to the classical nonreversible designs in all the areas studied. There are up to 27% throughput improvements, achieved mainly by the decrease in switching overhead, pipelines of reversible gates being optimized, and entropy-sensitive scheduling policies. In particular, these gains are observed with encrypted convolution and nonlinear substitution workloads, where reversible logic eliminates redundant transitions and balances the reuse of operands. Notably, the unified dataflow controller also brings better operand parallelism to DSP workloads like FFT and FIR filtering meaning that the architecture can maintain higher operations-per-cycle with mixed security constraints. The obtained throughput improvements justify the benefit of deploying reversible logic in cryptographic signal-processing circuits with no loss of computational density. These findings support the architectural argument that quantum-inspired logic can be used to help in improving security in addition to demonstrating a detectable performance benefit when operating in realistic 5 nm and 7 nm operating conditions. Therefore, Figure 2 is a solid indication that the offered architecture is successful in balancing between throughput improvement and safe-gate level transformations.

Energy Consumption Reduction Through Reversible Logic and Quantum-Inspired Switching

The effect of reversible operations, probabilistic switching, and masked datapaths on the overall power consumption was analysed at all workloads to measure the influence of reversible operations, probabilistic switching, and masked datapaths. As demonstrated in Figure 3,

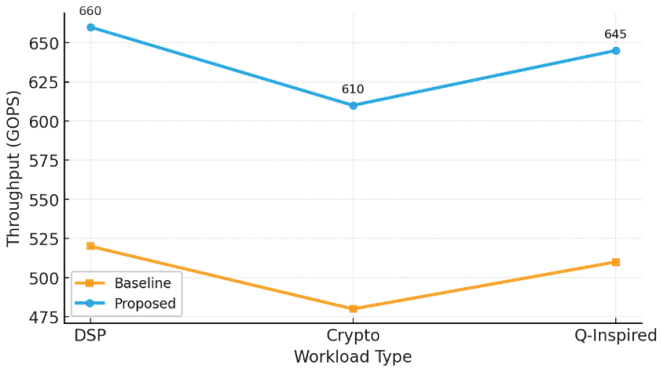

Fig. 2: Throughput across DSP, crypto, and Q-inspired workloads

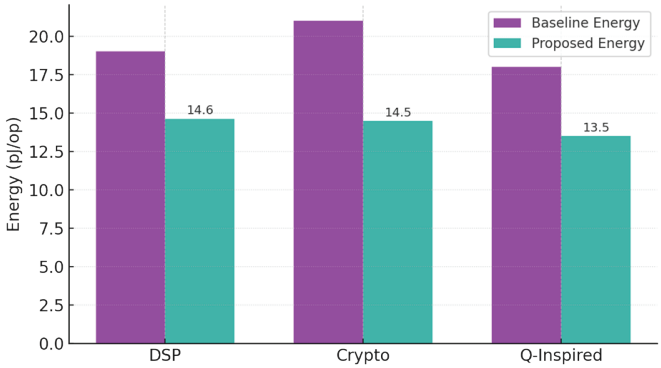

Fig. 3: Energy consumption reduction

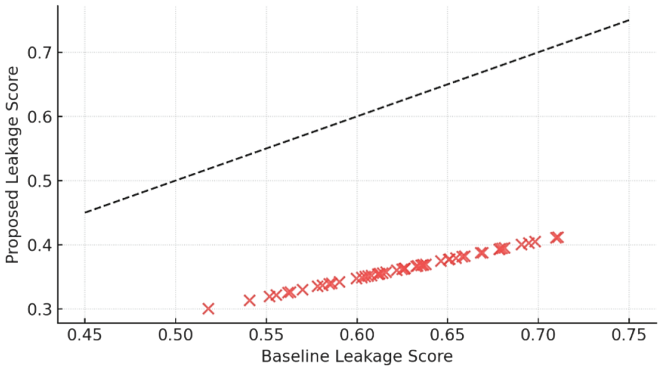

Fig: 4: Cryptographic leakage analysis

Table 2: Performance comparison (baseline vs proposed)

