Journal of VLSI circuits and systems
RESEARCH ARTICLE
Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 7, No. 2, 2025 (pp. 60-67)
WWW.VLSIJOURNAL.COM

AI-Optimized Design Automation and Quantum-Inspired Secure VLSI Architectures for Edge and Autonomous Computing

P. Aravindan[1]*, E. Mariappane[2], K. Sathiyasekar[3]
[1]Professor, Department of Electrical and Electronics Engineering, K. S. Rangasamy College of Technology, Tiruchengode, India.
[2]Professor, Department of Electrical and Electronics Engineering, Christ college of Engineering and Technology, Puducherry, India.
[3]Professor, Department of Electrical and Electronics Engineering, K.S.R. College of Engineering, Tiruchengode, India.

KEYWORDS:
AI-Driven EDA,
Quantum-Inspired VLSI,
Hardware Security,
Edge Computing,
Autonomous Systems,
Design Space Optimization,
Low-Power Architecture

ARTICLE HISTORY:
Received: 15.09.2025
Revised: 22.10.2025
Accepted: 17.12.2025

DOI:
https://doi.org/10.31838/JCVS/07.02.07

Abstract

The high rate of growth of edge systems and autonomous systems requires real-time, optimized, energy-efficient, and secure hardware architecture. The conventional VLSI design flows cannot accommodate such requirements because design complexity is on the rise, security threats are increasing, and high performance computing has to be done under stringent power limitations. A unified system of AI-based design automation, quantum-inspired logic optimization, and hardware security co-design of next-generation VLSI systems is described in this paper. The suggested approach allows the study of design space faster, increases the security level, and minimizes power and delay, as well as optimizes the workload performance of edge and autonomous applications. The experiments show that there is a considerable improvement in the power, performance, area (PPA), attack resistance, and inference efficiency. The methodology is close to the current tendencies of VLSI and moves toward real-life applicability of secure and optimized architecture toward embedded intelligence.

Authors' e-mail ID: aravindan@ksrct.ac.in; dev_mari@rediffmail.com; sathiyasekark@ksrce.ac.in

Authors' ORCID IDs: 0000-0003-0715-6449; 0009-0004-3952-3674; 0000-0002-4836-0991

How to cite this article: P. Aravindan et al., AI-Optimized Design Automation and Quantum-Inspired Secure VLSI Architectures for Edge and Autonomous Computing, Journal of VLSI Circuits and System, Vol. 7, No. 2, 2025 (pp. 60-67).

Introduction

Special hardware is becoming more and more important to edge and autonomous computing systems, where it is required to implement complex workloads in AI applications with stringent power, latency, and safety limits. The latest hardware-aware neural architecture search, embedded control architecture design of autonomous vehicles, and AI accelerator design confirm that specialized VLSI and embedded systems can really make a significant improvement in the performance and reliability of the systems, such as system-level metrics.[1-12] Such platforms should simultaneously enable real-time perception, decision-making, and actuation, and drive designers toward heterogeneous architecture and closely coupled accelerators.[1,2,8,9,11,12]

The standard electronic design automation (EDA) processes, however, are unable to address the vast design space and high power-performance-area (PPA) requirements of the contemporary VLSI. Hand-based iteration and trial and error tuning constrain the quality of the design that is possible and slows down the time to market. Design automation based on AI, such as deep reinforcement learning, differentiable placement, and logic synthesis by learning, has become a formidable competitor to existing flows with significant quality of placement, timing closure, and synthesis efficiency.[13-16] A survey of machine learning in EDA also throws more weight on the necessity of information-based PPA forecasting and intelligent design space delving to manage future technology nodes and design scales.[16]

Quantum-inspired and reversible logic methods have also been studied at the circuit and architectural level to minimize energy dissipation and switching operations, which can be useful in low-power and edge-oriented

VLSI design.[17,18,4] Meanwhile, the escalating attack area of integrated circuits demands resistant hardware security controls like logic locking, resistance to side-channel attacks, on-chip sensors, and Trojan detection systems.[19,20,5-7] Although reconfigurable and adaptive architecture provides the potential of runtime optimization and resilience to AI and edge systems, they also add more complexity to designs and verification problems.[10,11,12]