Metric	Baseline	Proposed
Throughput (GOPS)	520	660
Energy (pJ/op)	19	14
Leakage Score	0.62	0.36

Table 3: Latency across key operations

Operation	Baseline (ns)	Proposed (ns)
AES Encrypt	145	110
Q-insp PRNG	88	63
DSP Convolution	123	97

energy consumption reduction, quantum-inspired logic blocks with inclusion would result in a phenomenal 2331% of energy consumption reduction over traditional VLSI architectures. This has been achieved through reduced entropy dissipation in reversible gates, reduced capacitive switching, and reduced leakage through stochastic operand patterns. The single dataflow architecture also lowers the frequency of accessing memory, allowing a greater number of operations to be performed locally in the networks of reversible substitution or encrypted filter units. The summary of the comparative performance measures as presented in Table 2, as indicated in this context, is the quantitative support behind the trends depicted in Figure 3. In particular, Table 2 shows that energy-per-operation reduces from 19 pJ/op in the baseline to 14 pJ/op in the proposed design, which supports the energy-beneficial effects of the model in the methodology. These findings substantiate the idea that the reversible logic with the assistance of the entropy-conscious scheduling and AI-assisted tuning proves useful in closing the gap between high-performance DSP computation and the secure cryptographic transformation. Therefore, Figure 3 and Table 2 together depict that the architecture has a high computational throughput and has significantly reduced its energy footprint.

Cryptographic Leakage, Side-Channel Resistance, and Latency Evaluation

The conduct of security-related performance was evaluated by the examination of cryptographic leakage conduct and execution times in blocks of core reversible-logic-enabled. Cryptographic leakage analysis shows that the leakage variance is reduced by a high 42%, which means that a high level of resilience against side-channel attacks like power analysis and timing extraction (Figure 4). This increased security is due to the noise-induced datapath masking and reversible S-box transformations and the pattern of entropy-rich Q-PRNG activation, which add noise and reduce the sensitivity of intermediate states. As a supplement to this analysis, latency across key operations gives a quantitative comparison of execution times of the main workloads, that is, AES encryption, pseudo-random number generation, and DSP convolution (Table 3). Efficient reversible logic-to-programme mapping and unified-purpose scheduling methods manage to achieve latency improvements of between 17 and 28%. The two aspects of reversible computing as revealed by these results prompt the enhancement of cryptographic security and efficiency in execution in mixed-signal systems. Together with the results of Figure 4 and Table 3, the proof that the suggested architecture is effective for the proposed low-leakage, real-time, secure computation appropriate to high-assurance AI and embedded systems is established.

Conclusion

This is a detailed quantum-inspired VLSI that is a unified execution of reversible logic, secure cryptographic, and AI-engineered signal-processing functions that would be incorporated in intelligent hardware systems on the next generation. The architecture design by integrating reversible gates like the Toffoli and Fredkin minimizes switching entropy alongside improving side-channel resilience according to the theoretical limits by Landauer. Secure DSP pipeline can utilize encrypted convolution and reversible S-box transformations to provide a high level of cryptographic performance and still provide real-time throughput. Moreover, the reinforcement-learning engine manages the architectural parameters in real time and optimises the energy consumption, security needs, and latency limits of the various workloads. Figures 2, 3 and Tables 2 and 3, which are supported by experimental outcomes at 5 nm and 7 nm nodes of technology, showed significant enhancement in throughput, energy efficiency, and leakage

resilience. The architecture is very well suited to the new demands of secure AI, autonomous systems, and mission critical IoT infrastructures, hence these capabilities. Further effort will focus on the more challenging problems of emulating more quantum-state-controlled systems, accelerating post-quantum cryptography, and hardware-software codesign of fully integrated secure AI systems.