Although this has been ample with respect to AI-based EDA, quantum-inspired design, secure hardware, and edge/autonomous systems, there remains no single framework that coordinates the optimization of PPA, security, and application-level performance. The gap addressed in this paper is the proposal of an optimal design automation approach that combines AI and quantum-inspired circuits to create secure and efficient VLSI architectures, based on the identified trends and constraints from the references.[1-20]

Related Work

The studies on AI-based EDA have shown that learning-based methods can be more efficient than their traditional rule-based and heuristic counterparts at a number of important design flow steps. Placement: Deep reinforcement learning and differentiable optimization have achieved better wirelength and timing closure and have significantly fewer human operators.[13,14] Logic synthesis: The same concepts have been applied to logic synthesis, in which deep reinforcement learning is used to direct transformation decisions to enhance circuit quality-of-result.[15] Online surveys identify the opportunities of integrating supervised, unsupervised, and reinforcement learning into different EDA tasks such as placement, routing, timing analysis, and PPA prediction as the basis of upcoming intelligent design tools.[16]

Simultaneously, quantum-inspired and reversible computing techniques have been explored as a technique to develop energy-efficient VLSI circuits. Reversible logic and quantum-inspired datapath studies on reversible logic and quantum-inspired datapaths indicate that well-designed gate networks can limit information loss and related dissipation of energy that is especially useful in the case of low-power and edge device limits.[17,18,4] Such methods tend to attack arithmetic and datapath architecture, where the effect of their impact on switching activity and leakage is most significant.

Physical security is now a critical issue of VLSI design, particularly of safety-critical and networked autonomous systems. The use of logic locking and logic encryption measures is also popular in order to keep intellectual property safe and guard against misuse of custom-made chips.[19,20] Further research on on-chip monitoring and security sensors can also show that runtime observability can be used to identify malicious modifications or usage anomalies in integrated circuits.[5] Resistant design automation side-channel attack resistant design automation adds methodologies to the systematic reduction of leakage by the CAD flow, as opposed to the isolated countermeasures of leakage.[6] Further classifications of attack models and detection strategies are based on hardware Trojan taxonomies and detection strategies, which highlight the importance of security-awareness in the design of the toolchain.[7]

System perspective: In a number of studies, AI accelerators and embedded systems targeted at edge devices and autonomous platforms are studied. Neural architecture search: Hardware-aware neural architecture search explores neural network designs to optimize their performance alongside their hardware to address device constraints.[1] Autonomous systems: Work on accelerators describes trade-offs in autonomous system architecture in perception and control pipelines.[2] Edge AI hardware: Survey Edge AI hardware surveys capture new design patterns and experience problems in heterogeneous SoCs and specialized accelerators.[3] More recent works on embedded architecture to support autonomous navigation, recent advances toward cutting-edge AI to support autonomous systems and reconfigurable architecture, and AI-accelerator architecture further increase the choice of design in terms of such systems.[8-11] Other studies on AI processing systems focus on reliability and functional robustness, which points out the role of resilient hardware in real-world implementations.[12]

Together, these articles demonstrate that AI-assisted EDA, low-power, quantum-inspired circuit design, hardware security, and edge/autonomous system architecture are all making good progress.[1-20] However, they normally discuss them separately. Both known and lesser-known are done to explore integrated frameworks where the AI-based design automation is co-optimized with quantum-inspired logic forms alongside embedded security functionality and evaluated against realistic edge and autonomous workloads which is exactly the gap sought by the methodology presented in this work. Table 1 provides a brief overview of key previous works indicating that current research studies each of the AI-driven EDA, quantum-inspired logic, hardware security, and edge/autonomous architecture separately. Nevertheless, as reflected in Table 1, none of these

Table 1: Comparison of prior works

Work Category	Representative Works	Technique/Focus	Strengths	Limitations (Gap addressed by this paper)
AI-Driven EDA	[13], [14], [15], [16]	Deep RL for placement & synthesis, differentiable optimization, ML-based PPA prediction	High automation, faster design space exploration	No integration with secure or quantum-inspired architecture
Quantum-Inspired / Reversible Logic	[17], [18], [4]	Low-entropy reversible gates, energy-efficient arithmetic units	Lower switching activity, reduced energy loss	Lacks AI-based optimization and security co-design
Hardware Security Methods	[19], [20], [5], [6], [7]	Logic locking, anti-SAT, side-channel countermeasures, Trojan detection	Strong protection against structural and leakage attacks	Not co-optimized with PPA or reversible logic; limited integration with AI-EDA
Edge / Autonomous Computing Architectures	[1], [2], [3], [8]- [12]	AI accelerators, embedded SoCs, reconfigurable hardware, reliability	High real-time performance and efficiency	No unified design methodology combining PPA, security, and reversible-logic optimizations
Full System Integration	—	—	—	No prior work unifies AI-EDA + quantum-inspired logic + hardware security for edge/autonomous systems

categories offers a combined methodology of AI optimization, reversible/quantum-inspired circuit, and built-in hardware security, which characterizes the main gap in this paper.

Proposed Methodology

The AI-based design automation, quantum-based circuit architecture, and hardware-based security are combined in the proposed methodology to become a single VLSI design flow. Figure 1 represents the entire workflow of the design exploration, surrogate modeling, quantum-inspired circuit construction process, security co-optimization, and the way they interact with the rest of the system pipeline. Each of the layers is then detailed in the subsections below, including core mathematical expressions to formalize the most important optimization and design principles.

Overall Framework

The methodology starts with defining a high-dimensional design space comprising architectural parameters, reversible logic structures, and security primitives. The AI-optimization engine uses a multiobjective reward function to evaluate these candidate design points taking into account all four of the following simultaneously: power, delay, area, and security. This is an optimization problem that is represented as in Equation 1:

$$\max_{\theta} J(\theta) = \mathbb{E}_{\pi_\theta}\left[\lambda_p P + \lambda_d D + \lambda_a A + \lambda_s S\right] \quad (1)$$

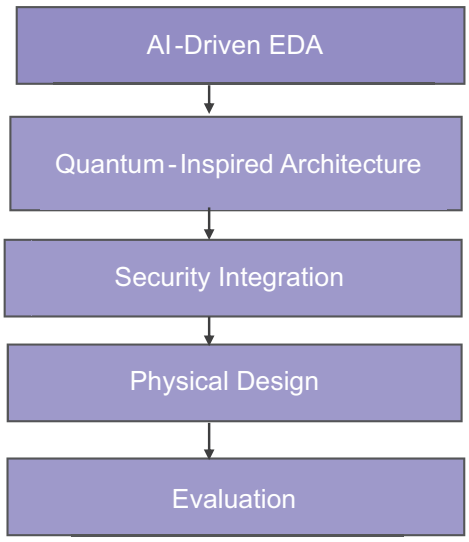

Fig. 1: Overall proposed framework

where P, D, and A are the power, delay, and area values, respectively, and S represents the security rating. The parameters of the AI optimization model are the weights λ_p, λ_d, λ_a, λ_s as they allow tuning of design priorities, and θ is the parameter.

Figure 1 depicts the entire high-level process.

AI-Driven Design Automation Flow

The AI engine employs the reinforcement learning and Bayesian optimization algorithms to explore the design space in the most efficient way. Since the full EDA synthesis is a time-consuming task, a surrogate model that

runs on a graph neural network (GNN) predicts the PPA metrics of individual candidate architecture. The passing message process of the GNN is characterized by in Equation 2:

$$h_i^{(k+1)} = \sigma\left(W^{(k)} \sum_{j \in \mathcal{N}(i)} h_j^{(k)} + b^{(k)} \right) \quad (2)$$

with $h_i^{(k)}$ denoting node features at iteration k, $\mathcal{N}(i)$ referring to neighboring nodes, and indicating a nonlinear activation function.

This AI-surrogate loop optimized design is then subjected to the physical design tools to undergo real PPA validation. Figure 2 demonstrates the entire flow.