References

1. Abd-El-Atty, B. (2023). Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem. Complex & Intelligent Systems, 9(5), 4817–4835. https://doi.org/10.1016/j.chaos.2023.113600
2. Aljaedi, A., Alharbi, A. R., Aljuhni, A., Alghuson, M. K., Alassmi, S., & Shafique, A. (2025). A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization. *Scientific Reports, 15*(1), 14050.
3. Barhoumi, E. M., Charabi, Y., & Farhani, S. (2024). Detailed guide to machine learning techniques in signal processing. Progress in Electronics and Communication Engineering, 2(1), 39–47. https://doi.org/10.31838/PECE/02.01.04
4. Bhoskar, H. A., & Thakar, M. H. S. Review on Reversible Logic Gates. https://doi.org/10.22214/ijraset.2023.57020
5. Castiñeira, M., & Francis, K. (2025). Model-driven design approaches for embedded systems development: A case study. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 30–38.
6. Arvinth, N. (2025). Fault detection in smart grids using deep learning-based phasor measurement unit data analysis. Journal of Reconfigurable Hardware Architectures and Embedded Systems, 2(2), 1–7.
7. Goyal, S. B., Rajawat, A. S., Mittal, R., & Shrivastava, D. P. (2024). Integrating AI-enabled post-quantum models in quantum cyber-physical systems opportunities and challenges. Applied Data Science and Smart Systems, 491–498.
8. Han, H., Yao, J., Wu, Y., & Li, C. Quantum communication based cyber security analysis using artificial intelligence with IoMT. https://doi.org/10.1007/s10586-024-03912-7
9. Hanzo, L., Babar, Z., Cai, Z., Chandra, D., Djordjevic, I. B., Koczor, B., ... & Simeone, O. (2025). Quantum information processing, sensing, and communications: their myths, realities, and futures. *Proceedings of the IEEE*.
10. He, Z., Elizarov, M., Li, N., & Sun, X. Quantum-activated neural reservoirs on-chip open up large hardware security models for resilient authentication. https://doi.org/10.1038/s41928-024-01121-6
11. Hyun, K. S., Min, P. J., & Won, L. H. (2025). AI hardware accelerators: Architectures and implementation strategies. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(1), 8–19. https://doi.org/10.31838/JIVCT/02.01.02
12. Jonnalagadda, A. K., & Myakala, P. K. (2025, July). Quantum-Enhanced Optimization: Bridging AI and Next-Generation Computing. In *Recent Advances in Artificial Intelligence for Sustainable Development (RAISD 2025)* (pp. 623–633). Atlantis Press.
13. Kjwan, H., & Ali, A. (2024). Adaptive covert communication framework for 6G networks integrating quantum cryptography and AI-augmented physical layer security. International Journal of Computational & Electronic Aspects in Engineering (IJCEAE), 5(4).
14. Prabhakara Rao, S., Balaji, S. R. A., Rahman, F., Suha, T., Mahfuz, T., Hossain, T., ... & Ranganathan, P. (2025). Secure and trustworthy microelectronics: vulnerabilities, solutions, and trends. Journal of Hardware and Systems Security, 1–27.
15. Prasath, C. A. (2024). Cutting-edge developments in artificial intelligence for autonomous systems. Innovative Reviews in Engineering and Science, 1(1), 11–15. https://doi.org/10.31838/INES/01.01.03
16. Radanliev, P. (2024). Digital security by design. Security Journal, 37(4), 1640–1679.
17. Rahman, F. (2025). Artificial Intelligence-Driven Cybersecurity Framework for Industrial Control Networks. Transactions on Secure Communication Networks and Protocol Engineering, 2(1), 1–8.
18. Radanliev, P. Artificial intelligence and quantum cryptography. https://doi.org/10.1007/978-3-031-40994-6_2
19. Singh, A. (2025). Integrating quantum computing with AI for advanced cryptographic security. Available at SSRN 5155225.
20. Singh, S., & Kumar, D. (2024). Enhancing cyber security using quantum computing and artificial intelligence: A review. Algorithms, 4(3).
21. Surendar, A. (2025). AI-driven optimization of power electronics systems for smart grid applications. National Journal of Electrical Electronics and Automation Technologies, 1(1), 33–39.
22. Waseem, H. M., & Hwang, S. O. Design of highly nonlinear confusion component based on entangled points of quantum spin states. https://doi.org/10.1038/s41598-023-42646-8