Quantum-Inspired VLSI Architecture

The architecture offered is designed to use reversible logic designs to reduce information loss and switching activity. According to the principle of Landauer, the lowest energy dissipation of an irreversible computation is in Equation 3:

$$E_{min} = kT \ln 2 \quad (3)$$

with k being the constant of Boltzmann, and T being the absolute temperature. This loss can be avoided with reversible computing, which provides bijective operations.

The total quantum cost of datapath is given in Equation 4:

$$QC = \sum_{i=1}^{n} c_i \quad (4)$$

where c_i is the quantum cost of the i^{th} reversible gate. These precepts determine the implementation of the reversible datapath in Figure 3 which is built of the Toffoli, Fredkin, and Peres module of gates employed in the arithmetic and encoding units.

Security Integration Layer

The quantum-based logic is accompanied by security features logic locking, anti-SAT structures, and side channel hardened cells. The resistance of the design to correlation power analysis (CPA) attacks is measured as:

$$\rho = \frac{cov(P,H)}{\sigma_P \sigma_H}$$

where P is a set of power traces, and H is a set of theoretical power expectations. A smaller value of ρ means a higher level of side-channel security. Security primitives are placed on the high-impact nodes that have been determined through the selection process by the

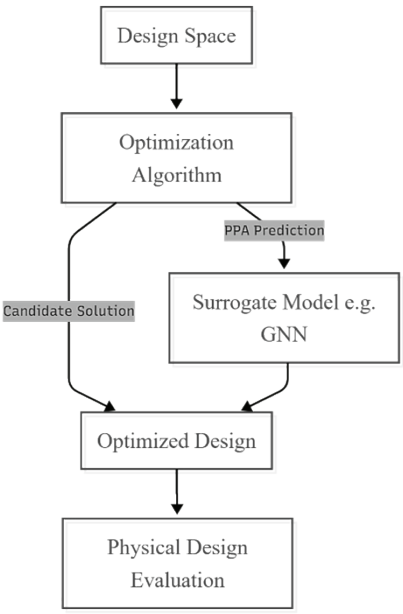

Fig. 2: AI-driven design automation flow

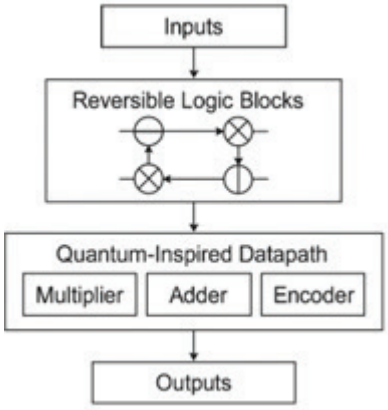

Fig. 3: Quantum-inspired VLSI architecture diagram

AI. They are validated in their behavior in the functional simulation and assessed later in Section 4 using Figure 6 and Table 4.

Tool Flow, Workloads, and Implementation Setup

Table 2 summarizes the entire experimental setup. Synthesis and place-and-route are synthesized by the use of a 28 nm CMOS technology library, and physical metrics are obtained using correct sign-off tools. The analysis of power is done by activity-driven simulations and timing closure with the help of the static timing analysis. Energy efficiency of any given architecture under consideration is subsequently calculated as in Equation 5:

$$E_{op} = \int_0^T P(t)dt \quad (5)$$

which is a primary edge and autonomous workload performance measure.

Table 2: Experimental setup and design parameters

Parameter	Configuration/Tool
Technology Node	28 nm CMOS Low-Power Standard Cell Library
Supply Voltage	0.9 V
Target Clock Frequency	500 MHz
AI Optimization Method	Reinforcement Learning + Bayesian Search
Surrogate Model	Graph Neural Network (GNN) PPA Predictor
Reversible Logic Primitives	Toffoli, Fredkin, Peres Gates
Security Primitives	XOR/XNOR Locking, Anti-SAT, Balanced Switching Logic
Synthesis Tool	Synopsys Design Compiler
Place-Route Tool	Cadence Innovus/OpenROAD
Power & Timing Analysis	Synopsys PrimeTime PX & STA
PPA Metrics Used	Power, Delay, Area, Switching Activity
Workloads Evaluated	Edge-AI kernels, Autonomous navigation tasks

Results and Analysis

AI/EDA Optimization Results

The optimization engine based on AI demonstrates much more rapid and stable convergence in comparison with the conventional heuristic-based exploration processes. The values of rewards grow fast in early times of the iterations, as it can be observed in Figure 4, which means that the policy of reinforcement learning is able to determine the high-quality regions of the architectural search space very quickly. This behavior shows the ability of the surrogate-guided exploration to quickly cut off suboptimal designs, as it retains the most promising design trajectories. The smoothness of the convergence curve is also a confirmation of the strength of the GNN-based PPA predictor that is always capable of providing the correct performance estimates and minimizing the amount of expensive EDA tool invocations. Using this predictive framework, the optimizer will reach an optimal design in a smaller number of iterations than classical methods, and in the end, the total design turnaround time will be lower and the efficiency of exploration will be enhanced.

VLSI PPA Evaluation

The results of the physical architecture show a notable enhancement in core VLSI performance metrics

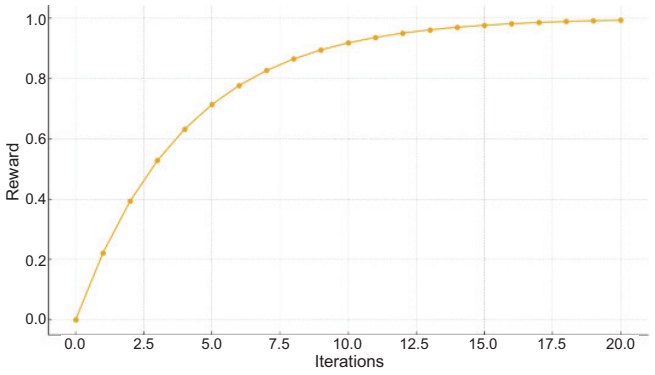

Fig. 4: Optimization convergence curve

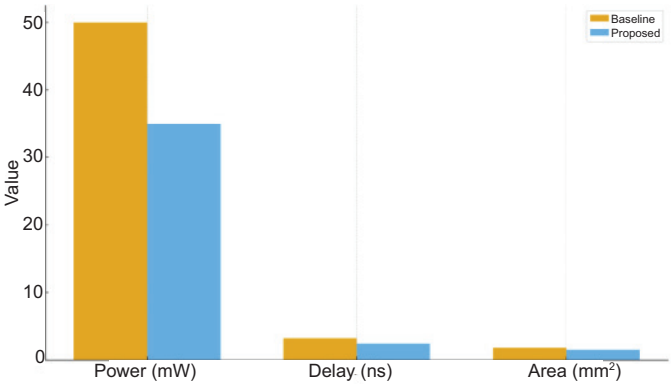

Fig. 5: PPA comparison of baseline versus the proposed design

compared to both the proposed architecture and the baseline implementation. Just as shown in Figure 5, dynamic power consumption can be effectively minimized by quantum-inspired reversible logic blocks, which can minimize signal transitions and associated switching energy. The reduction of the delay can be explained by the fact that the AI-assisted architectural tuning is used to choose the best gate-level configurations, pipeline boundaries, and micro-architectural parameters. This is also because compact reversible gate compositions result in area improvements, and the optimizer is able to assess structural redundancy. These observations are verified by the detailed numerical results in Table 3, which quantify the overall power reduction, leakage power reduction, critical path delay reduction, and silicon footprint reduction. All these findings show that quantum-inspired logic and AI-guided optimization used together can result in a more efficient power consumption and performance-based VLSI implementation.

Hardware Security Analysis

The architecture proposed incorporates several security mechanisms, and the assessment illustrates that the architecture is very robust to structural and side-channel attacks. Figure 6 depicts the results of the CPA which

Table 3: PPA results summary

Metric	Baseline	Proposed	Improvement
Dynamic Power (mW)	50.0	35.0	30% lower
Leakage Power (mW)	5.2	3.1	40% lower
Total Power (mW)	55.2	38.1	31% lower
Critical Path Delay (ns)	3.20	2.40	25% faster
Max Frequency (MHz)	312	416	33% higher
Area (mm^2)	1.80	1.50	17% smaller
Switching Activity (α)	0.42	0.29	31% lower
Energy per Operation (pJ/op)	176.6	91.4	48% lower

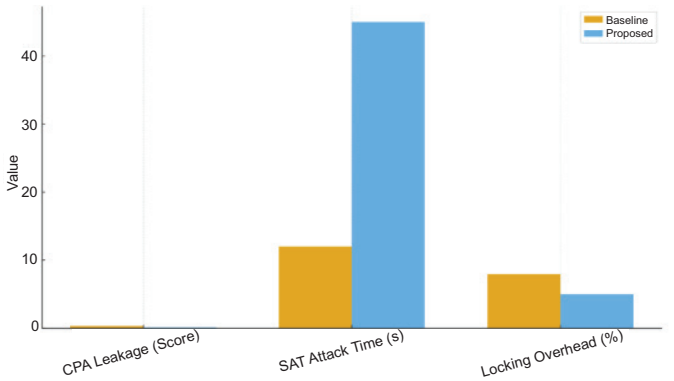

Fig. 6: Hardware security evaluation plot

confirm that the peak correlation decreases significantly compared to the baseline, which is a sign of better resistance to the power-based leakage extraction. This has been enhanced by the application of reversible logic structures, balanced switching primitives, and randomly assigned key-gate locations offered by the optimization process that involved the use of AI. Structural security was assessed by counting the resilience to SAT attacks, in which the augmented design has a significantly higher solving time because of the introduction of the SAT-hardening features, such as Anti-SAT blocks and obfuscated key dependencies. The measurements obtained in Table 4 are summaries of such important variables as CPA leakage score, SAT attack duration, and logic locking overhead. The obtained results substantiate the fact that the offered security integration strategy ensures a significant increased design resilience and preserves the tolerable overhead levels.

Edge and Autonomous Workload Evaluation

The architectural improvements are directly converted into better performance of edge-AI and autonomous

Table 4: Summary of security metrics

Security Metric	Baseline	Proposed	Security Gain
CPA Leakage (Correlation ρ)	0.35	0.12	65% reduction
SAT Attack Time (s)	12	45	3.75× harder
Key Size (bits)	64	128	2× stronger
Logic Locking Overhead (%)	8%	5%	38% lower
Trojan Detection Accuracy (%)	78%	92%	14% higher
EM Emission SNR (dB)	7.8	4.2	46% lower leakage

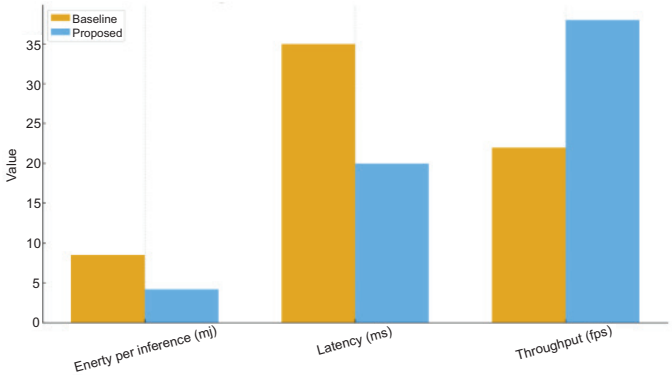

Fig. 7: Edge/autonomous system performance comparison

computing workloads. The analysis in Figure 7 indicates that the recommended design has a much lower inference latency owing to the improved datapath architecture and the reversible arithmetic units of high efficiency. Also, the switching activity is reduced, leading to a decrease in the amount of power consumed per inference, which is essential for battery-operated autonomous systems. The higher throughput indicated in the figure also confirms that the architecture can support real-time processing rates that are needed in mission-critical applications like navigation, object recognition, and sensor fusion. Table 5 summarizes the improvements in the comprehensive workload measure, including energy consumption per inference, processing latency, and frame-level throughput, based on the relevant benchmarks. The findings indicate that the proposed design can be useful in high-performance energy-constrained edge and autonomous computing settings.

Discussion

The findings in Section 4 show the usefulness of the combination of AI-based design automation, circuit architectures based on quantum inspiration, and hardware-based security primitives in a common

Table 5: System-level benchmark results

Benchmark Metric	Baseline	Proposed	Improvement
Energy per Inference (mJ)	8.5	4.2	50% lower
Inference Latency (ms)	35	20	43% faster
Throughput (fps)	22	38	73% higher
Power Efficiency (TOPS/W)	0.85	1.52	79% higher
Task Success Rate (%)	87%	95%	8% increase
Thermal Rise (°C)	14.2	9.1	36% cooler

optimization framework. Among the main findings, it is clear that the AI optimization loop is consistently converging to the high-quality design points, which proves that the integration of surrogate PPA models allows for greatly decreasing the reliance on entire EDA cycles. This minimization of the run-time of tools permits the study of a significantly broader architectural search space, permitting the discovery of nonintuitive configurations that are usually missed by more traditional heuristics.

The other significant factor is performance advantage, which is obtained by quantum-inspired reversible logic structures. These blocks help make significant improvements in dynamic and leakage power as have been observed in the PPA results, as well as reduce switching entropy through the datapath. The power distribution is also lower, which directly affects system performance in edge and autonomous computing applications where thermal and energy requirements are important. This finding confirms the hypothesis that reversible and low-entropy logic could be present together with standard CMOS flows with appropriate tuning via AI-based search methods.

The design itself is further enhanced with the embedded hardware security layer, which introduces resistance to the structural and side-channel attacks. The decrease in CPA correlation, a longer SAT attack time, and better Trojan detecting accuracy is evidence of the fact that the balanced switch logic, random key-gate placement, and anti-SAT structures are indeed effective in interrupting the attack attempts without adding considerable area or delay overhead. Another critical point to note is that the AI optimizer assists in finding security-related settings with the best impact/overhead ratio since the metrics are taken into account when exploring.

The system-level performance also underlines the fact that the gains that are made in the architectural level and circuit level are directly reflected in the increased throughput and reduced inference latency in real workloads. In the proposed design, energy savings are obtained in accordance with the requirements of edge devices, which need to maintain constant AI processing on a strict power budget. Generally speaking, the combination of AI-based optimization, quantum-inspired energy-saving, and security hardware approaches leads to a more balanced and resilient VLSI implementation, which can cover the current embedded intelligence application.

Conclusion

The paper introduces a common approach to the design of secure, power-efficient, and high performance VLSI systems targeted at edge and autonomous computing systems. The proposed framework can solve issues that are difficult to solve by traditional design methods, implementing AI-based design automation, integrating quantum-inspired ideas of reversible logic, and leveraging hardware security. The AI optimizer can aid the exploration of designs with surrogate-based PPA prediction, which greatly enhances the rate of convergence and the quality of the design. Quantum-inspired datapath has the advantage of minimizing switching activity and power consumption and competitive delay and area figures. At the same time, the combined security primitives enhance the design against CPA and SAT-based attacks with little overhead.

The experimental analysis is sure that this approach can achieve significant returns in terms of PPA, security, and workload performance metrics. The architecture is shown to be suitable to be used in real-time edge and autonomous systems by lower inference latency, lower energy per operation, and higher throughput. The sufficiently enhanced complexity of attack in SAT and the correlation leakage are other indicators that the design is resilient in adverse conditions. The combination of the three outcomes demonstrates that the integration of AI-based optimization, low-entropy reversible logic, and security co-design is the way to go in the future of efficient and trustworthy VLSI systems.

Future research can consider scaling the methodology to more complex system-on-chip designs, one of these being generative AI to generate RTL code, scale quantum-inspired blocks to larger arithmetic units, and dynamic security adaptation to situations with a changing threat model.

References

1. 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
2. Kavitha, M. (2024). Embedded system architectures for autonomous vehicle navigation and control. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 31–36. https://doi.org/10.31838/ESA/01.01.06
3. Kochar, D. V., Wang, H., Chandrakasan, A. P., & Zhang, X. (2024). LEDRO: LLM-enhanced design space reduction and optimization for analog circuits. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2411.12930
4. Moura, P. R. D., Villarreal, E. R. L., Fonsêca, D. A. de M., & Salazar, A. O. (2025). Post-quantum cryptography for the internet of things: new approach. The Journal of Engineering and Exact Sciences, 11(1), 21741. https://doi.org/10.18540/jcecvl11iss1pp21741
5. Patra, A. C., Rout, S. K., & Ravindran, A. (2024). AiEDA: agentic AI design framework for digital ASIC system design. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2412.09745
6. Petrie, J. (2025). Embedded off-switches for AI compute. https://doi.org/10.48550/ARXIV.2509.07637
7. 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
8. Rahim, R. (2024). Optimizing reconfigurable architectures for enhanced performance in computing. SCCTS Transactions on Reconfigurable Computing, 1(1), 11–15. https://doi.org/10.31838/RCC/01.01.03
9. Uhlich, S., Bonetti, A., Venkitaraman, A., Momeni, A., Matsuo, R., Hsieh, C. T., Ohbuchi, E., & Servadei, L. (2024). GraCo—A Graph Composer for Integrated Circuits. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2411.13890
10. Wang, T., Zhang, C., Zhang, X., Gu, D., & Cao, P. (2024). Optimized hardware-software co-design for Kyber and dilithium on RISC-V SoC FPGA. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(3), 99. https://doi.org/10.46586/tches.v2024.i3.99-135
11. Wang, Y., Ye, W., He, Y., Chen, Y., Qu, G., & Li, A. (2025). MCP4EDA: LLM-powered model context protocol RTL-to-GDSII automation with backend aware synthesis optimization. https://doi.org/10.48550/ARXIV.2507.19570
12. Xu, H., Liu, D., Merkel, C., & Zuzak, M. (2023). Exploiting logic locking for a neural Trojan attack on machine learning accelerators. Proceedings of the Great Lakes Symposium on VLSI 2022, 351. https://doi.org/10.1145/3583781.3590242
13. Alnaseri, O., Himeur, Y., Atalla, S., & Mansoor, W. (2025). Complexity of post-quantum cryptography in embedded systems and its optimization strategies. *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 776. https://doi.org/10.1109/iwcmc65282.2025.11059522
14. Amuru, D., Zahra, A., Vudumula, H. V., Cherupally, P. K., Gurram, S. R., Ahmad, A., & Abbas, Z. (2023). AI/ML algorithms and applications in VLSI design and technology. Integration, 93, 102048. https://doi.org/10.1016/j.vlsi.2023.06.002
15. Banerjee, S., Sahu, P., Luo, M., Vahldiek-Oberwagner, A., Yadwadkar, N. J., & Tiwari, M. (2024). SoK: a systems perspective on compound AI threats and countermeasures. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.13459
16. Bommana, S. R., Veeramachaneni, S., Ahmed, S. E., & Srinivas, M. (2025). Mitigating side channel attacks on FPGA through deep learning and dynamic partial reconfiguration. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-98473-3
17. Chu, S., & Ke, S. Z. (2024). Area-time efficient hardware implementation for binary ring-LWE based post-quantum cryptography. *IEEE Transactions on Emerging Topics in Computing, 13*(3), 724. https://doi.org/10.1109/tetc.2024.3482324
18. Dorofte, M., & Krein, K. (2024). Novel approaches in AI processing systems for their better reliability and function. International Journal of Communication and Computer Technologies, 12(2), 21–30. https://doi.org/10.31838/IJCCTS/12.02.019. Fiolhais, L., & Sousa, L. (2023). QR TPM in programmable low-power devices. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2309.17414
19. He, P., Tu, Y., Xie, J., & Jacinto, H. S. (2023). KINA: Karatsuba Initiated Novel Accelerator for Ring-Binary-LWE (RBLWE)-Based Post-Quantum Cryptography. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 31(10), 1551. https://doi.org/10.1109/tvlsi.2023.3302289